Abstract Algebra

Stjepan Poljak

Introduction I.

There is no higher intention for this script than to serve as a collection of solutions to problems in *The Book of Abstract Algebra* by Charles C. Pinter. I will, however, write down important definitions and theorems which are either necessary for solving exercises in the book or are of certain interest to the author of these passages. If anyone is to find this script, I certainly do hope it serves him well.

Introduction II.

As my works expanded far beyond the book of Charles C. Pinter, and they include some of my thoughts and conclusions, I have felt proper, then, to add some basic introduction to category theory, some of my excercises and theorems. Long have I fought my weak mind to discover something new, and most of my theorems were derived and proved independently, as my own ideas. However, as I have the fortune of the most misfortunate men, often have I discovered, that my observations were already observed. As to the category theory and new discoveries, I would only add one further comment. Everything has been put under a microscope, I feel that there is nothing new; and category theory does not add one single new specimen for observation, it only shifts the focus of observation. Oh, and one more thing, most have asked me with rather astonishing curiosity why I am writing this in English. The reason is simple. To show my ability to handle English. Furthermore, most of the namings are, especially for category theory, unknown to me in Croatian language, as I have access (for the time being) only to English literature; to invent my own word in Croatian for the name of the definiens would be, from my point of view, highly irrational and downright dumb. Yet, one may argue that writing in English is more irrational than only inventing names that resemble Slavic origin, which is my mother language. I may then argue, that my mother language is ugly, meaningless, clumsy and irrationaly difficult (and difficulty is not a positive quality) and that I prefer any other language as my mother language. If I had the ability to handle modern mathematical notions in Latin, may Heaven be my witness, I would do so without any hesitation.

Groups

In this chapter we shall deal with operations which take only two elements (an ordered pair) from a set to produce a unique third element from the same set. Altough this can be generalized and in the further text it won't be ambiguous if we use the term *operation*, we will however call it a *binary operation* due to specificity (to avoid the confusion if the reader is familiar with other terms other than these).

Definition. Let S be a non-empty set. *Binary operation* $*$ is every function of the form

$$* : S \times S \to S.$$

To further explain necessary conditions this definition imposes on us we have to take into consideration that every (binary) operation is necessary a *function*. Let us remember that a function is, non-formally speaking, a mapping from one set to the other such that every element from the first set (domain) is mapped in the second set (codomain) uniquely (in other words every element from domain must have one and only one corresponding element in the codomain). This must also hold for binary operations. Therefore, every binary operation (coming from the definition of the function) must satisfy these three conditions (*axioms of totality*[1]):

1. Operation $*$ must be defined for every ordered pair in S (e.g. division on $\mathbb{R}$ is not an operation for it is not defined when dividing with zero).

2. It must produce a unique element in S (we cannot have two or more different elements resulting from the same operation).

3. The operation must be closed on S; in other words, the element it produces is necessarily in S (e.g. subtracting on $\mathbb{N}$ is not an operation for it is not closed in $\mathbb{N}$; subtracting 5 from 3 yields -2 which is in $\mathbb{Z}$, but not in $\mathbb{N}$).

If for a certain rule only the axioms of uniqueness and closure are satisfied, that rule is then called *partial operation*, as it is defined by a partial function (a type of relation which does not require the mapping to be defined for every element in

[1] Axioms of totality would be more formally written by using first order logic semantics as:

1. $(\forall (x, y) \in S)\,(\exists\,(x * y))$
2. $(\forall (x, y), (m, n) \in S)\,((x * y \neq m * n) \to ((x, y) \neq (m, n)))$
3. $(\forall (x, y) \in S)\,((x * y) \in S)$

domain as opposed to total function which is a synonime for a function). One last note on the condition of the requirement for S to be a non-empty set. We do not want to deal with empty sets in this way, especially if we are considering its elements later in the definition, or propositions. For if S were to be empty, then we enter the area of a vacuous truth: everything we claim about its elements is logically (if not epistemologically) true (and the negation of the claim) because there are no elements to which we can assign these truths (if I were to say that cats which live underwater have nine-tails that would be true - so would be the opposite; there are no cats which live underwater, so logically I can claim anything I want about them; on the other hand, from an epistemological view, I *know* from experience that there are no cats living underwater and I would discern such claim as non-sense). This is one of the reasons why we have to be careful when *thinking logically*. Thinking logically takes form into consideration more than it does contents, and as everything in this universe, they are inseparable. And mathematics being mostly concerned with more form than contents (compared to other sciences, the only exception being logic itself) we have to be extremely careful not to fall into a paradox (which some say is a bad thing). Let us now elaborate on properties[2] an operation defined as above can have:

1. *Associativity.* We say that operation $*$ is associative if $(a * b) * c = a * (b * c)$, $\forall a, b \in S$. The importance of associativity comes from the fact that we can combine three elements using the same operation (but without changing their order; only their priorities) and obtain the same result. Associativity holds for addition, multiplication, composition, but not for subtraction and division.

2. *Commutativity.* Operation $*$ is commutative if $a * b = b * a,\ \forall a, b \in S$. Addition and multiplication are commutative, while composition, sutraction and division are not.

3. *Existence of identity.* We say that operation $*$ has an identity (neutral) element e if $\exists e \in S :\ a * e = e * a = a,\ \forall a \in S$. Neutral element for addition is 0, for multiplication 1; when we apply neutral element to any element on which the operation is defined we produce that element (on which the neutral element was applied in respect to the defined operation). Notice that here we assumed that operation $*$ is commutative (at least when observing neutral element). If that is not the case, then an operation may have only a left or a right neutral element

[2]In FOL, these properties can be written as:

1. $(\forall a, b, c \in S)\,((a * b) * c = a * (b * c))$
2. $(\forall a, b \in S)\,(a * b = b * a)$
3. $(\exists e \in S)\,(\forall x \in S)\,(x * e = e * x = x)$
4. $(\forall x \in S)\left(\exists x^{-1} \in S\right)\left(x * x^{-1} = x^{-1} * x = e\right)$

(in this case it has no neutral element, only exception being when left element equals the right element, in other words if it's commutative).

4. *Existence of inverse.* Operation $*$ has an inverse element a^{-1} if $\exists a^{-1} :\ a * a^{-1} = a^{-1} * a = e,\ \forall a \in S$. Notice that for an inverse to exist it is necessary that the same operation already has satisfied the condition of a neutral element. For addition, the inverse element is $-a$ and for multiplication a^{-1} (on the set of reals only zero has no inverse, therefore, only the set of reals without zero has an inverse). Similiar to identity, the inverse also assumes commutativity (at least for inverse; if that is not the case then we speak of left or right inverse element - if they are equal then we call it's simply an inverse element).

Definition. Let us take into consideration an ordered pair $(S, *)$. If such ordered pair satisfies conditions of associativity and existence of identity and inverse elements in respect to $*$ defined on S, then we call it a *group*. If a group also satisfies commutativity then we call it an *Abelian* or *commutative group*.

Problem. Which of the following rules are operations on the indicated set?

1. $a * b = \sqrt{|ab|}$, on the set $\mathbb{Q}$.
2. $a * b = a \ln b$, on the set $A = \{x \in \mathbb{R} :\ x > 0\}$.
3. $a * b$ is a root of the equation $x^2 - a^2b^2 = 0$, on the set $\mathbb{R}$.
4. Subtraction, on the set $\mathbb{Z}$.
5. Subtraction, on the set $B = \{n \in \mathbb{Z} :\ n \geq 0\}$.
6. $a * b = |a - b|$, on the set $C = \{n \in \mathbb{Z} :\ n \geq 0\}$.

Solution. First rule, $a * b = \sqrt{|ab|}$ defined on the set $\mathbb{Q}$ is not an operation because the square root of the product of two rational numbers can be an irrational number, e.g. $\frac{1}{2} * 4 = \sqrt{2}$; we see that $\frac{1}{2}, 4 \in \mathbb{Q}$, but $\sqrt{2} \in \mathbb{I}$ (operation is not closed on $\mathbb{Q}$). It would, however, be an operation if we were to expand the set on which it is defined to the set of reals, $\mathbb{R}$.

Second rule, $a * b = a \ln b$, on the set A, is not an operation for the similar reasons as the first rule; if we take $1, \frac{1}{e} \in A$ (where e denotes Euler's number), by operation $*$ we would obtain $1 * \frac{1}{e} = 1 \cdot \ln \frac{1}{e} = -1 \notin A$ (for $\log \frac{1}{a} = \log a^{-1} = -\log a$). Rule $*$ would be an operation if we were to take $A^* = \{x \in \mathbb{R} :\ x \geq e\}$; then, the smallest element (as natural logarithm is a strictly increasing function, and every $\ln x \geq 1,\ \forall x \in \mathbb{R},\ x \geq e$) would be $e * e = e \ln e = e \in A^*$ (e would therefore be a neutral element). All other elements would be larger then e and therefore contained in A^*.

Third rule does not satisfy uniqueness. For the equation $x^2 = a^2b^2$ returns two solutions $x = \pm ab$; therefore $a * b = \pm ab$, meaning it is not uniquely definied as we get two different values in return. If we were to take $\mathbb{R}^+$ instead of $\mathbb{R}$, then it would be an operation, as we would observe only positive solutions.

It is trivial to notice that the fourth rule (subtraction) is operation on the set of integers, $\mathbb{Z}$, for it satisfies all three conditions. We will not, however, conduct any rigorous proofs at this point. It is also trivial to notice that the fifth rule is not an operation, for it does not satisfy the condition of closure, for example if we take $3, 4 \in B$, subtracting 4 from 3 produces $-1 \notin B$.

Seventh rule is operation on the given set, which is easy to prove. Absolute value is defined for every real number (therefore also for every integer). Closure is satisfied because $|a - b| \geq 0,\ \forall a, b \in \mathbb{R}$. Uniqueness is also satisfied as absolute value is always unique, in other words it never produces more than one element.

Problem. Each of the following is an operation $*$ on $\mathbb{R}$. Indicate whether or not it is commutative, associative, whether $\mathbb{R}$ has an identity element and an inverse element for every $x \in \mathbb{R}$ with respect to $*$.

1. $x * y = x + y + 1$,
2. $x * y = x + 2y + 4$,
3. $x * y = x + 2y - xy$,
4. $x * y = |x + y|$,
5. $x * y = |x - y|$,
6. $x * y = xy + 1$,
7. $x * y = \max\{x, y\}$,
8. $x * y = \frac{xy}{x+y+1}$, on the set of positive real numbers.

Solution. For each example we will check all four properties in the following way, labeling associativity with "A", commutativity with "C", existence of neutral element with "N" and existence of inverses with "I".

1. $x * y = x + y + 1$

   A. $(x * y) * z = (x + y + 1) * z = x + y + 1 + z + 1 = x + (y + z + 1) + 1 = x * (y + z + 1) = x * (y * z)$.

   C. Valid due to commutativity of addition, $x * y = x + y + 1 = y + x + 1 = y * x$.

N. We seek $e \in \mathbb{R}$ such that $x * e = x$, id est $x + e + 1 = x$. From this expression it is trivial to notice that $e = -1$; $x * (-1) = x + (-1) + 1 = x$.

I. Let us see if there exists $x^{-1} \in \mathbb{R}$ for every $x \in \mathbb{R}$ such that $x * x^{-1} = e$, i.e. $x * x^{-1} = -1$. From definition of operation follows that $x + x^{-1} + 1 = -1$ and we conclude that $x^{-1} = -x - 2$, $x^{-1} \in \mathbb{R}$, $\forall x \in \mathbb{R}$. It is easy to verify that $x * (-x - 2) = x - x - 2 + 1 = -1 = e$, which also hold for $x^{-1} * x$ due to commutativity.

Ordered pair $(\mathbb{R}, *)$ therefore denotes a commutative group.

2. $x * y = x + 2y + 4$

A. $(x * y) * z = (x + 2y + 4) * z = x + 2y + 4 + 2z + 4 = x + 2y + 2z + 8$. This operation is not associative as expression $x * (y * z) = x * (y + 2z + 4) = x + 2(y + 4z + 4) + 4 = x + 2y + 4z + 12$ does not equal previous expression.

C. This operation is also not commutative as $x * y = x + 2y + 4$ differs from $y * x = y + 2x + 4$.

N. We can see that we have a right neutral element $x * e_r = x$, which is $x + 2e_r + 1 = x$, id est $e_r = \frac{-1}{2}$ and that a left neutral element, $e_l + 2x + 1 = x$, is $e_l = -x - 1$. As $e_r \neq e_l$, there is no neutral element.

I. No element $x \in \mathbb{R}$ has an inverse because neutral element is non-existent.

Ordered pair, such as $(\mathbb{R}, *)$ in this exercise, which satisfies only the three axioms of totality is called a *magma* (or sometimes a *groupoid*). If only the axioms of closure and uniqueness are satisfied (operation $*$ being just a partial operation), the ordered pair is called *partial magma*.

3. $x * y = x + 2y - xy$

A. Property of associativity is not satisfied as $(x * y) * z = (x + 2y - xy) * z = x + 2y - xy + 2z - (x + 2y - xy) \cdot z = x + 2y - xy + 2z - xz - 2yz + xyz$ does not equal $x * (y * z) = x * (y + 2z - yz) = x + 2y + 4z - 2yz + x(y + 2z - yz) = x + 2y + 4z + 2y + xy + 2xz - xyz$.

C. It is easy to see that $x * y = x + 2y - xy$ does not equal $y * x = y + 2x - xy$.

N. Due to failure of commutativity for this operation, the property of existence of neutral element will also not be satisfied as $x * e \neq e * x$.

I. As there is no neutral element, the property of existence of inverses cannot be satisfied.

As in previous exercise, ordered pair $(\mathbb{R}, *)$ is a magma.

4. $x * y = |x + y|$

   A. As in previous exercises, $x * (y * z) = x * |y + z| = |x + |y + z||$ differs from $(x * y) * z = |x + y| * z = ||x + y| + z|$, therefore associativity is not satisfied. We can think of a counterexample to further assure us in our thoughts; let us take $-5, 4, 2 \in \mathbb{R}$. Then it follows $|-5 + |4 + 2|| = |-5 + 6| = 1$ and $||-5 + 4| + 2| = |1 + 2| = 3$.

   C. Operation is, however, commutative as $x * y = |x + y| = |y + x| = y * x$.

   N. We obtain neutral element from $x * e = x$, i.e. $|x + e| = x$. This equation gives two solutions, one being 0 and the other being $-2x$. Already it is obvious that $-2x$ is not a neutral element as we need a unique neutral element for all $x \in \mathbb{R}$, not the reverse. We can, however, test $e = 0$. If we take $|x + 0| = |0 + x| = |x|$ we can see that this would be a neutral element only for non-negative real numbers, for if we take $-5 \in \mathbb{R}$ we see that $|-5 + 0| = 5 \neq -5$. Therefore, there is no neutral element.

   I. Existence of inverses does not come into question as there is no neutral element on which to observe, i.e. search for, inverses.

   This ordered pair $(\mathbb{R}, *)$ is a *commutative magma*.

5. $x * y = |x - y|$

   A. This operation is analogous to the previous operation and it is easy to verify that associativity is not satisfied, for $|x - |y - z|| \neq ||x - y| - z|$. We can take a counterexample, e.g. $5, 4, 2 \in \mathbb{R}$, to make sure our assertion is in order; $|5 - |4 - 2|| = |5 - 2| = 3$ and $||5 - 4| - 2| = |1 - 2| = 1$.

   C. Commutativity holds, because $|x - y| = |-(y - x)| = |y - x|$.

   N. Neutral element would be, analogous to the previous example, $e = 0$, but $|x - 0| = |0 - x| = |x|$, which can only hold for non-negative real numbers.

   I. Inverses are non-existent, for there is no neutral element.

   As in the previous case, ordered pair $(\mathbb{R}, *)$ is also a commutative magma.

6. $x * y = xy + 1$

   A. We obtain that $(x * y) * z = (xy + 1) * z = (xy + 1) \cdot z + 1 = xyz + z + 1$ and $x * (y * z) = x * (yz + 1) = x(yz + 1) + 1 = xyz + x + 1$. Those two expressions being different, operation is not associative.

   C. Operation is commutative as $x * y = xy + 1 = yx + 1 = y * x$ for all $x, y \in \mathbb{R}$.

   N. From $x * e = x$ we get $xe + 1 = x$, i.e. $e = \frac{x-1}{x}$, $x \neq 0$. Therefore, there is no neutral element in $\mathbb{R}$.

I. Property of existence of identity not being satisfied, there can be no inverses.

$(\mathbb{R}, *)$ is a commutative magma.

7. $x * y = \max\{x, y\}$

   A. Let us show that both $\max\{\max\{x, y\}, z\}$ and $\max\{x, \max\{y, z\}\}$ both produce the same element - the one with the greatest value among x, y, z. It is sufficient that we observe only two cases, when y is of the greatest value and when x or z are of the greatest vaule (those cases are analogous, because when we observe x on left side, on the right side we get the case what would be for z on the left side and conversely). Let us suppose that y is of the greatest value; then on the left side we have $\max\{x, y\} = y$ and therefore $\max\{y, z\} = y$. On the right side, similarly it holds that $\max\{y, z\} = y$; then it follows that $\max\{y, z\} = y$, so in this case associativity is satisfied. But what if x (or z) is the element of the greatest value? On the left side we would surely now have that $\max\{x, y\} = x$ and then that $\max\{x, z\} = x$. Yet, on the right side, following from condition that $x \geq y$ and $x \geq z$, we have $x \geq \max\{y, z\} = m$. Therefore, $\max\{x, m\} = x$, which proves associativity.

   C. Commutativity is satisfied as $x * y = \max\{x, y\} = \max\{y, x\} = y * x$.

   N. When will hold that $\max\{x, e\} = x$? It will hold if and only if $x \geq e$. In order for it to hold generally, we would need to take the smallest value possible for e in the set of reals, but no matter how small we set it to be, there can always be smaller $x \in \mathbb{R}$. Therefore, as there is no smallest real number, there can be no neutral element for this operation.

   I. There are no inverses as there is no neutral element.

Ordered pair $(\mathbb{R}, *)$, where associativity holds is called a *semigroup*. This one is also commutative (which is not necessary for it to be a semigroup).

8. $x * y = \frac{xy}{x+y+1}$

   A. Let us see if $x * (y * z) = (x * y) * z$. On the left side we have

$$\begin{aligned} x * (y * z) &= x * \left(\frac{yz}{y+z+1}\right) = \frac{x\frac{yz}{y+z+1}}{x + \frac{yz}{y+z+1} + 1} = \frac{\frac{xyz}{y+z+1}}{\frac{yz+x(y+z+1)+(y+z+1)}{y+z+1}} \\ &= \frac{xyz}{yz + xy + xz + 2z + y + 1}. \end{aligned}$$

   On the right side,

$$(x*y)*z = \left(\frac{xy}{x+y+1}\right)*z = \frac{z\frac{xy}{x+y+1}}{\frac{xy}{x+y+1}+z+1} = \frac{\frac{xyz}{x+y+1}}{\frac{xy+z(x+y+1)+(x+y+1)}{x+y+1}}$$
$$= \frac{xyz}{xy+zx+zy+x+y+z+1}.$$

These two expressions differ, therefore associativity does not hold.

C. Commutativity, however, holds because $x*y = \frac{xy}{x+y+1} = \frac{yx}{y+x+1} = y*x$.

N. We look for neutral element by observing expression $x*e = x$, i.e. $\frac{xe}{x+e+1} = x$. We multiply it with $x+e+1$ (which is always $\neq 0$, for $x, e, 1 \in \mathbb{R}^+$) and obtain $xe = x^2 + xe + x$. As xe is cancelled, we are left with $x^2 + x = 0$, which does not say much about the nature of e. Therefore, there is no neutral element.

I. There is no neutral element, so there are also no inverses.

Ordered pair $(\mathbb{R}^+, *)$ is a commutative magma.

Problem. Using the following three tables check the operation $*$ on the set $A = \{a, b\}$ for all four properties (note that (i, j) element in the matrix represents one in the i-th row and j-th column).

1.

$*$	a	b
a	a	b
b	b	a

2.

$*$	a	b
a	b	a
b	b	a

3.

$*$	a	b
a	b	a
b	b	b

Solution (1.)

A. Let us check associativity of this operation. We need to examine all eight cases (for we have three places where we can put two elements, that is $2 \cdot 2 \cdot 2 = 8$)[3]:

1. $a*(a*a) = a*a = a$ and $(a*a)*a = a*a = a$,
2. $a*(a*b) = a*b = b$ and $(a*a)*b = a*b = b$,
3. $a*(b*a) = a*b = b$ and $(a*b)*a = b*a = b$,
4. $a*(b*b) = a*a = a$ and $(a*b)*b = b*b = a$,
5. $b*(a*a) = b*a = b$ and $(b*a)*a = b*a = b$,
6. $b*(a*b) = b*b = a$ and $(b*a)*b = b*b = a$,

[3]Notice that we always perform the operation in the form of row$*$column, e.g. in third example, $a*b = a$, where all other combinations equal b.

7. $b * (b * a) = b * b = a$ and $(b * b) * a = a * a = a$,
8. $b * (b * b) = b * a = b$ and $(b * b) * b = a * b = b$.

As two expressions in all eight cases are equal, associativity is satisfied.

C. Commutativity is valid, which is obvious from the symmetry observed in the table (also, $a * b = b = b * a$).

N. Let us try to find a neutral element; we have only two candidates, a and b. Let us suppose that $e = a$ is a neutral element. Then $a * e = a$ and $b * e = e * b = b$. If we also consider $e = b$, then $a * e = e * a = b$ and $b * e = a$; it is obvious that this is not valid, therefore $e = a$ is a neutral element in respect to $*$ for all $x \in A$ (this can also be observed from the fact that the column and row in the table corresponding to a leaves other elements intact).

I. Let us verify that each element $x \in A$ has its corresponding inverse element. First, if we take $a * a^{-1} = e$, i.e. $a * a^{-1} = a$, we see that $a^{-1} = a$; it is also valid for $a^{-1} * a = e$ because $a * a = a$. Now, if we take $b * b^{-1} = e$ it follows that $b^{-1} = b$ as $b * b = a$. It is trivial to notice that this is valid also for $b^{-1} * b = e$. To conclude, every element in A has its inverse element in A, in respect to $*$.

Ordered pair $(A, *)$ is an Abelian group.

Solution. (2.)

A. We would examine all eight cases, but even in the first case we can see that associativity is not satisfied, beacuse $a*(a * a) = a*b = a$ differs from $(a * a)*a = b * a = b$.

C. Operation is not commutative which can be seen from the previous example; $a * b = a$, while $b * a = b$.

N. We look for neutral element in $a * e = e * a = a$ and $b * e = e * b = b$. Such e does not exist, because, if we take $e = a$, then $a * a = b$ is valid, but $b * a = b$ does not hold because $a * b = a$. Similarly, if we take $e = b$, not even $b * b = a$ holds. In conclusion, there is no neutral element.

I. There are no inverses.

Ordered pair $(A, *)$ is a magma.

Solution. (3.)

A. We can easily see that this operation is not associative as $a * (a * a) = a * b = a$ and $(a * a) * a = b * a = b$.

C. From upper counterexample we can also see that this operation is not commutative ($a * b = a$ and $b * a = b$).

N. Neutral element is also non-existent because if we take $a * e = e * a = a$, we can have $e = b$ so that $a * b = a$, but $b * a = b$. If we take $e = a$, then we have the same thing with b.

I. There are no inverses.

Ordered pair $(A, *)$ is a magma.

Problem. Digital computers and related machines process information which is received in the form of input sequences. An *input sequence* is a finite sequence of symbols from some alphabet A. For instance, if $A = \{0, 1\}$ (that is, if the alphabet consists of only the two symbols 0 and 1), then examples of input sequences are 011010 and 10101111. If $A = \{a, b, c\}$, then examples of input sequences are *babbcac* and *cccabaa*. *Output sequences* are defined in the same way as input sequences. The set of all sequences of symbols in the alphabet A is denoted by A^*.

There is an operation on A^* called *concatenation*: If $\mathbf{a}$ and $\mathbf{b}$ are in A^*, say $\mathbf{a} = a_1a_2 \dots a_n$ and $\mathbf{b} = b_1b_2 \dots b_m$, then

$$\mathbf{ab} = a_1a_2 \dots a_nb_1b_2 \dots b_m.$$

In other words, the sequence $\mathbf{ab}$ consists of the two sequences $\mathbf{a}$ and $\mathbf{b}$ end to end. For example, in the alphabet $A = \{0, 1\}$, if $\mathbf{a} = 1001$ and $\mathbf{b} = 010$, then $\mathbf{ab} = 1001010$.

The symbol λ denotes the empty sequence.

1. Prove that the operation defined above is associative.

2. Explain why the operation is not commutative.

3. Prove that there is an identity element for this operation.

Solution. Let A be an alphabet and A^* the set of all sequences of symbols in A. Then, let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in A^*$, in other words, $\mathbf{a} = a_1a_2 \dots a_p$, $\mathbf{b} = b_1b_2 \dots b_r$ and $\mathbf{c} = c_1c_2 \dots c_s$, where $p, r, s \in \mathbb{N}$.

1. First we will prove associativity, i.e. that $(\mathbf{ab})\,\mathbf{c} = \mathbf{a}\,(\mathbf{bc})$. If we check the left hand side of the equation we obtain $a_1a_2 \dots a_pb_1b_2 \dots b_r\mathbf{c}$, that is

$$a_1a_2 \dots a_pb_1b_2 \dots b_rc_1c_2 \dots c_s.$$

It is trivial to notice that the right hand side is the same and that associativity holds for this operation on A^* as $\mathbf{a}b_1b_2\ldots b_rc_1c_2\ldots c_s$ equals

$$a_1a_2\ldots a_p\ldots b_1b_2\ldots b_r\ldots c_1c_2\ldots c_s.$$

2. The operation is not commutative as the result of the operation depends on which side the element was applied; it is easy to show that by a simple counterexample, such as

$$\mathbf{ab} = a_1a_2\ldots a_pb_1b_2\ldots b_r \neq b_1b_2\ldots b_ra_1a_2\ldots a_p = \mathbf{ba}.$$

3. Let us suppose that an empty sequence λ is the identity element for this operation. We have to show that $\lambda\mathbf{a} = \mathbf{a}\lambda = \mathbf{a}$. It is easy to see that $\lambda a_1a_2\ldots a_p = a_1a_2\ldots a_p = \mathbf{a}$ and that $a_1a_2\ldots a_p\lambda = a_1a_2\ldots a_p = \mathbf{a}$. Can there exist an inverse element for every $\mathbf{a} \in A^*$? No, because from any non-empty sequence $\mathbf{a}$ we can never obtain the empty sequence λ by contatenation. All we can do is accumulate more and more symbols by performing the operation of concatenation, but never take them away to get empty sequence. So, the ordered pair $(A^*, \circ)$, where $\circ$ denotes the operation of concatenation, is at most a commutative *monoid* (an ordered pair of a set and of an operation that is defined on a set is called a monoid if associativity and identity hold; the only difference from a group is that there are some elements without inverses).

Problem. Prove that each of the following sets, with the indicated operation, is an Abelian group.

1. $x * y = x + y + k$, where k is a fixed constant, on the set $\mathbb{R}$.
2. $x * y = \frac{xy}{2}$, on the set $A = \{x \in \mathbb{R} :\ x \neq 0\}$.
3. $x * y = x + y + xy$, on the set $B = \{x \in \mathbb{R} :\ x \neq -1\}$.
4. $x * y = \frac{x+y}{xy+1}$, on the set $C = \{x \in \mathbb{R} :\ -1 < x < 1\}$.

Solution. Let us prove all properties, as in previous examples, for the ordered pairs above.

1. $x * y = x + y + k$, where k is a fixed constant, on the set $\mathbb{R}$.

   A. It is trivial to show that $(x * y) * z = x * (y * z)$, i.e. associativity holds. For the left hand side we have $(x + y + k)*z = x+y+k+z+k = x+y+z+2k$. On the right hand side, we obtain $x*(y + z + k) = x+y+z+k+k = x+y+z+2k$.

C. Commutativity holds because addition is also commutative (and only operation used in $*$), that is, $x * y = x + y + k = y + x + k = y * x$.

N. Neutral element can be found from expression $x * e = e * x = x$. We take $x * e = x$, that is, $x + e + k = x$ and obtain $e = -k$. It is easy to see that it is also a left neutral element (and by that a neutral element), as $-k * x = -k + x + k = x$, for all $x \in \mathbb{R}$.

I. We will obtain inverses from expression $x * x^{-1} = e$, that is $x + x^{-1} + k = -k$. We see that $x^{-1} = -x - 2k$. We can also show that x^{-1} is a left inverse by showing that $x^{-1} * x = -x - 2k + x + k = -k = e$, for all $x \in \mathbb{R}$.

Ordered pair $(\mathbb{R}, *)$ is truly an Abelian group.

2. $x * y = \frac{xy}{2}$, on the set $A = \mathbb{R} \setminus \{0\}$.

A. First, $x * (y * z) = x * \left(\frac{yz}{2}\right) = \frac{x\frac{yz}{2}}{2} = \frac{xyz}{4}$. On the other hand, $(x * y) * z = \left(\frac{xy}{2}\right) * z = \frac{z\frac{xy}{2}}{2} = \frac{xyz}{4}$. Both sides being equal, associativity holds.

C. Operation is commutative as $x * y = \frac{xy}{2} = \frac{yx}{2} = y * x$ for all $x, y \in A$.

N. Let us consider $\frac{xe}{2} = x$. We have $xe = 2x$, i.e. $e = 2$ when we divide expression by $x \neq 0$. As operation $*$ is commutative, the existence of the neutral element in $\mathbb{R} \setminus \{0\}$ is proved.

I. Is there $x^{-1} \in A$ such that $\frac{xx^{-1}}{2} = 2$? We have $xx^{-1} = 4$, and when we divide everything with $x \neq 0$, we obtain $x^{-1} = \frac{4}{x}$, for all $x \in A$ (as operation is commutative).

Ordered pair $(\mathbb{R} \setminus \{0\}, *)$ is an Abelian group.

3. $x * y = x + y + xy$, on the set $B = \mathbb{R} \setminus \{-1\}$.

A. On the left hand side we have $x * (y * z)$
$= x * (y + z + yz) = x + (y + z + yz) + x(y + z + yz) = x + y + z + yz + xy + xz + xyz$, while on the right hand side we have $(x * y) * z = (x + y + xy) * z = (x + y + xy) + z + z(x + y + xy) = x + y + z + xy + zx + yz + xyz$. Therefore, operation $*$ is associative.

C. Commutativity holds because $x * y = x + y + xy = y + x + yx = y * x$.

N. We'll try and find $e \in B$ such that $x * e = x$, i.e. $x + e + xe = x$. The two x cancel out and we have $e(1 + x) = 0$. After dividing with $(1 + x) \neq 0$ we have $e = 0$. As operation is commutative, neutral element is absolute for all $x \in B$.

I. We consider expression $x + x^{-1} + xx^{-1} = 0$. We then have $x^{-1}(1 + x) = -x$. After dividing expression with $(1 + x) \neq 0$ (notice that here is the condition that $x \neq -1$), we have $x^{-1} = -\frac{x}{1+x}$, for all $x \in B$ (operation being commutative, we don't have to check the existence and equality of left and right inverses).

Ordered pair $(\mathbb{R}\setminus\{-1\}, *)$ is an Abelian group.

4. $x * y = \frac{x+y}{xy+1}$, on the set $C = \{x \in \mathbb{R} : \ -1 < x < 1\}$.

   A. First, we obtain $(x * y)*z = \left(\frac{x+y}{xy+1}\right)*z = \frac{\frac{x+y}{xy+1}+z}{\frac{x+y}{xy+1}z+1} = \frac{\frac{x+y+xyz+z}{xy+1}}{\frac{xz+yz+xy+1}{xy+1}} = \frac{x+y+xyz+z}{xz+yz+xy+1}$.
   Next, we have $x * (y * z) = x * \left(\frac{y+z}{yz+1}\right) = \frac{x+\frac{y+z}{yz+1}}{x\frac{y+z}{yz+1}+1} = \frac{\frac{xyz+x+y+z}{yz+1}}{\frac{xy+xz+yz+1}{yz+1}} = \frac{x+y+z+xyz}{xz+yz+xy+1}$.
   Therefore, associativity holds (note that the denominator must not equal zero; yet, on the set C, we are only allowed to use numbers whose absolute value is less than one, i.e. numbers of the form $\pm\frac{a}{b}$, where $a < b$ and $a, b \in \mathbb{R}_0^+$ and $b \neq 0$; therefore, if we multiply such numbers as in set C, we will always obtain a new number from set C, i.e. a number whose absolute value is less than 1 so we can never get a zero denominator).

   C. Operation is commutative as $x * y = \frac{x+y}{xy+1} = \frac{y+x}{yx+1} = y * x$.

   N. Let us find $e \in C$ such that $\frac{e+x}{ex+1} = x$. We multiply the previous expression with denominator on the left-hand side and thus obtain $e+x = ex^2+x$. Now we have $ex^2 - e = 0$, i.e. $e(x^2 - 1) = 0$. Either it is $e = 0$ or $x = \pm 1$. From $x = \pm 1$ we get no information about neutral element, therefore our only choice is that $e = 0$. Indeed, it is easily verified that $\frac{0+x}{0\cdot x+1} = \frac{x+0}{x\cdot 0+1} = \frac{x}{1} = x$.

   I. Now we have to find x^{-1} such that $\frac{x+x^{-1}}{xx^{-1}+1} = 0$. Denominator here serves no purpose as only nominator is allowed to be zero (and denominator cannot be zero in C anyway). So $x + x^{-1} = 0$ and $x^{-1} = -x$.

   Ordered pair $(\langle -1, 1\rangle, *)$ is an Abelian group.

Problem. Which of the following subsets of $\mathbb{R} \times \mathbb{R}$, with the indicated operation, is a group?

1. $(a, b) * (c, d) = (ad + bc, bd)$, on the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y \neq 0\}$.
2. $(a, b) * (c, d) = (ac, bc + d)$, on the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} : \ x \neq 0\}$.
3. Same operation as in part 2, but on the set $\mathbb{R} \times \mathbb{R}$.
4. $(a, b) * (c, d) = (ac - bd, ad + bc)$, on the set $\mathbb{R} \times \mathbb{R}$ with the origin deleted.

5. Consider the operation of the preceeding problem on the set $\mathbb{R} \times \mathbb{R}$. Is this a group? Explain.

Solution.

1. $(a,b) * (c,d) = (ad + bc, bd)$, on the set $\{(x,y) \in \mathbb{R} \times \mathbb{R} : \ y \neq 0\}$

   A. First, we have $((a,b) * (c,d)) * (e,f) = (ad + bc, bd) * (e,f)$ $= ((ad + bc) f + bde, bdf) = (adf + bcf + bde, bdf)$. On the other hand, we have $(a,b) * ((c,d) * (e,f)) = (a,b) * (cf + ed, df) = (adf + b(cf + ed), bdf)$ $= (adf + bcf + bde, bdf)$. Therefore, associativity holds.

   C. We can easily conclude that $(a,b) * (c,d) = (ad + bc, bd) = (cb + ad, bd) = (c,d) * (a,b)$ which proves commutativity.

   N. Let us find (e_1, e_2) such that $(e_1, e_2) * (a,b) = (a,b)$, i.e. $(e_1 b + e_2 a, e_2 b) = (a,b)$. We have two equations, first being $e_1 b + e_2 a = a$ and $e_2 b = b$. It is trivial to see that necessarily $e_2 = 1$. Now we have $e_1 b + a = a$ which yields $e_1 = 0$. Neutral element is $(e_1, e_2) = (0,1)$, as commutativity also holds we need not check $(a,b) * (0,1) = (a,b)$.

   I. From expression $(a^{-1}, b^{-1}) * (a,b) = (0,1)$ we shall derive the inverse elements. We have $(a^{-1}b + b^{-1}a, b^{-1}b) = (0,1)$ from which we have $a^{-1}b + b^{-1}a = 0$ and $b^{-1}b = 1$. Obviously, $b^{-1} = \frac{1}{b}$ ($b \neq 0$ being consistent with the definition of the corresponding set), so by inserting new equality into first equation, we obtain $a^{-1}b + \frac{1}{b}a = 0$. That is, $a^{-1}b = -\frac{a}{b}$, and by dividing the equation with $b \neq 0$ we obtain $a^{-1} = -\frac{a}{b^2}$. Inverse elements are therefore defined for every element in the set as $(a^{-1}, b^{-1}) = \left(-\frac{a}{b^2}, \frac{1}{b}\right)$.

   Ordered pair $(\mathbb{R} \times (\mathbb{R} \setminus \{0\}), *)$ is an Abelian group.

2. $(a,b) * (c,d) = (ac, bc + d)$, on the set $\{(x,y) \in \mathbb{R} \times \mathbb{R} : \ x \neq 0\}$.

   A. On the left hand side, we have $((a,b) * (c,d)) * (e,f) = (ac, bc + d) * (e,f) = (ace, bce + de + f)$. On the right hand side, $(a,b) * ((c,d) * (e,f)) = (a,b) * (ce, de + f) = (ace, bce + de + f)$. This operation is associative.

   C. It is obvious that $(a,b) * (c,d) = (ac, bc + d) \neq (ac, da + b) = (c,d) * (a,b)$ so we conclude that the operation is not commutative.

   N. First, we check the existence of (e_1, e_2) on the set of $\mathbb{R}^2$ without $x = 0$, such that $(e_1, e_2) * (a,b) = (a,b)$. We have $(e_1 a, e_2 a + b) = (a,b)$. It has to be $e_1 a = a$, i.e. $e_1 = 1$ and $e_2 a + b = b$, that is, $e_2 = 0$. Notice that it must be $a \neq 0$. Now we can easily obtain $(a,b) * (e_1, e_2) = (a,b) * (1,0) = (a,b)$. Both sides being equal, $(1,0) \in (\mathbb{R} \setminus \{0\}) \times \mathbb{R}$ is a neutral element.

I. Let's find the inverses, if they exist, from $(a^{-1}, b^{-1}) * (a, b) = (1, 0)$. From that we get that $(a^{-1}a, b^{-1}a + b) = (1, 0)$. Now we have $a^{-1}a = 1$, that is $a^{-1} = \frac{1}{a}$ and $a \neq 0$, which is okay, since we already do not allow the first member to be zero. From the second members in the ordered pair we have $b^{-1}a + b = 0$. Now, $b^{-1} = -\frac{b}{a}$ and, again, $a \neq 0$. As commutativity does not hold in general, we must verify $(a, b) * (a^{-1}, b^{-1}) = (1, 0)$, i.e. $(a, b) * \left(\frac{1}{a}, -\frac{b}{a}\right) = (1, 0)$. We have $\left(a \cdot \frac{1}{a}, b \cdot \frac{1}{a} - \frac{b}{a}\right)$, which truly is $(1, 0)$. Therefore, every element in the set on which the operation $*$ is defined has an inverse element.

Ordered pair $((\mathbb{R}\setminus\{0\}) \times \mathbb{R}, *)$ is a group.

3. We need not check all the properties, for the condition that is changed, that is, the set, will affect only the inverses. Associativity still holds, commutativity does not and there is a unique neutral element for all $x \in \mathbb{R}^2$ because it's still valid even if we take $(0, b) * (1, 0) = (0, b)$. Yet, by eliminating the condition that the first member in ordered pairs cannot be zero, we have no inverse element for, exempli gratia, $(0, b)$, where b can be any real number. Notice that, the inverse would be $\left(\frac{1}{0}, -\frac{b}{0}\right)$, which is undefined. Therefore, without inverses, operation $*$ on $\mathbb{R}^2$ is only a monoid.

4. $(a, b) * (c, d) = (ac - bd, ad + bc)$, on the set $\mathbb{R}^2\setminus\{(0, 0)\}$.

   A. We can see that $((a, b) * (c, d)) * (e, f) = (ac - bd, ad + bc) * (e, f)$
   $= (ace - bde - adf - bcf, acf - bdf + ade + bce)$ and that
   $(a, b) * ((c, d) * (e, f)) = (a, b) * (ce - df, cf + de)$
   $= (ace - adf - cfb - deb, acf + ade + bce - bdf)$; the members of the former and the latter ordered pair, by careful observation, coincide respectively, therefore, the operation is associative.

   C. We have $(a, b)*(c, d) = (ac - bd, ad + bc) = (ca - db, da + cb) = (c, d)*(a, b)$ so commutativity holds.

   N. Let us find neutral elements. We take $(e_1, e_2) * (a, b) = (a, b)$, i.e. $(e_1a - e_2b, e_1b + e_2a) = (a, b)$. So we are looking for e_1 and e_2 such that $e_1a - e_2b = a$ and $e_1b + e_2a = b$. If we take from the former equation $e_1 = 1 + \frac{e_2b}{a}$, where $a \neq 0$, and combine it with the latter equation, we get $b + e_2b = b$, that is $e_2 = 0$ and $b \neq 0$. Then it follows that $e_1 = 1$. There is no need to check the other condition, for commutativity holds in general.

   I. Now, we try and find a^{-1} and b^{-1} such that $(a^{-1}, b^{-1}) * (a, b) = (1, 0)$. We now have two equations again, one being $a^{-1}a - b^{-1}b = 1$ and the other $a^{-1}b + b^{-1}a = 0$. From the former we get, e.g. that $a^{-1} = \frac{1+b^{-1}b}{a}$ and $a \neq 0$. We combine it again with the latter equation and we get $\frac{b+b^{-1}b^2}{a} + b^{-1}a = 0$.

Now, we multiply it by a and obtain $b + b^{-1}b^2 + b^{-1}a^2 = 0$. Then, we get $b^{-1} = -\frac{b}{b^2+a^2}$, while $b^2 + a^2 \neq 0$, that is both a and b must be different from zero. By inserting the result into the equation for a^{-1} we see that $a^{-1} = \frac{1}{a} - \frac{b^2}{b^2+a^2}$. So, we found that the inverse for each element except origin is $\left(\frac{1}{a} - \frac{b^2}{b^2+a^2}, -\frac{b}{b^2+a^2}\right)$.

Ordered pair $(\mathbb{R}^2 \setminus \{(0,0)\}, *)$ is Abelian group.

5. Again, as in previous examples, this cannot be a group if we allow origin to be in the set on which such operation is defined. Associativity and commutativity will hold and we can verify if we can have a neutral element for $(0,0)$. That would be $(0,0) * (1,0) = (0,0)$. But we cannot have an inverse element for $(0,0)$ as we would need denominators to be zero. That is impossible. Ordered pair $(\mathbb{R}^2, *)$ is a monoid.

Problem. Operation $A\Delta B = (A \setminus B) \cup (B \setminus A)$ is called a symmetric difference of sets A and B. Let D be a set and $\mathcal{P}_D$ power set of D (the set containing all subsets of D). The operation Δ is to be regarded as an operation on $\mathcal{P}_D$.

1. Prove that there is an identity element with respect to the operation Δ, which is the empty set, i.e. $\emptyset$.

2. Prove every subset A of D has an inverse with respect to Δ, which is the set A itself. Thus, $(\mathcal{P}_D, \Delta)$ is a group!

3. Let D be the three-element set $D = \{a, b, c\}$. List the elements of $\mathcal{P}_D$. (For example, one element is $\{a\}$, another is $\{a, b\}$, and so on. Do not forget the empty set and the whole set D.) Then write the operation table for $(\mathcal{P}_D, \Delta)$.

Solution.

1. Noting that $A \setminus \emptyset = A$ and $\emptyset \setminus A = \emptyset$ and $A \cup \emptyset = A$ for any set A in $\mathcal{P}_D$, it's easy to verify that $A\Delta\emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A$ and $\emptyset\Delta A = A$ due to commutativity of set union operation.

2. By using the fact that $A \setminus A = \emptyset$ from expression $A\Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset \cup \emptyset = \emptyset$ we see that every subset A of D has an inverse A (every element of $\mathcal{P}_D$ is an inverse of itself regarding operation Δ).

3. Power set of D is $\mathcal{P}_D = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, D\}$. We can write the operation table as follows:

Δ	$\emptyset$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	D
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	D
$\{a\}$	$\{a\}$	$\emptyset$	$\{a,b\}$	$\{a,c\}$	$\{b\}$	$\{c\}$	D	$\{b,c\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\emptyset$	$\{b,c\}$	$\{a\}$	D	$\{c\}$	$\{a,c\}$
$\{c\}$	$\{c\}$	$\{a,c\}$	$\{b,c\}$	$\emptyset$	D	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	D	$\emptyset$	$\{b,c\}$	$\{a,c\}$	$\{c\}$
$\{a,c\}$	$\{a,c\}$	$\{c\}$	D	$\{a\}$	$\{b\}$	$\emptyset$	$\{a,b\}$	$\{b\}$
$\{b,c\}$	$\{b,c\}$	D	$\{c\}$	$\{b\}$	$\{a,c\}$	$\{a,b\}$	$\emptyset$	$\{a\}$
D	D	$\{b,c\}$	$\{a,c\}$	$\{a,b\}$	$\{c\}$	$\{b\}$	$\{a\}$	$\emptyset$

Theorem. Let $(S, *)$ be a commutative magma. If there exists a left or a right neutral element, then there exists a neutral element. Furthermore, if $(S, *)$ is a commutative magma with a neutral element and with a left or a right inverse, then every element has its inverse element.

Proof. Without loss of generality let us suppose that $(S, *)$ has a right neutral element e_r. Then for every $x \in S$ holds that $x * e_r = x$. Applying commutativity, we have $x * e_r = e_r * x = x$, therefore $e_r = e_l$ and $e_r = e_l = e$, i.e. there exist a unique neutral element e for every $x \in S$. Now, if x_r^{-1} is a right inverse, again without the loss of generality, we have $x * x_r^{-1} = e$. With commutativity, it's $x * x_r^{-1} = x_r^{-1} * x = e$, i.e. $x_r^{-1} = x_l^{-1} = x$, which means that for every $x \in S$ there exists an inverse element x^{-1}.

□

Problem. Let $\Phi = \{\bot, \top\} \cup \{F_1, F_2, \ldots\}$ be a set which contains all well-formed formulae F_i and logical constants $\top$ (true) and $\bot$ (false). Check what structure following operations define on Φ:

1. Conjunction $F \wedge G$, which is true when and only when both F and G are true.
2. Disjunction $F \vee G$, which is false when and only when both F and G are false.
3. Implication $F \to G$, which is false when and only when F is true and G false.
4. Biconditional $F \leftrightarrow G$, which is true when and only when F and G have equal truth values.

Solution. It's trivial to see that both association and commutativity is valid for conjunction, disjunction and biconditional. Therefore, for these operations, we shall only check for neutral and inverse elements.

1. *Conjunction.* Neutral element for conjunction is $\top$, as $F \wedge \top$ and $\top \wedge F$ produce F ($\top$ is always true, so all truth values are dependant on F being true or false; we could not consider $\bot$ as we would never get the case when both F and $\bot$

are true). However, there are no inverse elements, as any formula G we can try, cannot make $F \wedge G$ true when F is false; we cannot get every case to be true because of this. Ordered pair $(\Phi, \wedge)$ is a commutative monoid.

2. *Disjunction.* For disjunction, neutral element is $\bot$, as $F \vee \bot$ and $\bot \vee F$ produce F ($\bot$ is always false, so all truth values are dependant on F; we could not consider $\top$ as we would never get the case when both F and $\top$ are false). There are no inverse elements as F is always going to be true if F is true, and that is something we cannot undo with any formula to get $\bot$. Ordered pair $(\Phi, \vee)$ is a commutative monoid.

3. *Implication.* Associativity is not valid. For $F \to (G \to H)$ is false when and only when F is true and $G \to H$ is false, which is in turn false only when G is true and H is false. So, for this case is false when and only when F and G are true and H is false. But $(F \to G) \to H$ is false when and only when H is false, meaning that the falsness of this expression does not depend on F and G at all. Therefore it can be false when F, G and H are all false, which is not the case for the first expression. Operation is also not commutative as $F \to G$ is true when and only when F is true and G false and $G \to F$ false when and only when G is true and F is false. Neutral element does not exist. For the neutral element to be unique for all formulae, we need look for it only in constants $\bot$ and $\top$. It's not $\bot$ as $F \to \bot$ is false when and only when F is true, and that would yield $\neg F$, not F. It's not $\top$ either as $F \to \top$ would never be false, that is, it would be equivalent to $\top$. We need not check the reverse cases ($\top \to F$ or $\bot \to F$), as even the necessary conditions that $F \to E$ (where E is presumed neutral element) is equivalent to F is not satisfied. There are no inverses as there is no unique neutral element. Therefore, ordered pair $(\phi, \to)$ is a magma.

4. *Biconditional.* Neutral element for biconditional is actually $\top$, as $F \leftrightarrow \top$ is true when and only when F is true, meaning that expression would yield F. The operation is commutative, therefore, $\top$ is definitely a neutral element for this operation on ϕ. Inverse element is actually F itself as $F \leftrightarrow F$ is always true, for $F \leftrightarrow F$ is true, or $\top$, when and only when truth values of F and F are equal, and that is something that will always be, considering it's the same formula. Ordered pair $(\phi, \leftrightarrow)$ is an Abelian group.

Problem. Prove that if closure (from axioms of totality) does not hold, then so does not associativity.

Solution. Let S be a set, and $*$ an operation which does not satisfy the condition of closure on set S. That means that there exist $a, b \in S$ such that $a * b \notin S$. Now, if we try to prove associativity, $x * (y * z) = (x * y) * z$, it has to be valid for all elements

$x, y, z \in S$. But, as we can take $x = a$ and $y = b$, then $a * (b * z)$ may be defined (as $b * z$ might yield some element $c \in S$ and $a * c$ might also be in S), but $(a * b) * z$ is certainly not in S, as we cannot take an element that is not in S and perform an operation with some element z that is in S (as binary operation demands that both operands be from the same set).

Problem. Name the structure that the following operations define on set $\mathbb{N}$ (the set of natural numbers):

1. Addition.
2. Subtraction.
3. Multiplication.
4. Division.

Solution. It's trivial to notice that associativity and commutativity hold for addition and multiplication, and that associativity and commutativity do not hold for subtraction and division. So, let's observe only the inverse and neutral elements.

1. *Addition.* Neutral element for addition is such $e \in \mathbb{N}$ that $x + e = e + x = x$, that would be $e = 0$, but $0 \notin \mathbb{N}$, so there is no neutral element for addition in $\mathbb{N}$. There can be no inverses without a neutral element. Ordered pair $(\mathbb{N}, +)$ is a commutative semigroup.
2. *Subtraction.* Operation of subtraction does not satisfy closure because, e.g. $4 - 5 = -1 \notin \mathbb{N}$ and $4, 5 \in \mathbb{N}$. Associativity then also does not hold, following from the previous problem. Neutral element would be $e = 0$ for $x - 0 = x$, but $0 \notin \mathbb{N}$ and $0 - x = -x \neq x = x - 0$ (if $x \in \mathbb{N}$, then definitely $-x \notin \mathbb{N}$; here we are presuming that $-x$ is defined in $\mathbb{Z} \supset \mathbb{N}$ so we can talk about notion of opposite numbers, though outside of $\mathbb{N}$). There are no neutral elements and no inverses. Ordered pair $(\mathbb{N}, -)$ is not even a partial magma.
3. *Multiplication.* Neutral element for multiplication is $e = 1$ as $x \cdot 1 = 1 \cdot x = x$, and $1 \in \mathbb{N}$. However, there are no inverse elements for some $x \in \mathbb{N}$, e.g. there exist no $x \in \mathbb{N}$ such that $5 \cdot x = 1$ (obviously $5 \in \mathbb{N}$; presuming that the reader considers $\mathbb{Q}$ then, x would be $\frac{1}{5} \in \mathbb{Q}$, but not in $\mathbb{N}$). Ordered pair $(\mathbb{N}, \cdot)$ is a commutative monoid.
4. *Division.* Closure is not satisfied as, e.g. $5 : 3 \notin \mathbb{N}$ (it is in $\mathbb{Q}$, however). Therefore, we cannot consider associativity. Neutral element might be $1 \in \mathbb{N}$ for $x : 1 = x$, but $1 : x = \frac{1}{x}$ (which is in $\mathbb{Q}\backslash\{0\}$, but not in $\mathbb{N}$). Plus, division by zero is not even defined. There are no inverses, so, as with subtraction, ordered pair $(\mathbb{N}, :)$ is not even a partial magma.

Problem. Name the structure that the following operations define on set $\mathbb{Z}$ (the set of integers):

1. Addition.
2. Subtraction.
3. Multiplication.
4. Division.

Solution. We will grant associativity and commutativity for addition and multiplication in $\mathbb{Z}$, for it's a trivial thing. Also, it's obvious to see that subtraction and division are not associative nor commutative in $\mathbb{Z}$.

1. *Addition on* $\mathbb{Z}$. Associativity and commutativity holds, as stated above. Now, 0 is obviously a neutral element as $x + 0 = x$ for all $x \in \mathbb{Z}$. And for every $x \in \mathbb{Z}$ there is an inverse $-x \in \mathbb{Z}$, as $x + (-x) = 0$. $(\mathbb{Z}, +)$ is an Abelian group! Yay!
2. *Subtraction on* $\mathbb{Z}$. Closure holds this time, as $a - b$ is defined on $\mathbb{Z}$ for all $a, b \in \mathbb{Z}$. There are no neutral elements and therefore no inverses, as $x - 0 = x$ but $0 - x = -x$ (our only candidate for a neutral element). $(\mathbb{Z}, -)$ is a magma.
3. *Multiplication on* $\mathbb{Z}$. Neutral element exists, that is $e = 1$. Inverses do not, generally, exist, e.g. for $3 \cdot x = 1$ there is no such x that would satisfy this equation (it would be $\frac{1}{3} \in \mathbb{Q}$). $(\mathbb{Z}, \cdot)$ is a commutative monoid.
4. *Division on* $\mathbb{Z}$. Not even closure holds here and for 0 divisor it is not even defined. $(\mathbb{Z}, :)$ is not even a partial magma, again.

Problem. Name the structure that the following operations define on set $\mathbb{Q}$ (the set of rational numbers):

1. Addition.
2. Subtraction.
3. Multiplication.
4. Division.

Solution. As in previous problems, we will check only for neutral elements and inverses.

1. *Addition on* $\mathbb{Q}$. Neutral element is again $e = 0$ and inverses are $-x \in \mathbb{Q}$. $(\mathbb{Q}, +)$ is an Abelian group.

2. *Subtraction on* $\mathbb{Q}$. As in previous example, there is no neutral element, and no inverse elements, therefore $(\mathbb{Q}, -)$ is a magma.

3. *Multiplication on* $\mathbb{Q}$. Neutral element is $e = 1$, and inverse for every $x \neq 0$, $x \in \mathbb{Q}$ exists and that is $\frac{1}{x} \in \mathbb{Q}$. Alas! The zero has no inverse, therefore $(\mathbb{Q}, \cdot)$ is a commutative monoid. But! All is not lost, as we can remove the zero (or can we perhaps define some element ζ to satisfy $0 \cdot \zeta = 1$?) and get an ordered pair $(\mathbb{Q}\backslash\{0\}, \cdot)$ to be an Abelian group.

4. *Division on* $\mathbb{Q}$. Again, division by zero is not defined, but even if we took $\mathbb{Q}\backslash\{0\}$, could we find a neutral element or inverses? It would have to be $x : e = e : x = x$, the only possibility would be $e = 1$ as $x : 1 = x$, but $1 : x \neq x$. Therefore, $(\mathbb{Q}, :)$ is a partial magma, but $(\mathbb{Q}\backslash\{0\}, :)$ is a magma.

Problem. Does even one operation defined on the set of irrational numbers satisfy at least closure?

Solution. If we add two irrational numbers we can get a rational number. *Example.* Obviously $\sqrt{2}$ is a rational number, as is $(-\sqrt{2})$. Yet, $\sqrt{2}+(-\sqrt{2}) = 0$ which is a whole number. The same goes for subtraction. As for multiplication, $\sqrt{2} \cdot \sqrt{2} = 2$, which is a natural number. For division, $\sqrt{2} : \sqrt{2} = 1$, which is, again, a natural number. Therefore not even one of the four standard arithmetic operations satisfy the axioms of totality.

Problem. Name the structure that the following operations define on set $\mathbb{R}$ (the set of real numbers):

1. Addition.

2. Subtraction.

3. Multiplication.

4. Division.

Solution.

1. *Addition on* $\mathbb{R}$. Neutral element is $e = 0$ and inverse is $-x$, both of which are in $\mathbb{R}$. Ordered pair $(\mathbb{R}, +)$ is an Abelian group.

2. *Subtraction on* $\mathbb{R}$. As with a previous example, there are no neutral elements and no inverses. Axioms of totality are satisfied, however. Ordered pair $(\mathbb{R}, -)$ is a magma.

3. *Multiplication on* $\mathbb{R}$. Neutral element is $e = 1$, but as in a previous example, there is no inverse for $0 \in \mathbb{R}$, therefore $(\mathbb{R}, \cdot)$ is a commutative monoid and $(\mathbb{R}\backslash\{0\}, \cdot)$ is an Abelian group.

4. *Division on* $\mathbb{R}$. There are no neutral elements, again, as in $\mathbb{Q}$, and no inverses. Division by zero is not defined so $(\mathbb{R}, :)$ is a partial magma, but $(\mathbb{R}\backslash\{0\}, :)$ is a magma.

Problem. Let $\alpha = \{0, 1\}$ be an alphabet and α_n a set of all words of length $n \geq 1$, derived by combining elements of α. Name the structure that following operations define on α_n:

1. (Bitwise) AND.

2. (Bitwise) OR.

3. (Bitwise) XOR.

4. (Bitwise) NOR (Sheffer stroke).

5. (Bitwise) NAND (Pierce arrow).

Solution. Before we begin, we will add a following table which will help us to solve all the problems above. For every $A, B \in \alpha$ we can define all the possibilities as follows:

A	B	$A \wedge_B B$	$A \vee_B B$	$A \underline{\vee}_B B$	$A \uparrow_B B$	$A \downarrow_B B$
1	1	1	1	0	0	0
1	0	0	1	1	1	0
0	1	0	1	1	1	0
0	0	0	0	0	1	1

Now, these operations can be observed if we look upon A and B as ordered n-tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ and then define $A \circ_B B$, where $\circ_B \in \{\wedge_B, \vee_B, \underline{\vee}_B, \uparrow_B, \downarrow_B\}$ as $(a_1 \circ b_1, \ldots, a_n \circ b_n)$. Then, e.g. if $A = 1001$ and $B = 1010$, then $A \wedge_B B = 1001 \wedge_B 1010 = 1000$. See that every new "digit" corresponds to the conjuction of corresponding "digits" of A and B. Obviously, this time, axioms of totality are satisfied as we are always bound to get a word and that word will be of length equal to n.

1. *Bitwise AND.* Associativity and commutativity hold because conjuction is associative and commutative. Reader can easily verify that claim. Neutral element is a word which contains only digit 1. Now we need $A^{-1} \in \alpha_n$ such that $(a_0 \wedge a^{-1}, \ldots, a_n \wedge a_n^{-1}) = (1, 1 \ldots, 1)$. Obviously the inverse does not exist if some $a_i = 0$. Through conjuction digit 1 cannot be obtained. Ordered pair $(\alpha_n, \wedge_B)$ is a commutative monoid.

2. *Bitwise OR.* Same thing as with AND, except that the neutral element is a word containing only zero digits. There is no inverse also, as if there is a 1 in a word, we never get a zero by disjunction. Ordered pair $(\alpha_n, \vee_B)$ is a commutative monoid.

3. *Bitwise XOR.* Operation is associative and commutative (actually every operation of this kind that has same value for different propositional values). Now, there is no neutral element and there are no inverses, so ordered pair $(\alpha_n, \veebar_B)$ is a commutative semigroup.

4. *Bitwise NOR (Sheffer stroke).* Operation is commutative and associative and there is a neutral element, that is a word containing all zeros. There are no inverses as we can never obtain zero if there is a zero in the word itself. Therefore, $(\alpha_n, \uparrow_B)$ is a commutative monoid.

5. *Bitwise NAND (Pierce arrow).* Same thing as with Sheffer stroke, except the neutral element is the word containing all digits 1. There are no inverses, as we can never get one when there is one in the word. Therefore $(\alpha_n, \veebar_B)$ is a commutative monoid.

Theorem. If $(G, \cdot)$ is a group and a, b and c are elements of G, then:

(i) $ab = ac$ implies $b = c$ and

(ii) $ba = ca$ implies $b = c$.

Proof. (i) Let us suppose that $ab = ac$. By multiplying that expression with a^{-1} (as $(G, \cdot)$ is a group there exists a^{-1} for every $a \in G$) on the left we have $a^{-1}(ab) = a^{-1}(ac)$. Now, as associativity also holds, we can rearrange the elements in expression so that $(a^{-1}a)b = (a^{-1}a)c$. As $a^{-1}a = e$, we have $eb = ec$. Now, as $ex = x$ for every $x \in G$, we finally have $b = c$. (ii) Proof is analogous to the (i) with exception of multiplying with a^{-1} on the right.

□

Theorem. If $(G, \cdot)$ is a group and a, b are elements of G, then $ab = e$ implies $a = b^{-1}$ and $b = a^{-1}$.

Proof. Let's multiply first expression by b^{-1} (as $(G, \cdot)$ is a group there is an inverse for each element in G and so for b) on the right. We get $(ab)b^{-1} = eb^{-1}$. Applying associativity, we have $a(bb^{-1}) = eb^{-1}$ and by using properties of neutral element e, finally, we have $ae = b^{-1}$, i.e. $a = b^{-1}$. For the second part, we only have to multiply first expression with a^{-1} on the left and we will obtain, following the same line of reasoning, $b = a^{-1}$.

□

Theorem. If $(G, \cdot)$ is a group and a, b are elements of G, then

(i) $(ab)^{-1} = b^{-1}a^{-1}$;

(ii) $(a^{-1})^{-1} = a$.

Proof. Ad (i). It is certainly true that $(ab)^{-1}(ab) = e$, as there is a neutral element for every element (and we can imagine ab being one element as the operation must yield a unique element if it's a group). Now, we multiply that expression by b^{-1} on the right and get $\left((ab)^{-1}(ab)\right)b^{-1} = eb^{-1}$. Using associativity we have $(ab)^{-1}((ab)\,b^{-1}) = eb^{-1}$ and by using properties of e and again associativity, we obtain $(ab)^{-1}(a\,(bb^{-1})) = b^{-1}$. Now we use $bb^{-1} = e$ so it is $(ab)^{-1}(ae) = b^{-1}$, and ae being a, we have $(ab)^{-1}a = b^{-1}$. By multiplying by a^{-1} on the right, we have $\left((ab)^{-1}a\right)a^{-1} = b^{-1}a^{-1}$. By using associativity, we have $(ab)^{-1}(aa^{-1}) = b^{-1}a^{-1}$. Now, as $aa^{-1} = e$ we finally obtain $(ab)^{-1}e = b^{-1}a^{-1}$, i.e. $(ab)^{-1} = b^{-1}a^{-1}$. Ad (ii). As $(G, \cdot)$ is a group, every element has its inverse and so does a^{-1} which would be $(a^{-1})^{-1}$. Now, it's $a^{-1}(a^{-1})^{-1} = e$. By multiplying the expression with a on the left, we have $a\left(a^{-1}(a^{-1})^{-1}\right) = ae$. We use properties of e, that is $ae = a$, and associativity to obtain $(aa^{-1})(a^{-1})^{-1} = a$. Finally, as $aa^{-1} = e$ we have $e(a^{-1})^{-1} = a$, that is, $(a^{-1})^{-1} = a$. That would say, the inverse of the inverse of the original is the original.

□

Remark. (i) In last three theorems we were very rigorous when explicitly stating what is group and what is a set. But from now on, due to simplicity, we shall denote by G both the group and the set G on which it is defined (if it is unambiguous). (ii) Notice that associativity actually tells us that parentheses are redundant. So, we don't need that kind of rigorous treatment of associativity, if it holds (and in a group, monoid and semigroup it certainly will). If we define $abc = a(bc)$, then we get that $(ab)c = a(bc) = abc$. By mathematical induction we can prove it for arbitrarily many elements (in the following lemma).

Proposition. Let S be a set on which we define binary operation $\cdot : S \times S \to S$ satisfying axioms of totality and at least property of associativity. Parentheses are redundant.

Proof. We have already shown, for $n = 3$ (which will be the basis of our induction), that, as $a(bc) = (ab)c$, and because there are no more distributions of parentheses, we can write $a(bc) = (ab)c = abc$. If we assume the claim is valid for all $k < n$, that is, all

distributions of parentheses are equal and can be uniquely designated by $a_1a_2\cdots a_{n-1}$, then we can show that it will also be valid for $a_1a_2\cdots a_{n-1}a_n$. First, note that the former expression can be broken into two subproducts so that $(a_1\cdots a_i)\,(a_{i+1}\cdots a_n)$. This can be done, as if it were not the case, in distribution of the parentheses, we would never be allowed to place the parentheses in between to members, changing nothing (i.e. $(a_1\cdots a_n) = a_1\cdot a_n$). Then, as $(i-1)+1 = i < n$ and $n-(i+1)+1 = n-i < n$ (we can never have $i = 0$, as such index does not exist), then by assumption of induction, both those subproduct can be written without parentheses. When moving i from 1 to n, we exhaust all possibilities.

□

Theorem (Catalan's problem). The number of ways in which we can associate a sequence of n factors is equal to Catalan's number, that is,

$$C_n = \sum_{i=1}^{n-1} C_i C_{n-i} = \frac{1}{n}\binom{2(n-1)}{(n-1)},$$

for $n > 2$, $n \in \mathbb{N}$, and $C_1 = C_2 = 1$.

Proof. As for $n = 1$ we have only one element and for $n = 2$ only two elements, we can say that, in both cases we have only one choice to associate them, (a_1) and (a_1a_2), where the parentheses are actually even sintacticaly redundant. So we can set $C_1 = C_2 = 1$. Now, for $n = 3$, we can see that we have two cases, that is $C_3 = 2$, because we only have $(a_1a_2)a_3$ and $a_1(a_2a_3)$. For $n = 4$, we have $((a_1a_2)a_3)\,a_4$, $(a_1(a_2a_3))\,a_4$, $a_1\,((a_2a_3)a_4)$, $a_1\,(a_2(a_3a_4))$ and $(a_1a_2)(a_3a_4)$, that is $C_4 = 5$. Now, we can see the line of reasoning we are going to follow. Let us analyze all the possibilities we can have for $n = 4$, than we will generelize it for any $n \in \mathbb{N}$ $(n > 2)$. First case is when we had $(a_1)(a_2a_3a_4)$. Here, a_1 can be associated in one way $(C_1 = 1)$ and $a_2a_3a_4$ in two ways $(C_3 = 2)$, that is, $C_1 \cdot C_3 = 1 \cdot 2 = 2$ ways altogether. Now, we move the parentheses to the right until we reach the end. Now, we have $(a_1a_2)(a_3a_4)$. Both of these parentheses we can associate in only one way as $C_2 = 1$, so we have only one way altogether as $C_2 \cdot C_2 = 1 \cdot 1 = 1$. Finally, we have $(a_1a_2a_3)(a_4)$. There are two ways to associate the factors inside the former parentheses and only one way to associate the latter parentheses, that is $C_3\cdot C_1 = 2\cdot 1 = 2$. That is $C_4 = C_3C_1+C_2C_2+C_1C_3 = 2+1+2 = 5$. Notice the movement of the indices and notice the useful fact that their sum equals 4 in every summand. In fact, for n the sum of indeces will move from 1 to $n-1$ in both directions and their sum will always be n. Let's try and justify this fact further. Let's observe the expression of the form $a_1a_2a_3\cdots a_n$. Now, we will start associating, as in $n = 4$, with $(a_1)(a_2a_3\cdots a_n)$ and move the right parentheses enclosing a_1 and left parentheses enclosing $a_2\cdots a_n$ to the right, one by one step. We can do that for

$n-1$ steps. In that way we form a meaningful sequence (top row) with number of associations for the case above (bottom row):

$(a_1)(a_2\cdots a_n)$	$(a_1a_2)(a_3\cdots a_n)$	$\ldots$	$(a_1\cdots a_{n-2})(a_{n-1}a_n)$	$(a_1\cdots a_{n-1})(a_n)$
$C_1\cdot C_{n-1}$	$C_2\cdot C_{n-2}$	$\ldots$	$C_{n-2}\cdot C_2$	$C_{n-1}\cdot C_1$

This way, summing all the cases, we have justified that $C_n=\sum_{i=1}^{n-1}C_iC_{n-i}$ for $n>2$.

Now we want to show that $C_n=\frac{1}{n}\binom{2(n-1)}{(n-1)}$. First, we shall use the generating function defined as

$$C(x)=C_1+C_2x+C_3x^2+\ldots+C_nx^{n-1}+C_{n+1}x^n+\ldots$$

to get the recursive formula for C_n. One can easily check that

$$\begin{aligned}C^2(x) &= \left(C_1+C_2x+C_3x^2+\ldots\right)^2\\ &= \left(C_1+C_2x+C_3x^2+C_4x^3+\ldots\right)\left(C_1+C_2x+C_3x^2+C_4x^3+\ldots\right)\end{aligned}$$

gives us the recursion we need. For, if we multiply all the summands necessary to get C_n, then we need to have x^ix^j such that $i+j=n-1$. As indices follow the exponents, differing only by 1, we will have the sum of all the combinations of C_iC_j whose indices together add to $n+1$ (that is $(n-1)+2$ as each C_i differs from the corresponding exponent by 1; adding two indices, the difference becomes 2). By multiplying first few members, we get the general idea:

$$\begin{aligned}C^2(x) &= C_1C_1+x\left(C_2C_1+C_1C_2\right)+x^2\left(C_1C_3+C_2C_2+C_3C_1\right)+\ldots\\ &+ x^{n-2}\left(\sum_{i=1}^{n-1}C_iC_{n-i}\right)+\ldots\end{aligned}$$

Now, by using the recursive formula, we see that where in $C(x)$ we have C_nx^{n-1} there we in $C^2(x)$ have C_nx^{n-2}. Therefore, we will multiply $C^2(x)$ by x to get coefficients right; now we have:

$$\begin{aligned}xC^2(x) &= xC_1C_1+x^2\left(C_2C_1+C_1C_2\right)+x^3\left(C_1C_3+C_2C_2+C_3C_1\right)+\ldots\\ &+ x^{n-1}\left(\sum_{i=1}^{n-1}C_iC_{n-i}\right)+\ldots\end{aligned}$$

Further progress is made if we subtract $xC^2(x)$ from $C(x)$. Every summand disappears,

leaving only C_1, that is 1 (notice that $C_1 = C_2 = 1$ so $xC_2 - xC_1C_1 = x - x = 0$). So we have $C(x) - xC^2(x) = 1$. That is the quadratic equation, $xC^2(x) - C(x) + 1 = 0$ which we are going to solve for $C(x)$. We use the standard formula:

$$C(x) = \frac{-1 \pm \sqrt{1-4x}}{2x}.$$

All we have to do now is to decide whether to use positive or a negative side in front of square root. That we can easily verify by calculating $C(0)$. Now, we cannot have zero in the denominator so we have to do a little trick. We will substitute $C(x)$ for the formula above:

$$\frac{-1 \pm \sqrt{1-4x}}{2x} = C_1 + C_2x + C_3x^2 + \ldots + C_nx^{n-1} + \ldots$$

We multiply the whole expression by $2x$, we transfer the -1 to the right-hand side and we have:

$$\pm\sqrt{1-4x} = -1 + 2C_1x + 2C_2x^2 + 2C_3x^3 + \ldots + 2C_nx^n + \ldots$$

Now if we take $x = 0$ (keeping in mind it's actually a limit), on the left only ± 1 remains and on the right only -1. For the two sides of equation to be equal we have to take the negative sign, that is, the generating function for our recursion is

$$C(x) = \frac{-1 - \sqrt{1-4x}}{2x},$$

and by the same logic, we have

$$-\sqrt{1-4x} = -1 + 2C_1x + 2C_2x^2 + 2C_3x^3 + \ldots + 2C_nx^n + \ldots$$

By using a generalized form of binomial formula, we have

$$(1-4x)^{\frac{1}{2}} = \sum_{n=0}^{\infty} (-4)^n \binom{\frac{1}{2}}{n} x^n.$$

By equating the latter formula with the former one, we easily see that

$$-(-4)^n \binom{\frac{1}{2}}{n} = 2C_n.$$

Now we use the formula

$$\binom{n}{k} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}.$$

Using that, we now have:

$$-(-4)^n \frac{\prod_{i=0}^{n-1}\left(\frac{1}{2}-i\right)}{n!} = 2C_n.$$

Dividing everything by 2 and setting $(-4)^n = (-2)^n 2^n$ we get:

$$C_n = -(-2)^n 2^n \frac{\prod_{i=0}^{n-1}\left(\frac{1}{2}-i\right)}{2n!}.$$

To further simplify the expression, we will use the fact that $a^n = \prod_{i=0}^{n-1} a$, for some $a \in \mathbb{R}$, which gets us to expression

$$C_n = -2^n \left(\prod_{i=0}^{n-1}(-2)\right)\left(\frac{\prod_{i=0}^{n-1}\left(\frac{1}{2}-i\right)}{2n!}\right).$$

We have the same number of factors in both products so we can distribute them as $(-2)\left(\frac{1}{2}-i\right)$ to obtain

$$C_n = -\frac{2^n \prod_{i=0}^{n-1}(2i-1)}{2n!}.$$

Notice that for $i = 0$ we will have (-1) in the product. We can extract that member to make the negative sign disappear, leaving the expression explicitly positive:

$$C_n = \frac{2^n \prod_{i=1}^{n-1}(2i-1)}{2n!}.$$

We can also further simplify $\frac{2^n}{2}$ as 2^{n-1}. Also, notice that the product actually gives the sequence $1 \cdot 3 \cdot 5 \cdots (2n-5)(2n-3)$. If we multiplied that product with even factors such as $2 \cdot 4 \cdot 6 \cdots (2n-2) = \prod_{i=1}^{n-1} 2i$, that would nicely equal $(2(n-1))!$. So we do it this way:

$$C_n = \frac{2^{n-1}\prod_{i=1}^{n-1}(2i-1)}{n!} \cdot \frac{\prod_{i=1}^{n-1} 2i}{\prod_{i=1}^{n-1} 2i} = \frac{2^{n-1}\prod_{i=1}^{n-1}((2i-1)\,2i)}{n!\prod_{i=1}^{n-1} 2i}.$$

It's obvious to notice that $\prod_{i=1}^{n-1}((2i-1)(2i)) = (2(n-1))!$. Furthermore, we can see that $\prod_{i=1}^{n-1} 2i = 2^{n-1}\prod_{i=1}^{n-1} i = 2^{n-1}(n-1)!$. Now we have

$$C_n = \frac{2^{n-1}\,(2(n-1))!}{2^{n-1}n(n-1)!(n-1)!} = \frac{(2(n-1))!}{n\,(2(n-1)-(n-1))!\,(n-1)!}.$$

Finally, by using $\binom{n}{k} = \frac{n!}{(n-k)!k!}$, we have the general formula:

$$C_n = \frac{1}{n}\binom{2(n-1)}{n-1},$$

for any $n > 2$ and $n \in \mathbb{N}$. That is the solution to the Catalan's problem and C_n are called Catalan's numbers. Notice that, in some other literatures, indices might slightly differ, as we took (for good reasons) the starting number as C_1, where it's usually taken as C_0 and then it's $C_n = \frac{1}{n+1}\binom{2n}{n}$, for $n > 1$, $n \in \mathbb{N}$ and $C_0 = C_1 = 1$.

□

Theorem. Let S be a non-commutative semigroup. The number of different ways in which the expression $a_1a_2\cdots a_n$, where $a_1, \ldots, a_n \in S$, can be evaluated is $(n-1)!$.

Proof. If $n = 2$, the number of ways in which it can be calculated is only one as we only have a_1a_2. Let us suppose that $a_1\cdots a_n$ can be calculated in $(n-1)!$ ways. We need to prove that $a_1\cdots a_na_{n+1}$ can be calculated in $n!$ different ways. Now, from $n+1$ factors, we can choose consecutive pairs in n ways. Without loss of generality, we can suppose we chose a_na_{n+1} which yields some element b. Now, we have $a_1\cdots a_{n-1}b$, an expression with n factors which can be calculated in $(n-1)!$ ways. That is $n(n-1)! = n!$ different ways for $n+1$ factors.

□

Theorem. Let G be a group and $a_1, \ldots, a_n \in G$. Then:

$$(a_1a_2\cdots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_1^{-1}.$$

Proof. For $n = 1$ we have $a_1^{-1} = a_1^{-1}$. For $n = 2$ we have $(a_1a_2)^{-1} = a_2^{-1}a_1^{-1}$. That we can prove by the fact that $(a_1a_2)^{-1}(a_1a_2) = e$. Then, by multiplying the expression on the right-hand side with a_2^{-1} and a_1^{-1}, succesively, we get the much desired expression. Let's assume that it's true that $(a_1\cdots)^{-1} = a_n^{-1}\cdots a_1^{-1}$ for some $n \in \mathbb{N}$. Now, let's prove that $(a_1\cdots a_{n+1})^{-1} = a_{n+1}^{-1}\cdots a_1^{-1}$ is also true. We can use the fact that $a_n^{-1}\cdots a_1^{-1} = (a_1\cdots a_n)^{-1}$. Then we have $a_{n+1}^{-1}\cdots a_1^{-1} = a_{n+1}^{-1}(a_1\cdots a_n)^{-1}$. We can consider $a_1\cdots a_n$ as a single element, let's say b. Now, $a_{n+1}^{-1}b^{-1} = a_{n+1}^{-1}\cdots a_1^{-1}$. From case when $n = 2$, we can write the expression as $(ba_{n+1})^{-1} = a_{n+1}^{-1}\cdots a_1^{-1}$. Returning substitution for b, we have $(a_1\cdots a_{n+1})^{-1} = a_{n+1}^{-1}\cdots a_1^{-1}$.

□

Remark. The former theorem can be more neatly expressed as:

$$\left(\prod_{i=1}^{n} a_i\right)^{-1} = \prod_{i=1}^{n} a_{n-(i-1)}^{-1}.$$

Problem. Let a, b, c and x be elements of a group G. Solve for x in terms of a, b and c following equations:

1. $x^2 = b$ and $x^5 = e$;
2. $axb = c$;
3. $x^2b = xa^{-1}c$;
4. $x^2a = bxc^{-1}$ and $acx = xac$;
5. $ax^2 = b$ and $x^3 = e$;
6. $x^2 = a^2$ and $x^5 = e$;
7. $(xax)^3 = bx$ and $x^2 = (xa)^{-1}$;

Solution.

1. $x^2 = b$ and $x^5 = e$. We can write x^5 as x^2x^2x, then the latter expression becomes $x^2x^2x = e$. Substituting x^2 for b, we have $bbx = e$, that is $b^2x = e$. Now, multiplying by $(b^2)^{-1}$ on the left, we have $(b^2)^{-1}b^2x = (b^2)^{-1}$, i.e. $x = (b^2)^{-1}$.
2. $axb = c$. Multiplying by a^{-1} on the left and by b^{-1} on the right. That way, it's $a^{-1}axbb^{-1} = a^{-1}cb^{-1}$, i.e. $x = a^{-1}cb^{-1}$.
3. $x^2b = xa^{-1}c$. After writing equation as $xxb = xa^{-1}c$, we shall multiply the expression by x^{-1} on the left and by b^{-1} on the right. Now, it's $x^{-1}xxbb^{-1} = x^{-1}xa^{-1}cb^{-1}$ which implies, after using $x^{-1}x = e$ and $bb^{-1} = e$, that $x = a^{-1}cb^{-1}$.
4. $x^2a = bxc^{-1}$ and $acx = xac$. By multiplying the second equation with x on the left, we have $xacx = x^2ac$. If we substitute x^2a from the first equation, we have $xacx = bxc^{-1}c$, i.e. $xacx = bx$. Multiplying this equality with x^{-1} on the right, we have $xacxx^{-1} = bxx^{-1}$, that is, $xac = b$. Now, we multiply this equality with c^{-1} and then with a^{-1} on the right, and we have $xacc^{-1}a^{-1} = bc^{-1}a^{-1}$, that is, using successive properties of the neutral element, $xaa^{-1} = bc^{-1}a^{-1}$ and finally $x = bc^{-1}a^{-1}$.

5. $ax^2 = b$ and $x^3 = e$. If we simply multiply former equality with x on the right, we have $ax^3 = bx$. Using $x^3 = e$, we have $a = bx$. Multiplying by b^{-1} on the left, the solution is $x = b^{-1}a$.

6. $x^2 = a^2$ and $x^5 = e$. We can write the latter equality as $x^2x^2x = e$. Substituting $x^2 = a^2$ we have $a^2a^2x = e$, i.e. $a^4x = e$. We multiply this with $(a^4)^{-1}$ on the left and get $(a^4)^{-1}a^4x = (a^4)^{-1}$, that is $x = (a^{-1})^4$ (notice that, from previous theorem, we have $(a^n)^{-1} = (a^{-1})^n$; actually, using this fact, we could allow ourselves to write this as a^{-n} without any ambiguity).

7. $(xax)^3 = bx$ and $x^2 = (xa)^{-1}$. Let's write the former equation in a different way, that is, as $(xax)(xax)(xax) = bx$, that is $xax^2ax^2ax = bx$. Substituting x^2 from the second equation, we have $xa\,(xa)^{-1}\,a\,(xa)^{-1}\,ax = bx$. Now it's $aa^{-1}x^{-1}ax = bx$, i.e. $x^{-1}ax = bx$. If we multiply that equality with x on the left and x^{-1} on the right, we obtain $a = xb$, that is, by multiplying with b^{-1} on the right, $x = ab^{-1}$.

Problem. Prove or disprove that following arguments hold for any group[4]. If the argument generally does not hold, find an example of a group (or an Abelian group) where it would hold.

1. If $x^2 = e$ then $x = e$.

2. If $x^2 = a^2$ then $x = a$.

3. $(ab)^2 = a^2b^2$.

4. If $x^2 = x$ then $x = e$.

5. Let G be a group. Then, for all $x \in G$ there exists $y \in G$ such that $x = y^2$.

6. Let G be a group. Then, for all $x, y \in G$ there exists $z \in G$ such that $y = xz$.

Solution.

1. It's true in $\mathbb{R}\backslash\{0\}$ (considering $x = -1$ and $e = 1$) that $(-1)^2 = 1$, but $-1 \neq 1$ (i.e. $x \neq e$). Therefore, this argument does not generally hold. From $x^2 = e$, we can say that $x = x^{-1}$ (by multiplying the equation with x^{-1} from either left or right) and from that that $x^{-1} = e$ (by substituting x^{-1} for x). However, considering an Abelian group $(\mathbb{Z}, +)$ and taking $e = 0$ (which is a neutral element for addition), we would have $x + x = 0$ and from that $x = -x$ which is true only for $x = 0$. So, in this case this argument is valid.

[4]For now, consider that $(\mathbb{R}\backslash\{0\}, \cdot)$ is an Abelian group; if something does not hold for an Abelian group then it will hold nor for a group, nor for a semigroup, nor for a monoid, nor for a magma. Take any necessary counterexamples from this Abelian group.

2. It's true in $\mathbb{R}\backslash\{0\}$ (considering $x = -1$ and $a = 1$) that $(-1)^2 = 1^2$, but $-1 \neq 1$. Therefore, this argument does not generally hold. But, in Abelian group $(\mathbb{Z}, +)$, taking $a = 1$, we have $x + x = a + a$, that is $x + x = 2$, and the only option being $x = 1$. So here, it follows that $x = a$ from $x^2 = a^2$.

3. I say that if G is a group that is not commutative then it is not true that $(ab)^2 = a^2b^2$ for all $a, b \in G$. We will prove this by contradiction. Let's assume that G is a non-commutative group (it's not true that for all $a, b \in G$ holds $ab = ba$, i.e. there exist some $x, y \in G$ such that $xy \neq yx$) and that it's true that $(ab)^2 = a^2b^2$ for all $a, b \in G$. Now, we write this expression down as $abab = aabb$. We multiply it by b^{-1} on the right and by a^{-1} on the left, only to obtain $ba = ab$. Now, as operation is not generally commutative, e.g. for those $x, y \in G$, we have a contradiction, therefore affirming our first argument, that in a non-commutative group it is not necessarily true that $(ab)^2 = a^2b^2$. However, the argument would be valid if group G were commutative. Then, $(ab)^2 = abab = aabb = a^2b^2$.

4. Assume that $x^2 = x$, i.e. $xx = x$. Then, by multiplying it on the right (we could also multiply it on the left and get the same result) by x^{-1} we get $xxx^{-1} = xx^{-1}$, that is $x = e$.

5. Let's consider again $\mathbb{R}\backslash\{0\}$ with multiplication. Obviously, $-1 \in \mathbb{R}\backslash\{0\}$, but there does not exist $y \in \mathbb{R}\backslash\{0\}$ such that $-2 = y^2$ (y^2 is necessarily non-negative, and -2 is negative). Therefore this argument is not generally true.

6. Let G be a group and $x, y \in G$. As G is a group there exists inverse of x, $x^{-1} \in G$ (it also holds that $x^{-1}x = xx^{-1} = e$). Now, if we take $x^{-1}y$, as x^{-1} is in G, and y is by assumption in G, and axioms of totality being satisfied (otherwise it wouldn't be a group), $x^{-1}y$ must yield a unique element in G which we can designate by z. That way, $x^{-1}y = z$. Multiplying on the left by x, we have $xx^{-1}y = xz$, that is $ey = xz$ and finally $y = xz$. Thus we have proved this argument.

Problem. If $a, b \in G$ and G is an Abelian[5] group, prove the following:

1. $a^{-1}b^{-1} = b^{-1}a^{-1}$;

2. $ab^{-1} = b^{-1}a$;

3. $a(ab) = (ab)a$;

4. $a^2b^2 = b^2a^2$;

5. $(xax^{-1})(xbx^{-1}) = (xbx^{-1})(xax^{-1})$ for any $x \in G$;

[5]In Abelian groups, commutativity necessarily holds, i.e. for any $a, b \in G$ it's true that $ab = ba$. Use this fact to your own advantage.

6. $ab = ba$ if and only if $aba^{-1} = b$;

7. $ab = ba$ if and only if $aba^{-1}b^{-1} = e$.

Solution.

1. $a^{-1}b^{-1} = b^{-1}a^{-1}$. As G is commutative, $ab = ba$. Multiplying by a^{-1} on the left, we have $a^{-1}ab = a^{-1}ba$, i.e. $b = a^{-1}ba$. Now, we multiply it again by a^{-1}, but on the right and obtain $ba^{-1} = a^{-1}baa^{-1}$, that is, $ba^{-1} = a^{-1}b$. We do the same thing with b^{-1}. We multiply the last equality with b^{-1} on the left and then on the right to get $a^{-1}b^{-1} = b^{-1}a^{-1}$.

2. $ab^{-1} = b^{-1}a$. We start off with $ab = ba$. We multiply this equality by b^{-1} on the right and get $abb^{-1} = bab^{-1}$. Now, it's $a = bab^{-1}$. We shall multiply that expression with b^{-1} on the left and we have $b^{-1}a = b^{-1}bab^{-1}$, i.e. $b^{-1}a = ab^{-1}$, or $ab^{-1} = b^{-1}a$, which is really the same as the former expression.

3. $a(ab) = (ab)a$. Again, we use $ab = ba$. Minding associativity more carefully here, we multiply it on the left with a to get $a(ab) = a(ba)$. Now, using associativity, i.e. the fact that $a(ba) = (ab)a$, we get $a(ab) = (ab)a$.

4. $a^2b^2 = b^2a^2$. Consider multiplying $ab = ba$ with b on the right to get $ab^2 = bab$, and now multiplying with a on the left, we have $a^2b^2 = abab$. As G is associative we can more explicitly group elements on the right-hand side so that $a^2b^2 = a(ba)b$. We've done this only to emphasise what we are going to do next; we are going to use commutativity on the expression in the parentheses and get $a^2b^2 = a(ab)b$. Removing parentheses by applying associativity, we have $a^2b^2 = a^2b^2$.

5. $(xax^{-1})(xbx^{-1}) = (xbx^{-1})(xax^{-1})$ for any $x \in G$. Again, we start with $ab = ba$. Wherever we put neutral element e (which exists as G is an Abelian group), the expression is not changed. We can put it between the first two factors and get $aeb = ba$. We can put it again between the second two factors and now have $aeb = bea$. As G is an Abelian group, satisfying the condition of the existence of inverse elements, it is true for any $x \in G$ that $xx^{-1} = x^{-1}x = e$. So, we put these expressions into our former equality so that $ax^{-1}xb = bx^{-1}xa$. Now, we multiply it with x on the left and x^{-1} on the right and get $xax^{-1}xbx^{-1} = xbx^{-1}xax^{-1}$, and when we group those elements, using associativity, we have $(xax^{-1})(xbx^{-1}) = (xbx^{-1})(xax^{-1})$.

6. $ab = ba$ if and only if $aba^{-1} = b$. First, we will prove: if $ab = ba$, then $aba^{-1} = b$. Assume that $ab = ba$, multiply it with a^{-1} on the right and it's $aba^{-1} = baa^{-1}$, that is, $aba^{-1} = b$. Now we prove: if $aba^{-1} = b$ then $ab = ba$. By multiplying $aba^{-1} = b$ on the right with a, we get $aba^{-1}a = ba$, i.e. $ab = ba$.

7. $ab = ba$ if and only if $aba^{-1}b^{-1} = e$. First, let's prove: if $ab = ba$ then $aba^{-1}b^{-1} = e$. We multiply $ab = ba$ by a^{-1} on the right and get $aba^{-1} = baa^{-1}$, i.e. $aba^{-1} = b$. Now, we multiply this with b^{-1} on the right and get $aba^{-1}b^{-1} = bb^{-1}$, that is, $aba^{-1}b^{-1} = e$. Now, let's prove: if $aba^{-1}b^{-1} = e$ then $ab = ba$. Assume that $aba^{-1}b^{-1} = e$ and multiply it on the right with b. We get $aba^{-1}b^{-1}b = eb$, which is $aba^{-1} = b$. Now, multiply it on the right by a to obtain $aba^{-1}a = ba$, i.e. $ab = ba$.

Problem. Let G be a group. Let a, b, c denote elements of G, and let e be the neutral element of G. Prove:

1. If $ab = e$, then $ba = e$;
2. If $abc = e$, then $cab = e$ and $bca = e$;
3. If $xay = a^{-1}$, then $yax = a^{-1}$;
4. Let a, b and c each be equal to its own inverse. If $ab = c$, then $bc = a$ and $ca = b$.
5. $a = a^{-1}$ if and only if $aa = e$.
6. If abc is its own inverse, then bca is its own inverse, and cab is its own inverse.
7. Let a and b each be equal to its own inverse. Then ba is the inverse of ab.
8. Let $c = c^{-1}$. Then $ab = c$ if and only if $abc = e$.

Solution.

1. If $ab = e$, then $ba = e$. Assume that $ab = e$. Then, we multiply that expression by a^{-1} on the left and get $b = a^{-1}$. Now, we multiply this expression with a on the right and we have $ba = e$.
2. If $abc = e$, then $cab = e$ and $bca = e$. Suppose $abc = e$. We multiply this expression by a^{-1} on the right and get $a^{-1}abc = a^{-1}$, i.e. $bc = a^{-1}$. Now we multiply this by a on the right and get $bca = a^{-1}a$, which is $bca = e$. In the same spirit, multiplying this expression on the left by b^{-1}, and then by b on the right, we get $cab = e$. We will later formally prove the generalization of this and previous property.
3. If $xay = a^{-1}$, then $yax = a^{-1}$. Assume that $xay = a^{-1}$. We multiply it with y^{-1} on the right and get $xa = a^{-1}y^{-1}$; then, we multiply it by a^{-1} on the right and then it's $x = a^{-1}y^{-1}a^{-1}$. If we multiply it by a on the left, we will then have $ax = y^{-1}a^{-1}$. Finally, multiplying this expression by y on the left gets us $yax = a^{-1}$.

4. $a = a^{-1}$ if and only if $aa = e$. Assume $a = a^{-1}$. Multiplying that expression by a on the right, we have $aa = a^{-1}a$, that is $aa = e$ or, more neatly, $a^2 = e$. Conversely, suppose $aa = e$. Multiplying that expression by a^{-1} on the right yields $aaa^{-1} = ea^{-1}$, that is $a = a^{-1}$.

5. Let a, b and c each be equal to its own inverse. If $ab = c$, then $bc = a$ and $ca = b$. Our premise is that $a = a^{-1}$, $b = b^{-1}$ and $c = c^{-1}$; by using previous problem, we actually have $a^2 = e$, $b^2 = e$ and $c^2 = e$. Now if $ab = c$, then, multiplying it with b on the right, we have $ab^2 = cb$, which is $a = cb$, as $b^2 = e$. Now, we multiply $a = cb$ with c on the left and get $ca = c^2b$, that is, $ca = b$. Then we multiply this expression with a on the right to get $ca^2 = ba$, which is $c = ba$. Now, we multiply this by b on the left and get $bc = b^2a$, id est $bc = a$.

6. If abc is its own inverse, then bca is its own inverse, and cab is its own inverse. Suppose that $(abc)(abc) = e$ or, by applying associative law, $abcabc = e$. If we multiply this expression with a^{-1} on the left, we get $bcabc = a^{-1}$. Now, multiplying it with a on the right gets us $bcabca = e$, that is $(bca)^2 = e$. If we multiply former expression by b^{-1} on the left, we have $cabca = b^{-1}$. Finally, multiplying this equality on the right by b yields $cabcab = e$, that is, $(cab)^2 = e$.

7. Let a and b each be equal to its own inverse. Then ba is the inverse of ab. Suppose $aa = e$ and $bb = e$. We multiply the former expression with b on the right and now have $aab = b$. Multiplying this on the left by b gets us $baab = bb$, that is, $(ba)(ab) = e$ (or ab is the inverse of ba and reverse).

8. Let $c = c^{-1}$. Then $ab = c$ if and only if $abc = e$. Premise is that $cc = e$ (same as $c = c^{-1}$ as proved in a previous problem). Suppose $ab = c$. Then, if we multiply it by c on the right, we have $abc = cc$, that is, $abc = e$. Conversely, suppose $abc = e$; multiply this expression on the right by c to obtain $abcc = ec$, i.e. $ab = c$.

Theorem[6]**.** Let G be a group and $a_0, a_1, \ldots, a_n, a_{n+1} \in G$, where $a_0 = a_{n+1} = e$ (neutral element[7] in G). If

$$\prod_{i=n-p+2}^{n+1} a_i \prod_{i=0}^{n-p+1} a_i = e,$$

where $n, p \in \mathbb{N}$ such that $n + 1 \geq p$, then

$$\prod_{i=n-k+2}^{n+1} a_i \prod_{i=0}^{n-k+1} a_i = e,$$

[6]What this theorem actually tells us is that if factors are equal to a neutral element, then some rotation of these factors is also equal to a neutral element.

[7]We defined $a_0 = a_{n+1} = e$ only because it's more convinient to manipulate the expression this way. There is no other special reason.

where $k \in \mathbb{N}$ such that $p \geq k$. Reverse also holds.

Proof. Before we start with formal proof, consider this case, when $n = 10$ (only tells us the number of elements involved), $p = 7$ and $k = 3$:

$$\prod_{i=10-7+2}^{10+1} a_i \prod_{i=0}^{10-7+1} a_i = e,$$

which is actually:

$$\prod_{i=5}^{11} a_i \prod_{i=0}^{4} a_i = e.$$

Now, writing this down without product symbols gives us:

$$a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_0 a_1 a_2 a_3 a_4 = e.$$

Keep in mind that we defined $a_0 = a_{11} = e$, so we can neatly write the expression above, grouping it, as:

$$(a_5 a_6 a_7 a_8 a_9 a_{10})\,(a_1 a_2 a_3 a_4) = e.$$

Now, consider the consequent of the theorem implication, when $k = 3$ and compare it with the above. We would have:

$$\prod_{i=10-3+2}^{10+1} a_i \prod_{i=0}^{10-3+1} a_i = e,$$

which is again:

$$\prod_{i=9}^{11} a_i \prod_{i=0}^{8} a_i = e.$$

Considering $a_0 = a_{11} = e$ and grouping them meaningfully we have:

$$(a_9 a_{10})\,(a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8) = e.$$

In order to see the pattern between $p = 7$ and $k = 3$ rotations, we will make use of the following table, grouping them further in a meaningful way:

$$\begin{array}{c|l} p=7 & [a_5a_6a_7a_8]\,(a_9a_{10})\,(a_1a_2a_3a_4)=e \\ \hline k=3 & (a_9a_{10})\,(a_1a_2a_3a_4)\,[a_5a_6a_7a_8]=e \end{array}$$

So, to get from $p = 7$ to $k = 3$ we would need to multiply the $p = 7$ case with inverse of factors in square brackets on the left, and then with the same square brackets on the right. Observe that key factors are around brackets. In $p = 7$, first is a_5 whose index can be written down as $10 - 7 + 2$, that is $n - p + 2$. Next is a_8 whose index is actually $10 - 3 + 1$, i.e. $n - k + 1$. So a_9 index is $n - k + 2$, obviously, a_{10} is n and a_1 is 1. Last is a_4, whose index is $10 - 7 + 1$, i.e. $n - p + 1$. This will help us generalize the product in a more appropriate way, following that line of reasoning:

$$\prod_{i=n-p+2}^{n-k+1} a_i \prod_{i=n-k+2}^{n+1} a_i \prod_{i=0}^{n-p+1} a_i = e.$$

Notice that again we added a_0 and a_{11}, not changing actually anything; yet this additional condition will allow the proof to work for $p = n$ and $p = 1$ (same for $k = n$ and $k = 1$ in reverse). Now we need to multiply this equation by the inverse of the first product on the left. Now, we have:

$$\left(\prod_{i=n-p+2}^{n-k+1} a_i\right)^{-1} \prod_{i=n-p+2}^{n-k+1} a_i \prod_{i=n-k+2}^{n+1} a_i \prod_{i=0}^{n-p+1} a_i = \left(\prod_{i=n-p+2}^{n-k+1} a_i\right)^{-1}.$$

Now the first two products form a neutral element, leaving only

$$\prod_{i=n-k+2}^{n+1} a_i \prod_{i=0}^{n-p+1} a_i = \left(\prod_{i=n-p+2}^{n-k+1} a_i\right)^{-1}.$$

And finally, we multiply, on the right, this expression by the product inside the inverse on the right-hand side and get:

$$\prod_{i=n-k+2}^{n+1} a_i \prod_{i=0}^{n-p+1} a_i \prod_{i=n-p+2}^{n-k+1} a_i = \left(\prod_{i=n-p+2}^{n-k+1} a_i\right)^{-1} \prod_{i=n-p+2}^{n-k+1} a_i.$$

Joining products on the left-hand side in respect to their indices and seeing that two products on the right yield a neutral element, we have proved the first part of the theorem:

$$\prod_{i=n-k+2}^{n+1} a_i \prod_{i=0}^{n-k+1} a_i = e.$$

The reverse of the theorem implication is proved in the same way.

□

Lemma. If G is a group and $a_1, a_2, b \in G$, then, if b is inverse of a_1 and a_2, then $a_1 = a_2$.

Proof. Let a_1, a_2, b be elements of G such that $a_1 b = e$ (and $b a_1 = e$) and $a_2 b = e$ (and $b a_2 = e$). Then it follows that $a_1 b = a_2 b$. Multiplying by b^{-1} on the right, we have $a_1 b b^{-1} = a_2 b b^{-1}$, that is $a_1 = a_2$.

□

Remark. The lemma above tells us that every element has it's own unique inverse in a group.

Definition. If G is a finite group, then the **order of group** G, denoted by $|G|$, is equal to the number of elements in G.

Remark. We will use the same notation for cardinality of a set. Difference between those two notions is marginal.

Problem. Let G be a finite group and let S be the set of all the elements of G which are not equal to their own inverse, i.e.

$$S = \left\{ x \in G : \ x \neq x^{-1} \right\}.$$

Prove the following:

1. In any finite group G, the number of elements not equal to their own inverse is an even number, i.e. $|S| = 2k$, $k \in \mathbb{N}_0$ (give an example when $|S| = 0$).
2. The number of elements in G equal to their own inverse ($G \backslash S$) is odd or even, depending on whether the number of elements in G is odd or even.
3. If the order of G is even, there is at least one element x in G such that $x \neq e$ and $x = x^{-1}$.
4. If G is in addition Abelian, then:
   (a) $(a_1 a_2 \cdots a_n)^2 = e$;
   (b) If there is no element $x \neq e$ in G such that $x = x^{-1}$, then $a_1 a_2 \cdots a_n = e$.
   (c) If there is exactly one $x \neq e$ in G such that $x = x^{-1}$, then $a_1 a_2 \cdots a_n = x$.

Solution.

1. *In any finite group G, the number of elements not equal to their own inverse is an even number, i.e. $|S| = 2k$, $k \in \mathbb{N}_0$ (give an example when $|S| = 0$).* We suppose that all elements a_i in G, $i \in \{1, \ldots, n\}$ and $n \in \mathbb{N}$ are denoted so that $a_i \neq a_j$, for every $i \neq j$, $i, j \in \{1, \ldots, n\}$. In a previous lemma we have clearly proved that each a_i needs to have his pair a_j which is its unique inverse. If that were not so, if a_j was inverse to some other element a_k, by the previous lemma, a_i would equal a_k, contradicting our premise. Therefore, all elements that do not equal their own inverses, elements in S, need to come in unique pairs; in conclusion $|S|$ must be even. And S can be empty, i.e. for a trivial Abelian group $(G, *)$, where $G = \{a\}$ and $* : G \times G \to G$ such that $a * a = a$. It's trivial to show that this operation satisfies both axioms of totality and properties of an Abelian group. But, as a is a neutral element and $a * a = a$, it is it's own inverse and not contained in S. So, $|S| = 0$.

2. *The number of elements in G equal to their own inverse ($G \backslash S$) is odd or even, depending on whether the number of elements in G is odd or even.* Suppose that number of elements in G is even, that is $|G| = 2k$, $k \in \mathbb{N}$. Being that $|S| = 2l$, $l \in \mathbb{N}_0$, then, the number of elements equal to their own inverse is $|G \backslash S| = |G| - |S| = 2k - 2l = 2(k - l)$; in other words, it's even if $|G|$ is even. Similarly if G has odd number of elements, i.e. $|G| = 2k + 1$, $k \in \mathbb{N}_0$, then, being that $|G| - |S| = 2k + 1 - 2l = 2(k + l) + 1$, the number of elements equal to their own inverse is odd if number of elements in G is odd.

3. *If the order of G is even, there is at least one element x in G such that $x \neq e$ and $x = x^{-1}$.* If G is even, then, by the previous problem, number of elements which equal their own inverse ($|G \backslash S|$) is even. Being that neutral element is counted inside this set, i.e. $e \in G \backslash S$ (because $ee = e$, that is, neutral element is its own inverse), then removing it makes the number of elements inside that same set odd, leaving room for at least one element that equals its own inverse (of course $G \backslash S$ can never be empty, as it will always contain at least e; so if it's order is even, we cannot consider case when it's equal to zero).

4. If G is also Abelian, then:

   (a) $(a_1 a_2 \cdots a_n)^2 = e$. We can write this down as $(a_1 \ldots a_n)(a_1 \ldots a_n) = e$. Being that G is a group, associativity holds so we may as well write

   $$a_1 a_2 \ldots a_n a_1 a_2 \ldots a_n = e.$$

   Now, without loss of generality, let's suppose that $a_k = a_k^{-1}$ for $k \leq n$. In other words $a_k^2 = e$. We can organize the factors in the former equation,

using commutativity, to have $a_1a_1a_2a_2\dots a_ka_ka_{k+1}a_{k+1}\dots a_na_n = e$, that is $a_1^2a_2^2\dots a_k^2a_{k+1}a_{k+1}\dots a_na_n = e$. Because we presumed that $a_k^2 = e$, we are left with only $a_{k+1}a_{k+1}\dots a_na_n = e$. Now, we got rid off all the elements that equal their own inverse and are left with elements who do not equal their inverses. But, as G is a group, and all the other elements are contained in the former equation, their number is surely equal and we can pair them using commutativity with their inverses. We can presume that $a_ia_{i+1} = e$ (and if not, we can always rearrange them in such manner due to commutativity), where $k < i < n$, $i \in \mathbb{N}$. We would have

$$\prod_{i=\frac{k+1}{2}}^{\frac{n-1}{2}} (a_{2i}a_{2i+1})^2 = \prod_{i=\frac{k+1}{2}}^{\frac{n-1}{2}} e^2 = e^{n-k-2} = e,$$

thereby proving the desired inequality (note that we got the exponent on the neutral element by subtracting $\frac{n-1}{2} - \frac{k+1}{2} = \frac{n-1-k-1}{2} = \frac{n-k-2}{2}$, and then multiplying it by 2, as we had e^2).

(b) *If there is no element $x \neq e$ in G such that $x = x^{-1}$, then $a_1a_2\cdots a_n = e$.* This problem is similar to the previous problem. As we have no elements which equal their own inverses in the sequence of factors a_i in the previous equation, and, because every element needs to have its own inverse, we can pair them using commutativity as in the previous problem. Therefore, we would get, supposing $a_ia_{i+1} = e$, that $(a_1a_2)(a_3a_4)\cdots(a_{n-1}a_n) = e$ (here, commutativity was not necessary in our presumption, altough anyway we chose the indices to behave, we could arrange them in such manner through commutativity). Then, $ee\dots e = e^{\frac{n}{2}} = e$.

(c) *If there is exactly one $x \neq e$ in G such that $x = x^{-1}$, then $a_1a_2\cdots a_n = x$.* As in the previous two problems, suppose that, without loss of generality $a_1 = a_1^{-1}$, i.e. $a_1 = x$. Then, we can arrange factors, by commutativity, to get $x(a_2a_3)\cdots(a_{n-1}a_n) = xe^{\frac{n}{2}} = xe = x$.

Problem. Let G be any group. Let e denote the neutral element of G.

1. If a, b are any elements of G, prove each of the following:

   (a) If $a^2 = a$, then $a = e$;

   (b) If $ab = a$, then $b = e$;

   (c) If $ab = b$, then $a = e$;

2. Explain why every row of a group table must contain each element of the group exactly once.

3. There is exactly one group G on any set of three distinct elements. Use the operation table for this and further two excercises.

4. There is exactly one group G on any set of four distinct elements satisfying condition that $xx = e$ for every $x \in G$.

5. There is exactly one group G on any set of four distinct elements satisfying condition that $xx = e$ for some $x \in G$ and $yy \neq e$ for some $y \in G$.

Solution.

1. If a, b are any elements of G, prove each of the following:

   (a) If $a^2 = a$, then $a = e$. Multiplying this equality on the right (or left) by a^{-1} gets us $a^2a^{-1} = aa^{-1}$, that is, $a = e$.

   (b) If $ab = a$, then $b = e$. Multiplying this equality on the left by a^{-1} yields $b = e$.

   (c) If $ab = b$, then $a = e$. Multiplying this equality on the right by b^{-1} gives us $a = e$.

   Remark. Note that we could have used cancellation law on all three equations, i.e. $ab = ae$, and by cancellation law, that is necessarily $b = e$. But, proving cancellation law over and over again implicitly for an excercise is not a bad thing in itself.

2. *Explain why every row of a group table must contain each element of the group exactly once.* Suppose that we have a group of $n+1$ elements, $G = \{a_1, \ldots, a_n, e\}$, where e is a neutral element and that some element a_i (we can take a_1 without loss of generality) occurs k times in a row j (we can take $j = n-1$ also for illustrative purposes), where $k \in \mathbb{N}_0 \backslash \{1\}$. First we shall analyize it for a non-zero number in that set. That table would look something like this:

$\cdot$	a_1	a_2	a_3	$\ldots$	a_{n-1}	a_n	e
a_1				$\ldots$			a_1
a_2				$\ldots$			a_2
a_3				$\ldots$			a_3
$\vdots$							
a_{n-1}		a_1	a_1	$\ldots$		a_1	a_{n-1}
a_n				$\ldots$			a_n
e	a_1	a_2	a_3	$\ldots$	a_{n-1}	a_n	e

   Now, it must be true, e.g. $a_{n-1}a_2 = a_1$ and $a_{n-1}a_3 = a_1$ and so on... These two first equations are enough to conclude that $a_{n-1}a_2 = a_{n-1}a_3$, therefore, by

cancellation law (or by multiplying with a_{n-1}^{-1} on the left), it must be $a_2 = a_3$. We would get a chain of equalities for k elements (as we assumed some element occurs k times in a row), but that is a contradiction that we have $n+1$ elements as, if we consider set R which contains all equal elements,

$$R = \{a_i, a_j \in G : \ a_i = a_j, \ i, j \in S_k \subseteq \mathbb{N}\backslash\{1\}, \ |S_k| = k\},$$

we can easily substitute all $a_i \in R$ for one element, say, some a_j, and say that G actually has $n-k+1$ elements (of course, when we said in the beggining that G had n elements, we implicitly assumed they were distinct, which would have been enough for a proof by contradiction). And, as for $k = 0$, that means that our a_1 does not appear at all in a row. Now, as we have $n+1$ places in that row (for $a_1, a_2, \ldots, a_n$ and e) and only n elements on disposal (that is $a_2, \ldots, a_n$ and e), it would mean that some of these forementioned elements would have to appear twice; that is not advisable as we saw what happened earlier in this problem.

3. *There is exactly one group on any set of three distinct elements.* We can assume we have a set $G = \{e, a, b\}$. Now, one would think that we actually have room for 27 permutations (in each "box" of the table we have three possible elements to distribute) to complete that table (we will write a number of possibilities in each "box"):

$\cdot$	e	a	b
e	3	3	3
a	3	3	3
b	3	3	3

Keep in mind that every element has to appear exactly once in every row and that every element multiplied by a neutral element yields that same element. That limits our possibilities to $27 - 15 = 8$ (15 counting all the possibilities in rows and columns for e) cases because of the latter property (notice that we can distribute only two remaining elements in order to remain consistent with the former property):

$\cdot$	e	a	b
e	e	a	b
a	a	2	2
b	b	2	2

We must also mind not to have $ba = b$ or $ab = a$, as it would mean, by cancellation

law, that $a = e$ or $b = e$, respectively. Now, that means that we must fill this places with the only remaining element and that is e, leaving us only two possibilities:

$\cdot$	e	a	b
e	e	a	b
a	a	1	e
b	b	e	1

But, these two are easily filled, as we must also not allow ourselves to put a on the diagonal in the same row where we have a (same goes for b), as we would get, e.g. $a^2 = a$ and by cancellation property (being that we can write it as $aa = ae$) that would yield $a = e$. Therefore, it must be that $a^2 = b$ and $b^2 = a$, leaving us with the following table:

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. *There is exactly one group G on any set of four distinct elements satisfying condition that $xx = e$ for every $x \in G$.* We shall only present the finished table, presuming that $G = \{e, a, b, c\}$:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

5. *There is exactly one group G on any set of four distinct elements satisfying condition that $xx = e$ for some $x \in G$ and $yy \neq e$ for some $y \in G$.* We will follow the same example, as in a previous excercise, making only slight modifications to the operation table (suppose that $aa = e$ and $bb \neq e$). Notice that it must be $ba \neq b$ and $ba \neq a$, leaving $ba = c$. Furthermore, if $b^2 \neq e$, that means that either $ba = e$ or $bc = e$. But we have $a^2 = e$ and that would mean $ba^2 = a$, that is $b = a$. So it must be $bc = e$ (and the only remaining place in the row is for a, that is $b^2 = a$), but then it must not be $c^2 = e$ (we would get $bc^2 = c$, that is, $b = c$). So, we can then take $cb = e$ or $ca = e$. If we took $ca = e$, we would have $ca = a^2$ and then $c = a$. So, the only remaining option is to have $cb = e$ and $c^2 = a$. The operation table is such:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Definition. If G and H are any two groups, their **direct product** is denoted by $G \times H$ and consists of all ordered pairs (x, y) where $x \in G$ and $y \in H$, that is:

$$G \times H = \{(x, y) : \ x \in G, \ y \in H\}.$$

Remark. The definition above considers that a consistent operation is also defined on both groups, and is transfered to their direct product. Customary, if operation is multiplication-like, we will write:

$$(x, y)(x', y') = (xx', yy').$$

Similarly, if operation is addition-like, we will write:

$$(x, y) + (x', y') = (x + x', y + y').$$

Theorem. If G and H are groups, then $G \times H$ is a group. Furthermore, if G and H are Abelian groups, then $G \times H$ is also Abelian group.

Proof. We will do the proof by checking all the group axioms. If we manage to prove associativity and existence of neutral element and inverses, we will have proved that $G \times H$ is a group. In addition, if we prove commutativity, we will have proved that $G \times H$ is an Abelian group. We will prove commutativity before we find neutral elements and inverses, as we cut our work in half.

A. On the left-hand side we have:

$$(x_1, y_1)\left[(x_2, y_2)(x_3, y_3)\right] = (x_1, y_1)(x_2x_3, y_2y_3) = (x_1x_2x_3, y_1y_2y_3).$$

On the right-hand side,

$$\left[(x_1, y_1)(x_2, y_2)\right](x_3, y_3) = (x_1x_2, y_1y_2)(x_3, y_3) = (x_1x_2x_3, y_1y_2y_3).$$

Thus we have proved associativity.

C. It's obvious that $(x, y)(x', y') = (xx', yy')$. Now, as G and H are Abelian, we can write the previous expression as $(x, y)(x', y') = (x'x, y'y) = (x', y')(x, y)$, thus proving commutativity.

N. We need $(e_1, e_2) \in G \times H$ such that, for every $(x, y) \in G \times H$, holds $(x, y)(e_1, e_2) = (e_1, e_2)(x, y) = (x, y)$. From this we have $(e_1 x, e_2 y) = (x, y)$. We need e_1 such that $e_1 x = x$ and e_2 such that $e_2 y = y$. As $x \in G$ and $y \in H$, we will need neutral elements from G and H. Let e_G be neutral element in G and e_H neutral element in H. Then, obviously $e_G x = x$ and $e_H y = y$. Therefore, our neutral element is $(e_G, e_H) \in G \times H$.

I. Let's find (x^{-1}, y^{-1}) such that $(x^{-1}, y^{-1})(x, y) = (x, y)(x^{-1}, y^{-1}) = (e_G, e_H)$. From this expression we can derive that $xx^{-1} = e_G$ and $yy^{-1} = e_H$. As G and H all have inverses, we can take $x_G^{-1} \in G$ such that $xx_G^{-1} = x_G^{-1}x = e_G$ and $y_H^{-1} \in H$ such that $yy_H^{-1} = y_H^{-1}y = e_H$. So, our inverse elements do exist and they are $(x_G^{-1}, y_H^{-1}) \in G \times H$.

By this, we have proved that $G \times H$ is (Abelian group) if G and H are both (Abelian) groups.

□

Problem. List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$, and write its operation table (with additive notation).

Solution. As $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_3 = \{0, 1, 2\}$, their direct product will be the set

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

Operation table is as follows:

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Problem. Suppose the groups G and H both have the property that every element is its own inverse. Prove that $G \times H$ also has this property.

Solution. We can write the fact that every element is its own inverse in this fashion:

$x^2 = e_G$ for every $x \in G$ and $y^2 = e_H$ for every $y \in H$, where e_G is a neutral element in G and e_H neutral element in H. Now, let us prove that $(x, y)(x, y) = (e_G, e_H)$, that is, that every element in $G \times H$ is its own inverse. We know that $(x, y) = (x, y)$ for every $(x, y) \in G \times H$. Multiplying that expression on the right (or left) with (x, y) gets us $(x, y)(x, y) = (x, y)(x, y)$. We will calculate the right-hand side. We have $(x, y)(x, y) = (xx, yy)$, which is actually $(x, y)(x, y) = (x^2y^2)$. Now, that is, by properties of G and H, $(x, y)(x, y) = (e_G, e_H)$.

Problem. Let G be a group, and $a, b \in G$. For any positive integer n we define a^n by $a^n = \prod_{i=1}^{n} a$. If there is an element $x \in G$ such that $x^2 = a$, we say that a has a square root in G. Similarly, if $a = y^3$ for some $y \in G$, we say a has a cube root in G. In general, a has an nth root in G if $a = z^n$ for some $z \in G$. Prove the following:

1. $(bab^{-1})^n = ba^nb^{-1}$;
2. If $ab = ba$, then $(ab)^n = a^nb^n$ for every positive integer n.
3. If $xax = e$, then $(xa)^{2n} = a^n$.
4. If $a^3 = e$, then a has a square root.
5. If $a^2 = e$, then a has a cube root.
6. If a^{-1} has a cube root, so does a.
7. If $x^2ax = a^{-1}$, then a has a cube root.
8. If $xax = b$, then ab has square root.

Solution.

1. $(bab^{-1})^n = ba^nb^{-1}$. Proof by induction. For $n = 1$ it's easy to see that $(bab^{-1})^1 = ba^1b^{-1}$, that is, $bab^{-1} = bab^{-1}$. Assume that the argument is valid for some $n = k$, i.e. $(bab^{-1})^k = ba^kb^{-1}$ is true. Let's prove that it's true for $n = k + 1$. Then we have $(bab^{-1})^{k+1} = ba^{k+1}b^{-1}$. From the left-hand side we get $(bab^{-1})^k(bab^{-1})$. By using assumption of mathematical induction that is $(bab^{-1})^k(bab^{-1}) = (ba^kb^{-1})(bab^{-1})$. Due to associativity we can disregard parentheses on the right to get $(bab^{-1})^k(bab^{-1}) = ba^kb^{-1}bab^{-1}$. Now, as $b^{-1}b = e$, we have $(bab^{-1})^k(bab^{-1}) = ba^kab^{-1}$; as $a^ka = a^{k+1}$, we have proved the argument, as we now have $(bab^{-1})^{k+1} = ba^{k+1}b^{-1}$.

2. *If $ab = ba$, then $(ab)^n = a^nb^n$ for every positive integer n.* Proof by induction. For $n = 1$ we have $(ab)^1 = a^1b^1$, that is $ab = ab$, and thus a proved basis of induction. Now, assume that $(ab)^k = a^kb^k$ is true for some $k \in \mathbb{N}$. Let's prove that it's true

for $k+1$. We have, on the right-hand side, $(ab)^{k+1} = (ab)^k(ab)$. Now, by our hypothesis, it's $(ab)^{k+1} = a^k b^k ab$. As our premise is commutativity, we are able to rearrange the elements on the right in such manner that $(ab)^{k+1} = a^k ab^k b$ (we switched places of b^k and a). Now we have $(ab)^{k+1} = a^{k+1}b^{k+1}$. This proves our argument. *Remark.* Notice that this property does not hold for commutativity, as we can only say that $(ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_{n \text{ times}}$.

3. *If $xax = e$, then $(xa)^{2n} = a^n$.* Proof by induction. First we have $n = 1$. That is, $(xa)^{2\cdot 1} = a^1$. Now, $xaxa = a$, and by using premise, we have $ea = a$, i.e. $a = a$. Basis of induction is proved. Suppose the argument $(xa)^{2k} = a^k$ is valid for some $k \in \mathbb{N}$. Let's prove that $(xa)^{2k+2} = a^{k+1}$ is also true, that is, $(xa)^{2k}(xa)^2 = a^{k+1}$. From our assumption for k it follows that $(xa)^{2k}(xa)^2 = a^k(xa)^2$. But, from basis of induction we had $(xa)^2 = a$. So, we have $(xa)^{2k+2} = a^k a$ and then $(xa)^{2k+2} = a^{k+1}$, quod erat demonstrandum. *Example.* If we take group $\mathbb{R}\backslash\{0\}$ with multiplication, we can take $x = \frac{1}{5}$ and $a = 25$. Then, $\frac{1}{5}\cdot 25 \cdot \frac{1}{5} = 1$, obviously; note that this yields 1, which is the neutral element for multiplication in $\mathbb{R}\backslash\{0\}$. Now, $\left(\frac{1}{5}\cdot 25\right)^{2n} = 5^{2n}$, which is exactly 25^n, that is a^n.

4. *If $a^3 = e$, then a has a square root.* We need to find $x \in G$ such that $x^2 = a$. Multiplying $a^3 = e$ by $(a^2)^{-1}$ on the right (or on the left) we have $aa^2(a^2)^{-1} = (a^2)^{-1}$. Now, all that remains is $a = (a^2)^{-1}$. We can write this a bit different, as $a = (a^{-1})^2$. We found $x \in G$ such that $x^2 = a$, and that is $x = a^{-1}$. It's inverse is it's square root! *Example.* One fine example is in group of real numbers (without zero). It's obvious that $(1)^3 = 1$ (and 1 is neutral element for multiplication in $\mathbb{R}\backslash\{0\}$) and also that there exist such x that $x^2 = 1$, and that is, not only 1 (which is the multiplicative inverse of 1, that is, of itself), but also -1. In group $(\mathbb{Z}, +)$ we have $3 \cdot 0 = 0$ (notice that, when addition or addition-like operations are in question, we do not write a^n, but na, or $n \cdot a$), and then there exists such x that $2x = 0$, and that is $x = 0$ (which is the additive inverse of 0, i.e. itself).

5. *If $a^2 = e$, then a has a cube root.* We need to find $x \in G$ such that $x^3 = a$. If we multiply the equation in our implication's antecedent by a (on the left or right) we have $a^3 = a$. Therefore, $x = a$ is the square root of a. In other words, if $a^2 = e$, cube root of a is itself. *Example.* Take, for instance, $\mathbb{R}\backslash\{0\}$, with multiplication. Obviously $1^2 = 1$, which is a neutral element for multiplication in $\mathbb{R}\backslash\{0\}$. By this theorem, 1 has a cube root, and that is itself, as $1^3 = 1$. Similarly, $(-1)^2 = 1$ and $(-1)^3 = -1$ (cube root of -1 is itself).

6. *If a^{-1} has a cube root, so does a.* As a^{-1} has a cube root, then there exists such $x \in G$ that $x^3 = a^{-1}$. If we multiply this by a on the right and then by $(x^3)^{-1}$ on the left, we have $ax^3(x^3)^{-1} = aa^{-1}(x^3)^{-1}$. Now, from this we get $(x^{-1})^3 = a$.

That is, the cube root of a is the inverse of the cube root of a^{-1}. *Example.* In $\mathbb{R}\backslash\{0\}$ with multiplication we have, e.g. $(\frac{1}{2})^3 = \frac{1}{8}$. Obviously, inverse of $\frac{1}{8}$ is 8, and inverse of $\frac{1}{2}$ (which is cube root of $\frac{1}{8}$) is 2. So we have $2^3 = 8$. In $(\mathbb{Z}, +)$ we have, e.g. $3 \cdot 5 = 15$. Inverse of 5 is -5 and inverse of 15 is -15. So, it's $3 \cdot (-5) = -15$, which is, again, true.

7. *If $x^2ax = a^{-1}$, then a has a cube root.* We need $y \in G$ such that $y^3 = a$. Suppose $x^2ax = a^{-1}$. Multiplying this by $(ax)(xax)$ on the left gives us $x^2(ax)(ax)(xax) = a^{-1}ax^2ax$, i.e. $(xax)^3 = x^2ax$ and that is $(xax)^3 = a^{-1}$. Thus, it follows that a^{-1} has a cube root, that is xax. And, by the previous problem, if a^{-1} has a cube root, so does a, and it's the inverse of the cube root of a^{-1}, which would, in this case, be $y = (xax)^{-1}$, i.e., $y = x^{-1}a^{-1}x^{-1}$.

8. *If $xax = b$, then ab has square root.* Multiplying this on the left by a gives us $axax = ab$, that is, $(ax)^2 = ab$. Therefore, ab has a square root and it is ax.

Problem. Let $M(n) \in \mathbb{R}^{n\times n}$ denote the set of all $n \times n$ square matrices. Is $M(n)$ with matrix multiplication[8] a group?

Solution. We will check all the properties. It's obvious that closure is satisfied as, by definition, we get a $n \times n$ matrix when multiplying two $n \times n$ matrices. As for the rest:

A. Let $A, B, C \in M(n)$ such that $A = [a_{ij}]_{n\times n}$, $B = [b_{ij}]_{n\times n}$ and $C = [c_{ij}]_{n\times n}$. We will check whether $A(BC) = (AB)C$. We see that:

$$AB = \left[\left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)_{ij}\right]_{n\times n}.$$

Then, $(AB)C$ is defined as:

$$(AB)C = \left[\left(\sum_{l=1}^{n}\left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)_{il} c_{lj}\right)_{ij}\right]_{n\times n}.$$

But that can be written as:

$$(AB)C = \left[\left(\sum_{l=1}^{n} c_{lj}\sum_{k=1}^{n} a_{ik}b_{kl}\right)_{ij}\right]_{n\times n} = \left[\left(\sum_{l=1}^{n}\sum_{k=1}^{n} a_{ik}b_{kl}c_{lj}\right)_{ij}\right]_{n\times n}.$$

[8]Let $A = [a_{ij}]_{n\times n}$ and $B = [b_{ij}]_{n\times n}$ be matrices. Then their product is a matrix $AB = [c_{ij}]_{n\times n}$ with $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$.

Rearranging sums, we can see that associativity holds:

$$\begin{aligned}(AB)C &= \left[\left(\sum_{k=1}^{n} a_{ik} \sum_{l=1}^{n} b_{kl} c_{lj}\right)_{ij}\right]_{n\times n} \\ &= \left[\left(\sum_{k=1}^{n} a_{ik} \left(\sum_{l=1}^{n} b_{kl} c_{lj}\right)_{kj}\right)_{ij}\right]_{n\times n} = A(BC).\end{aligned}$$

N. Neutral element is $I = [p_{ij}]_{n\times n}$ such that $p_{ii} = 1$ for all $i \in \{1, \ldots, n\}$ and $p_{ij} = 0$ for all $i \neq j$, where $i, j \in \{1, \ldots, n\}$. Take $A \in M(n)$. Then:

$$AI = \left[\left(\sum_{k=1}^{n} a_{ik} p_{kj}\right)_{ij}\right]_{n\times n}.$$

Obviously $a_{ik}p_{kj} = 0$ when $k \neq j$, so all that remains is $a_{ij}p_{jj} = a_{ij}$ corresponding to ij-th element of the AI matrix. Same thing goes for IA. Therefore $AI = IA = A$, where $I \in M(n)$ is the identity matrix.

I. There are no inverses, in general, e.g. take $A \in M(n)$ such that $a_{ij} = 0$ for all $i, j \in \{1, \ldots, n\}$. Then we would need B such that $AB = I$, but:

$$\left[\left(\sum_{k=1}^{n} a_{ik} b_{kj}\right)_{ij}\right]_{n\times n} = [0_{ij}]_{n\times n},$$

which can never be equal to I.

C. Matrix multiplication is not commutative in general as

$$\left[\left(\sum_{k=1}^{n} a_{ik} b_{kj}\right)_{ij}\right]_{n\times n} = \left[\left(\sum_{k=1}^{n} b_{ik} a_{kj}\right)_{ij}\right]_{n\times n}$$

will not hold due to different arrangements of matrix members.

Set $M(n)$ with matrix multiplication is a monoid.

Problem. Let $O(n) \in \mathbb{R}^{n\times n}$ be the set of all $n \times n$ orthogonal matrices[9]. Is $O(n)$ with matrix multiplication a group?

[9] A matrix A is orthogonal if $AA^T = A^TA = I$.

Solution. We have already checked associativity and found a neutral element (identity matrix) in the previous problem for $M(n) \supset O(n)$. Now, by definition of orthogonal matrices it's true that $AA^T = A^TA = I$ for all $A \in O(n)$. Therefore there are inverses for all orthogonal matrices and it's their respective transpose matrix. Commutativity, of course, does not still hold in general. Set $O(n)$ with matrix multiplication is a group.

Category Theory Basics

Before we venture further into the stunning world of abstract algebra by defining subgroups in the next chapter, I would like, as I have mentioned in introduction to say something about the basics of categories in mathematics. The reason why I'm doing this, is because I feel that gentle comparison with abstract algebra, and gentle introduction of modern concepts might accelerate the infusion of the latter into the reader's mind. However, I do not feel that there ever will be a reader, and even if it were the case, I see no point in it. The beauty was to lie only for me, the beauty was to affirm my power over the academic circles which have ignored me for years and which have, and perhaps forever will, consider me a complete failure. Let it be so. For may I be then considered Ed Wood of mathematics and derogatively called Euler for my ventures in philosophy. There is no point at all.

Definition. Sometimes it is easier to say what something consists of than what it is. The difference in quality is infinite, yet it's so far the best I can do. So, a **category** (denoted by $\mathcal{C}$; or, in case when we're dealing with more categories, $\mathcal{A}$, $\mathcal{B}$, et cetera) consists of:

1. **Objects.** Usually denoted by A, B, C, etc. The collection of objects in category $\mathcal{C}$ is then $ob(\mathcal{C}) = \{A, B, C, \ldots\}$ (a bit naively).

2. **Morphisms.** A morphism can be considered as an *arrow* going from one object to the other; usually denoted by f, g, h, and so on. The collection of morphisms in category $\mathcal{C}$ is then $ar(\mathcal{C}) = \{f, g, h, \ldots\}$.

3. **Typings.** Typing on a morphism is the relation that actually relates (forgive me for a bit some Hegelian dialectic) objects by the use of morphisms. Therefore, they can be thought of as functions whose domain is one object and codomain another. one example of a typing would be $f : A \to B$. In this case, $A \to B$ is the *type* of f and f is a *morphism from* A to B. If we're dealing with more categories, we will use, exempli gratia, $f : A \to_{\mathcal{C}} B$ for a morphism from A to B in category $\mathcal{C}$. Now, if we want all the morphisms (say we have f, g and h) of the type $A \to B$, we get them all in one collection denoted by, e.g. $Hom(A, B) = \{f, g, h\}$. Sometimes it's $Mor(A, B)$, $Hom_{\mathcal{C}}(A, B)$ (especially when dealing with more then one category) and rarely $\mathcal{C}(A, B)$.

4. **Compositions.** We have already discussed the notion of a partial binary relation (it has to be closed and give unique elements, but does not have to be defined for each ordered pair). Now, in category theory, a partial binary relation is a sort of composition (denoted in many ways, but for now, we shall use either $\circ$ or

juxtaposition) between morphisms (that we can intuitively know from function composition).

5. **Identities.** For each object, there is a identity morphism, i.e. for some object A, there is $id_A : A \to A$.

Remark. Now, we have defined, all sorts of "things": objects, morphisms, compositions, etc. But what do they really represent? I would say, nothing special, but that would be, sort of, the same as to say, anything at all! One may fall into a beginner's trap, which they sure nailed in category-theoretic alphabet, and consider morphisms as functions when describing certain categories, and objects as elements of a set, et similis. But, of course, this is only half-true. Sometimes, as we will see, morphisms can themselves represent elements of some set we're defining as a category, but in another, objects might do the same trick. This will be explained later through some examples.

Now, every category is subject to the following three typing axioms and two composition axioms.

Typing axioms.

1. *Unique type*[10]. If $f : A \to B$ and $f : A' \to B'$, then $A = A'$ and $B = B'$.
2. *Composition type.* For every $f : A \to B$ and $g : B \to C$, there is $g \circ f : A \to C$ (i.e. $fg : A \to C$).
3. *Identity type.* For every A, there is $id_A : A \to A$.

Composition axioms.

1. *Associativity.* For every $f : A \to B$, $g : B \to C$ and $h : C \to D$ it's $h \circ (g \circ f) = (h \circ g) \circ f$, i.e. $(fg)h = f(gh)$.
2. *Identity.* For every $f : A \to B$, it's $id_B \circ f = f = f \circ id_A$ (or, $fid_B = f = id_A f$).

If only unique type axiom is not satisfied, then we're dealing with a *pre-category.*

Set. Set can be defined as a category whose objects are viewed as elements of a set, and we have only identity arrows, no other morphisms. It's trivial to see that all axioms are satisfied.

[10]There are no duplicates of the same morphisms.

Monoid. Monoid is a one-object category whose (identity) morphisms are elements of the underlying monoid set, with composition between morphisms serving as an operation defined on that underlying monoid set. If we have a monoid $(S, *)$, where $S = \{e, a_1, \ldots, a_n\}$, then define category $\mathcal{C}$ such that $ob(\mathcal{C}) = \{A\}$ and $ar(\mathcal{C}) = \{a_1, \ldots, a_n\}$, such that $a_i : A \to A$, for $i = 1, \ldots, n$. Obviously $Mor(A \to A) = S$. It's easy to see that associativity is satisfied, there is a neutral element for composition, $id_A : A \to A$, which can be denoted by e. Then $e \circ a_i = a_i \circ e = a_i$ for all $i = 1, \ldots, n$. So, it's trivial to see that this is a monoid structure satisfying category axioms.

Group. Monoid category can be made into a category resembling a group by further defining $a_i^{-1} : A \to A$ for every $a_i : A \to A$, for all $i = 1, \ldots, n$. Same thing can be done with Abelian group, by defining $a_i a_j = a_j a_i$ for all $i, j = 1, \ldots, n$.

Of course, these were some rather naive examples that are useful mostly to make us see the way we can view structures in algebra from categorical point of view.

Subgroups

Definition. Let G be a group and $S \subseteq G$, $S \neq \emptyset$. If $xy \in S$ for every $x, y \in S$, and if $a^{-1} \in S$, for every $a \in S$, then S is called a **subgroup** of G (we are assuming, of course, that we're dealing with the same operation that is defined on G).

Theorem. Let G be a group. Every subgroup of G is a group.

Proof. Let G be a group and S a subgroup of G. We need only check associativity and existence of a neutral element, as, by definition, S is closed with respect to the same operation defined on G, and every element in S has its inverse in S. As for associativity, take any $a, b, c \in S$. As $S \subseteq G$, then $a, b, c \in G$. Being that G is a group, it is necessarily associative, and then it must be that $a(bc) = (ab)c$. Therefore, S is also associative. Now, as $a^{-1} \in S$ for every $a \in S$, and as $xy \in S$ for every $x, y \in S$, then also, necessarily, $aa^{-1} \in S$. But, $aa^{-1} = e$, which proves that $e \in S$. Thus, S is a group.

□

Problem. Let C and D be sets, with $C \subseteq D$. Then $\mathcal{P}_C$ is a subgroup of $\mathcal{P}_D$ (operation is symmetric difference).

Solution. By definition, $\mathcal{P}_C = \{S : S \subseteq C\}$ and $\mathcal{P}_D = \{S : S \subseteq D\}$. If we take some $S \subseteq D$ then it must be that $S \in \mathcal{P}_D$. In this problem, it's $C \subseteq D$, so $C \in \mathcal{P}_D$. Now, if we take some $S \in \mathcal{P}_C$, then, by definition, $S \subseteq C$, which is, in turn, subset of D, therefore $S \subseteq D$ and it must be that $S \in \mathcal{P}_C$. By definition of set inclusion[11], it must be that $\mathcal{P}_C \subseteq \mathcal{P}_D$. We have shown previously that $(\mathcal{P}_D, \Delta)$ is an Abelian group, but so is $(\mathcal{P}_C, \Delta)$! Therefore, it must be that $\mathcal{P}_C$ is closed under operation of symmetric difference Δ and with respect to inverses, by definition of a group. Then it must be, as, in addition, $\mathcal{P}_C \subseteq \mathcal{P}_D$ that $\mathcal{P}_C$ is a subgroup of $\mathcal{P}_D$.

Remark. In further excercises, we will denote $\mathbb{R}\backslash\{0\}$ as $\mathbb{R}^*$. Also, we will use $\mathcal{F}(\mathbb{R})$ to represent the set of all functions going from $\mathbb{R}$ to $\mathbb{R}$. Similarly, with $\mathcal{C}(\mathbb{R})$ the set of all continuous functions going from $\mathbb{R}$ to $\mathbb{R}$, and with $\mathcal{D}(\mathbb{R})$ the set of all differentiable functions going from $\mathbb{R}$ to $\mathbb{R}$.

Theorem. Let $\mathcal{F}(\mathbb{R}) = \{f : \ f : \mathbb{R} \to \mathbb{R}\}$. Then $(\mathcal{F}(\mathbb{R}), +)$ is a group, and $(\mathcal{C}(\mathbb{R}), +)$ and $(\mathcal{D}(\mathbb{R}), +)$ are subgroups of $(\mathcal{F}(\mathbb{R}), +)$, and therefore groups by themselves.

[11] $(\forall x)(x \in X \to x \in Y)$ iff $X \subseteq Y$

Proof. Note that we define function addition[12] as $[f+g](x) = f(x)+g(x)$ for all $x \in \mathbb{R}$. Take $f, g, h \in \mathcal{F}(\mathbb{R})$. We will check whether associativity holds. Now, take $[f+[g+h]](x) = f(x)+[g+h](x) = f(x)+g(x)+h(x) = [f+g](x)+h(x) = [[f+g]+h](x)$, for all $x \in \mathbb{R}$; in conclusion, it is associative. Commutativity holds as $[f+g](x) = f(x)+g(x) = g(x)+f(x) = [g+f](x)$, for all $x \in \mathbb{R}$. Now, neutral element is $\mathcal{O}(x) = 0$, as $[f+\mathcal{O}](x) = f(x)+\mathcal{O}(x) = f(x)+0 = f(x)$ (remember that we need not show that it's a left neutral element because addition is commutative). It's obvious that $[-f](x) = -f(x)$ is the inverse function, as $[f+[-f]](x) = f(x)+(-f(x)) = 0 = \mathcal{O}(x)$, for all $x \in \mathbb{R}$. Thus we have proved that $(\mathcal{F}(\mathbb{R}), +)$ is an Abelian group. Now, it's obvious[13] that $\mathcal{D}\mathbb{R} \subset \mathcal{C}(\mathbb{R}) \subset \mathcal{F}(\mathbb{R})$. Now, as the sum of two continuous functions is a continuous function and the sum of two differentiable functions is a differentiable functions, both are closed under addition. If f is continuous then so is $-f$ which is it's additive inverse. Also, if f is differentiable, then so is $-f$, which is it's additive inverse. Thus, $(\mathcal{C}(\mathbb{R}), +)$ and $(\mathcal{D}(\mathbb{R}), +)$ are subgroups of $(\mathcal{F}(\mathbb{R}), +)$, and then groups by themselves.

□

Problem. Determine whether or not H is a subgroup of G (again, assume that the operation on H is the same as on G; and of course, from previous excercises we should *know* that G are groups in all problems below):

1. $G = (\mathbb{R}^*, \cdot)$, $H = \{2^n : \ n \in \mathbb{Z}\}$;
2. $G = (\mathbb{R}, +)$, $H = \{\log a : \ a \in \mathbb{Q}, \ a > 0\}$;
3. $G = (\mathbb{R}, +)$, $H = \{\log n : \ n \in \mathbb{Z}, \ n > 0\}$;
4. $G = (\mathbb{R}, +)$, $H = \{x \in \mathbb{R} : \ \tan x \in \mathbb{Q}\}$;
5. $G = (\mathbb{R}^*, \cdot)$, $H = \{2^n 3^m : \ m, n \in \mathbb{Z}\}$;
6. $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, y) : \ y = 2x\}$;
7. $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, y) : \ x^2 + y^2 > 0\}$;
8. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(0) = 0\}$;

[12]Note that most people get confused with $(f+g)(x) = f(x)+g(x)$, thinking that there is some underlying mathematical construction of function addition. But, we cannot *add* functions themselves. And, thus, to avoid confusion, we will use $[f+g](x) := (f+g)(x)$, to suggest to reader that the plus sign is just a part of notation, not some operation between the two mapping rules. We could as well write $h(x) = f(x)+g(x)$; the difference between the latter and the former is only in notation, nothing more, nothing less.

[13]We're using the fact that all differentiable functions are continuous.

9. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(x) = 0, \ \forall x \in [0,1]\}$;

10. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(-x) = -f(x)\}$;

11. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(x + n\pi) = f(x), \ \forall n \in \mathbb{Z}, \ \forall x \in \mathbb{R}\}$;

12. $G = (\mathcal{C}(\mathbb{R}), +)$, $H = \left\{f \in \mathcal{C}(\mathbb{R}) : \ \int_0^1 f(x)dx = 0\right\}$;

13. $G = (\mathcal{D}(\mathbb{R}), +)$, $H = \left\{f \in \mathcal{D}(\mathbb{R}) : \ \frac{df}{dx} = c, \ c \in \mathbb{R}\right\}$;

14. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(x) \in \mathbb{Z}, \ \forall x \in \mathbb{R}\}$;

Solution. Now, we only need to check whether $H \subseteq G$ (if it's not obvious), check whether the operation is closed on H and if it's closed with respect to inverses.

1. $G = (\mathbb{R}^*, \cdot)$, $H = \{2^n : \ n \in \mathbb{Z}\}$. Obviously if $n \in \mathbb{Z}$, then $2^n \in \mathbb{Q} \subset \mathbb{R}$, so $H \subset G$. Now, take $a, b \in H$, we need to show that $ab \in H$. So, let $a = 2^n$, $n \in \mathbb{Z}$ and $b = 2^m$, $m \in \mathbb{Z}$. If we take $ab = 2^n \cdot 2^m$, obviously $ab \in H$, as $ab = 2^{m+n}$, which is in H. Let's find inverse of $a \in H$; take, the same $a = 2^n$ and try to find $2^n \cdot x = 1$. That is of course 2^{-n}, because $2^n \cdot 2^{-n} = 2^0 = 1$. Of course, $a^{-1} = 2^{-n}$ is in H as $-n \in \mathbb{Z}$. Therefore H is a subgroup of G.

2. $G = (\mathbb{R}, +)$, $H = \{\log a : \ a \in \mathbb{Q}, \ a > 0\}$. If $a \in \mathbb{Q}^+$, then $\log a \in \mathbb{R}$, so $H \subset G$. Take $x, y \in H$, such that $x = \log a$, $y = \log b$, where $a, b \in \mathbb{Q}^+$. Now, $x + y = \log a + \log b = \log ab \in H$. Now, to find inverse, we need $x^{-1} \in H$, take $x^{-1} = \log z$, $z \in \mathbb{Q}$, such that $x + x^{-1} = 0$. Now $\log az = 0$ iff $z = \frac{1}{a}$ as $\log a\frac{1}{a} = \log 1 = 0$. So there is an inverse, now we can denote it by $-x = -\log a$, and it is in H, as $\frac{1}{a} \in \mathbb{Q}^+$ ($a \in \mathbb{Q}^+$ also, so we are secure of it being zero). H is a subgroup of G.

3. $G = (\mathbb{R}, +)$, $H = \{\log n : \ n \in \mathbb{Z}, \ n > 0\}$. Obviously H will not be a subgroup of G as it's not closed with respect to inverses. There is no $-x = -\log n$ for every $x = \log n$ because $-x = \log \frac{1}{n}$ which is in H if and only if $n = 1$.

4. $G = (\mathbb{R}, +)$, $H = \{x \in \mathbb{R} : \ \tan x \in \mathbb{Q}\}$. It's true that $H \subset G$ as x defined to be in $\mathbb{R}$. Now, take $x, y \in H$ such that $\tan x \in \mathbb{Q}$ and $\tan y \in \mathbb{Q}$. Let $\tan x = \frac{a}{b}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and $\tan y = \frac{c}{d}$, $c \in \mathbb{Z}$, $d \in \mathbb{N}$. Then, we need to show that $x + y$ is such that $\tan(x + y) \in \mathbb{Q}$. An addition formula tells us:

$$\tan(x + y) = \frac{\tan x + \tan y}{1 - \tan x \tan y} = \frac{\frac{a}{b} + \frac{c}{d}}{1 - \frac{ab}{cd}} = \frac{\frac{ad+bc}{bd}}{\frac{cd-ab}{cd}} = \frac{(ad + bc)(cd)}{(bd)(cd - ab)}.$$

So, as both $\tan x$ and $\tan y$ are rational, their sum and product will be rational, and we will have that $\tan(x + y)$ is a rational number. But what if $\tan x \tan y =$

1, i.e. $cd = ab$? Then we have division by zero! Well, as $\tan\left(\frac{\pi}{4} + k\frac{\pi}{2}\right) = 1$, then $\tan x \tan y = 1$ for $x = y = \frac{\pi}{4} + k\frac{\pi}{2}$, $k \in \mathbb{Z}$ and both $\tan x$ and $\tan y$ will be rational (they will each equal 1). So, this operation is not closed on H and H is not a subgroup of G.

5. $G = (\mathbb{R}^*, \cdot)$, $H = \{2^n 3^m : \ m, n \in \mathbb{Z}\}$. It's obvious that $2^n 3^m \in H \subset \mathbb{R}^*$. Now, if we take $2^n 3^m, 2^p 3^q \in H$, then $2^n 3^m 2^p 3^q = 2^{n+p} 3^{m+q}$. As $n, m, p, q \in \mathbb{Z}$, then also $(n+p), (m+q) \in \mathbb{Z}$; therefore H is closed in respect to multiplication. As for inverses, obviously it's $2^{-n}3^{-m} \in H$ because $2^n 3^m 2^{-n} 3^{-m} = 2^{n-n} 3^{m-m} = 2^0 3^0 = 1$, which is neutral element for multiplication. Therefore, H is a subgroup of G.

6. $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, y) : \ y = 2x\}$. Obviously $(x, 2x) \in H \subset \mathbb{R}^2$. Now, if we take $(x, y), (p, q) \in H$ such that $y = 2x$ and $q = 2p$, if we add them, $(x, y) + (p, q) = (x + p, y + q)$ is $y + q = 2(x + p)$? Well, considering that $y = 2x$ and $q = 2p$, then $y + q = 2x + 2p = 2(x + p)$, therefore H is closed with respect to addition. Neutral element for addition is 0, so neutral element in G is $(0, 0)$. And that we shall get if we take $(x, y) + (x^{-1}, y^{-1}) = 0$. Therefore, it must be that $x + x^{-1} = 0$ and $y + y^{-1} = 0$. So, obviosly $x^{-1} = -x$, and if $y = 2x$ and $y^{-1} = -y$ then $y^{-1} = -2x = 2x^{-1}$. So, inverse element for $(x, y) \in H$ is $(-x, -2x) \in H$. In conclusion, H is a subgroup of G.

7. $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, y) : \ x^2 + y^2 > 0\}$. As all elements in H, except $(0, 0)$, satisfy $x^2 + y^2 > 0$, obviously $H = (\mathbb{R} \times \mathbb{R}^2) \setminus \{(0, 0)\} \subset (\mathbb{R} \times \mathbb{R})$. But, take $(-4, 4), (4, -4) \in H$. Obviously $(-4)^2 + 4^2 = 16 + 16 = 32 > 0$, and same goes for $(4, -4)$, so they really are in H, but $(-4, 4) + (4, -4) = (-4 + 4, 4 - 4) = (0, 0) \notin H$, as $0^2 + 0^2 = 0 + 0 = 0$ and it's not the case that $0 > 0$. So H cannot be a subgroup of G.

8. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(0) = 0\}$. Obviously $H \subset \mathcal{F}(\mathbb{R})$. Now, take $f, g \in H$ such that $f(0) = g(0) = 0$. We need to show that for $f + g$ it's $[f + g](0) = 0$. Now, it's true that $f(x) + g(x) = [f + g](x)$, so if $f(0) = 0$ and $g(0) = 0$, then $0 = f(0) + g(0) = [f + g](0)$. So, $[f + g] \in H$. Now, obviously, $f(x) + (-f(x)) = 0 = \mathcal{O}(x)$ which is a neutral element for addition in G, so H is a subgroup of G, as $-f(x) \in H$ if $f(x) \in H$; because $f(0) = 0$ and then $-f(0) = 0$.

9. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(x) = 0, \ \forall x \in [0, 1]\}$. Obviously, again, $H \subset \mathcal{F}(\mathbb{R})$. But, take $f, g \in H$ and then it's $f(x) = 0$ and $g(x) = 0$ for every x in $[0, 1]$. If we add f and g, we get $f(x) + g(x) = [f + g](x) = 0$ for all x in $[0, 1]$ (as $f(x) = 0$ and $g(x) = 0$ in $[0, 1]$, their sum on this segment is also zero). Now, as for the inverse $f \in H$ and then $f(x) = 0$ for all $x \in [0, 1]$. But then, also $-f(x) = -0 = 0$, for all $x \in [0, 1]$. And, $f(x) + (-f(x)) = \mathcal{O}(x)$, which is a

neutral element for addition of functions in G. in conclusion, H is a subgroup of G.

10. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(-x) = -f(x)\}$. Again, it's obvious that $H \subset G$ (through definition: H is only strengthening of G by adding more conditions). Let f, g be in H. Then, $f(-x) = -f(x)$ and $g(-x) = -g(x)$. Now, if we take $[f+g](-x) = f(-x)+g(-x) = -f(x)-g(x) = -(f(x)+g(x)) = -[f+g](x)$, so if $f, g \in H$ then $[f+g] \in H$, therefore, H is closed under addition. Take $f \in H$. It's inverse should be some $g \in H$ such that $f(x) + g(x) = 0$, i.e. $g(x) = -f(x)$, but $-f(x) = f(-x)$, so for every $f \in H$ there is $(-f) \in H$ and H is closed with respect to inverses. H is a subgroup of G.

11. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(x + n\pi) = f(x), \ \forall n \in \mathbb{Z}, \ \forall x \in \mathbb{R}\}$. Again, $H \subset \mathcal{F}(\mathbb{R})$. Take $f, g \in H$ and we will show that $[f+g] \in H$. Indeed, $[f+g](x) = f(x) + g(x) = f(x + n\pi) + g(x + n\pi) = [f + g](x + n\pi)$, $\forall n \in \mathbb{Z}$. H is closed under function addition, but is it closed with respect to inverses? Obviously, $f(x) + (-f(x)) = \mathcal{O}(x)$. Now, if $f \in H$ then $-f \in H$, as $f(x) = f(x + n\pi)$, and multiplying it by (-1) yields $-f(x) = -f(x + n\pi)$, for all $n \in \mathbb{Z}$. Therefore, H is a subgroup of G.

12. $G = (\mathcal{C}(\mathbb{R}), +)$, $H = \left\{f \in \mathcal{C}(\mathbb{R}) : \ \int_0^1 f(x)dx = 0\right\}$. Obviously $H \subset \mathcal{C}(\mathbb{R})$. Now, let $f, g \in H$ and observe $[f+g](x) = f(x)+g(x)$. We will integrate both sides of equation to get $\int_0^1 [f + g](x)dx = \int_0^1 (f(x) + g(x))dx = \int_0^1 f(x)dx + \int_0^1 g(x)dx = 0 + 0 = 0$. So, $[f + g] \in H$. Now, as for the inverse, for every $f \in H$ there must be $-f \in H$. But, $-f(x) = \int_0^1 (-f(x))dx = -\int_0^1 f(x)dx = -0 = 0$, so $-f \in H$ and H is closed under addition and in respect to inverses: H is a subgroup of G.

13. $G = (\mathcal{D}(\mathbb{R}), +)$, $H = \left\{f \in \mathcal{D}(\mathbb{R}) : \ \frac{df}{dx} = c, \ c \in \mathbb{R}\right\}$. It's easy to see that $H \subset \mathcal{D}(\mathbb{R})$. Take $f, g \in H$. Then, $[f + g](x) = f(x) + d(x)$. Applying differential operator on this equation, we get $\frac{d[f+g]}{dx}(x) = \frac{d}{dx}(f(x) + g(x)) = \frac{df}{dx}(x) + \frac{dg}{dx}(x) = c_f + c_g = c_{f+g}$, $c_{f+g} \in \mathbb{R}$. Now, $-f(x) = \frac{d}{dx}(-f(x)) = -\frac{df}{dx}(x) = -c = c_{-f}$, $c_{-f} \in \mathbb{R}$. Therefore, H being closed under function addition and with respect to inverses, H is a subgroup of G.

14. $G = (\mathcal{F}(\mathbb{R}), +)$, $H = \{f \in \mathcal{F}(\mathbb{R}) : \ f(x) \in \mathbb{Z}, \ \forall x \in \mathbb{R}\}$. Again, $H \subset \mathcal{F}(\mathbb{R})$. Let f, g be in H and let us consider $(f + x)(x) = f(x) + g(x)$. But, $f(x) \in \mathbb{Z}$ and $g(x) \in \mathbb{Z}$ for all $x \in \mathbb{R}$. Therefore their sum is also in $\mathbb{Z}$ and $(f + x)(x) \in \mathbb{Z}$, for every $x \in \mathbb{R}$, and so $[f + g] \in H$. Now, $f(x)$ being in $\mathbb{Z}$, then $-f(x)$ is also obviously in $\mathbb{Z}$, for every $x \in \mathbb{R}$, and therefore in H. H is a subgroup of G.

Problem. Let G be an Abelian group.

1. If $H = \{x \in G : \ x = x^{-1}\}$, that is, H consists of all the elements of G which are their own inverses, prove that H is a subgroup of G.

2. Let n be a fixed integer, and let $H = \{x \in G : \ x^n = e\}$. Prove that H is a subgroup of G.

3. Let $H = \{x \in G : \ x = y^2, \ y \in G\}$; that is, let H be the set of all the elements of G which have a square root. Prove that H is a subgroup of G.

4. Let H be a subgroup of G, and let $K = \{x \in G : x^2 \in H\}$. Prove that K is a subgroup of G.

5. Let H be a subgroup of G, and let K consist of all the elements x in G such that some power of x is in H. That is, $K = \{x \in G : x^n \in H, \ n > 0, \ n \in \mathbb{Z}\}$. Prove that K is a subgroup of G.

6. Suppose H and K are subgroups of G, and define HK as follows:

$$HK = \{xy : \ x \in H \text{ and } y \in K\}.$$

   Prove that HK is a subgroup of G.

Solution.

1. *If $H = \{x \in G : \ x = x^{-1}\}$, that is, H consists of all the elements of G which are their own inverses, prove that H is a subgroup of G.* Obviously $H \subseteq G$. Now if we take $x, y \in H$, then, $x^2 = e$ and multiplying it by y^2 on the left gives us $x^2y^2 = y^2$. But, $y^2 = e$, so $x^2y^2 = e$. Rearranging the elements using commutativity, we get $(xy)(xy) = e$, i.e. their product is the inverse of itself, so it must be in H. This of course, would not work, generally, if G were not Abelian; we could not rearrange the elements in such manner. And, H is, naturally, closed in respect to inverses by definition. Therefore, H is a subgroup of G.

2. *Let n be a fixed integer, and let $H = \{x \in G : \ x^n = e\}$. Prove that H is a subgroup of G.* We can easily see that $H \subset G$. Now, let $x, y \in H$. Obviously $x^n = e$, but if we multiply it on the right (or left, doesn't matter, it's Abelian) by y^n, we get $x^ny^n = y^n$. But, $y^n = e$, so we have $x^ny^n = e$. By previously proven property, we have $(xy)^n = x^ny^n$ and so $(xy)^n = e$. So their product xy is such that $(xy)^n = e$ and it must be in H. Again, take $x \in H$, and we have $x^n = e$. Now, we have $xx^{n-1} = e$, therefore, the inverse of x is x^{n-1}. Is it in H? Obviously $e^n = (x^n)^n = e$. Now, $(xx^{n-1})^n = e$. Then, $x^n(x^{n-1})^n = e$ and, as $x^n = e$, it's $(x^{n-1})^n = e$, so $x^{n-1} \in H$ and H is a subgroup of G.

3. *Let $H = \{x \in G : \ x = y^2, \ y \in G\}$; that is, let H be the set of all the elements of G which have a square root. Prove that H is a subgroup of G.* Again, $H \subset G$

by definition. If we take $x, y \in H$, then $x = z^2$ and $y = w^2$, for some $w, z \in G$. Their product is then $xy = z^2w^2$, and by using $(zw)^2 = z^2w^2$ (which would not hold if the group was not Abelian in nature), we have $xy = (zw)^2$. In conclusion product xy has a square root $zw \in G$ so it must be in H. If $x \in H$ then $x = y^2$ for some $y \in G$. Now, y has an inverse in G and that is y^{-1}. So, multiplying this by $(y^{-1})^2$ (which must be also in G, as product $y^{-1}y^{-1} \in G$) it has to be $x(y^{-1})^2 = e$. So, the inverse of x is $(y^{-1})^2$ (the squared inverse of it's square root). But is $(y^{-1})^2$ in H? Obviously it is, as H contains all elements of G that have a square root in G and, square root of $(y^{-1})^2$ is obviously y^{-1}. And, again, H is a subgroup of G.

4. *Let H be a subgroup of G, and let $K = \{x \in G : x^2 \in H\}$. Prove that K is a subgroup of G.* Notice that $K \subset G$. If $x, y \in K$, then $x^2 \in H$ and $y^2 \in H$. As, H is a group it's closed under multiplication, therefore product x^2y^2 is in H. But, that product is $x^2y^2 = (xy)^2 \in H$ (for this commutativity is necessary). As $x, y \in K$, also $x, y \in G$. So $(xy) \in G$, as G is closed under multiplication. And, as $(xy) \in G$ and $(xy)^2 \in H$, by definition of K, then $(xy) \in K$. Now, is inverse of $x \in K$ in K? Obviously, $x^2 \in H$ and, due to H being a group, there it has an inverse and it's $(x^2)^{-1} \in H$. That is, $(x^{-1})^2 \in H$. Of course, x^{-1} is in G, as $x^{-1} \in H \subset G$, so, because it's also $(x^{-1})^2 \in H$, it's also $x^{-1} \in K$. Therefore, K is closed with respect to inverses and it's true that K is a subgroup of G.

5. *Let H be a subgroup of G, and let K consist of all the elements x in G such that some power of x is in H. That is, $K = \{x \in G : x^n \in H,\ n > 0,\ n \in \mathbb{Z}\}$. Prove that K is a subgroup of G.* Obviously, $K \subset G$. Take $x, y \in H$ and then it's $x^n, y^n \in H$. Yet, H is a group, so $x^n y^n \in H$, i.e. $(xy)^n \in H$ (we cannot claim this without commutativity). As $x, y \in K \subset G$, and G is a group, therefore closed under multiplication, it's $(xy) \in G$. Combining that fact with $(xy)^n \in H$, obviously $(xy) \in K$. Therefore, K is closed under multiplication. Now, if $x \in K$, then $x^n \in H$. As H is a group, it's closed with respect to inverses, so it's also that $(x^n)^{-1} \in H$. That is, $(x^{-1})^n \in H$. As $x^{-1} \in H \subset G$, it's also $x^{-1} \in G$. Now it's obvious that $x^{-1} \in K$ and K is closed with respect to inverses, thus proving that K is a subgroup of G.

6. *Suppose H and K are subgroups of G, and define HK as follows:*

$$HK = \{xy :\ x \in H \text{ and } y \in K\}.$$

Prove that HK is a subgroup of G. If $(xy) \in HK$, then, due to $x \in H \subset G$, it's $x \in G$ and, by the same logic, as $y \in K \subset G$, it's also $y \in G$. G is closed under multiplication, so $(xy) \in G$. That proves that $HK \subseteq G$. Now, take

some $(ab) \in HK$ and $(cd) \in HK$. Obviously, $a, c \in H$ and $b, d \in K$. Now, as $HK \subseteq G$, $(ab), (cd) \in G$. As G is a group it's closed under multiplication, so $(ab)(cd) \in G$. By using associativity and commutativity (necessary for this one) we can rearrange elements to get $(ab)(cd) = (ac)(bd) \in G$. Now, as $a, c \in H$, their product is in H, i.e. $(ac) \in H$. Also, $(bd) \in K$. Now, as $(ac)(bd) \in G$, $(ac) \in H$ and $(bd) \in K$, obviously $(ac)(bd) \in HK$. But as $(ac)(bd) \in G$, then it's $(ac)(bd) = (ab)(cd) \in G$, and those product being equal, obviosly also $(ab)(cd) \in HK$. Now, if we take $xy \in HK$, then $x^{-1} \in H$ and $y^{-1} \in K$. As both of these groups are subgroups of G, and G is closed under multiplication, we have $x^{-1}y^{-1} \in G$ such that $x^{-1} \in H$ and $y^{-1} \in K$. So, $x^{-1}y^{-1} \in HK \subset G$. In G, it's $x^{-1}y^{-1} = (xy)^{-1} \in G$. Those expressions being equal, i.e. it's the one and the same element, it's $(xy)^{-1} \in HK$, which is inverse of $(xy) \in HK$. Therefore, HK is a subgroup of G.

Problem. Let G be a group.

1. If H and K are subgroups of G, prove that $H \cap K$ is a subgroup of G.

2. Let H and K be subgroups of G. Prove that if $H \subseteq K$, then H is a subgroup of K.

3. By the *center* of a group G we mean the set of all the elements of G which commute with every element of G, that is,

$$C = \{a \in G : \ ax = xa, \ \forall x \in G\}.$$

   Prove that C is a subgroup of G.

4. Let $C' = \{a \in G : \ (ax)^2 = (xa)^2, \ \forall x \in G\}$. Prove that C' is a subgroup of G.

5. Let G be a *finite* group, and let S be a nonempty subset of G. Suppose S is closed with respect to multiplication. Prove that S is a subgroup of G.

6. Let G be a group and $f : G \to G$ a function. A *period* of f is any element a in G such that $f(x) = f(ax)$ for every $x \in G$. Prove that the set of all the periods of f is a subgroup of G.

7. Let H be a subgroup of G, and let $K = \{x \in G : \ xax^{-1} \in H \text{ iff } a \in H\}$. Prove:

   (a) K is a subgroup of G.

   (b) H is a subgroup of K.

8. Let G and H be groups, and $G \times H$ their direct product.

(a) Prove that $\{(x, e) : \ x \in G\}$ is a subgroup of $G \times H$.

(b) Prove that $\{(x, x) : \ x \in G\}$ is a subgroup of $G \times G$.

Solution.

1. *If H and K are subgroups of G, prove that $H \cap K$ is a subgroup of G.* Obviously $(H \cap K) \subseteq G$. If we take $x, y \in H \cap K$, then x and y are both in H and K. Now, as H is a subgroup of G and $x, y \in H$, then $xy \in H$. Same thing goes for K; it's also a subgroup of G, therefore it's closed with respect to multiplication and $xy \in K$. So, the following conjuction is true: $xy \in H$ and $xy \in K$, which, by definition of set intersection tells us that $xy \in H \cap K$. So $H \cap K$ is closed under multiplication. Take $x \in H \cap K$. Then, as $x \in H$ and $x \in K$, it has an inverse in $x^{-1} \in H$ and $x^{-1} \in K$, that is, $x^{-1} \in H \cap K$. So, $H \cap K$ is a subgroup of G.

2. *Let H and K be subgroups of G. Prove that if $H \subseteq K$, then H is a subgroup of K.* Let $x, y \in H$. As H is a subgroup of G, then $xy \in H$ and $xy \in K$. Now, if $x \in H$, it has an inverse $x^{-1} \in H$. But, also $x^{-1} \in K$ as H is a subset of K. So, H is a subset of K, it's closed with respect to multiplication and inverses, therefore H is a subgroup of K.

3. *By the center of a group G we mean the set of all the elements of G which commute with every element of G, that is,*

$$C = \{a \in G : \ ax = xa, \ \forall x \in G\}.$$

Prove that C is a subgroup of G. Notice that $C \subseteq G$. If we take some $a, b \in C$, then $ax = xa$ and $bx = xb$, for all $x \in G$. Now, as $x \in G$, and G is a group, then $x^{-1} \in G$. We can say that $a = xax^{-1}$ and $b = xax^{-1}$, for all $x \in G$. Let's take their product, $ab = xax^{-1}xbx^{-1}$, that is, $ab = xabx^{-1}$. Multiplying that by x^{-1} gives us $(ab)x = x(ab)$. As (ab) obviously commute with all $x \in G$, then $(ab) \in C$. Therefore, C is closed under multiplication. Take $a \in C$. Then, $ax = xa$ for all $x \in G$. Now, as $a \in G$, it has an inverse in G, and that is $a^{-1} \in G$. So we can multiply the previos equation with a^{-1} on the left and get $x = a^{-1}xa$. Multiplying it by $(xa)^{-1}$ on the right gives us $x(xa)^{-1} = a^{-1}$. We multiply it again by x^{-1} on the left and get $(xa)^{-1} = x^{-1}a^{-1}$. Obviously, that is $a^{-1}x^{-1} = x^{-1}a^{-1}$. We can multiply this again by x on the left and on the right to get $xa^{-1}x^{-1}x = xx^{-1}a^{-1}x$, i.e. $xa^{-1} = a^{-1}x$, for all $x \in G$. So $a^{-1} \in G$ commutes with all $x \in G$ and therefore must be in C. Thus, we have proved that C is a subgroup of G.

4. *Let $C' = \{a \in G : \ (ax)^2 = (xa)^2, \ \forall x \in G\}$. Prove that C' is a subgroup of G.* Obviously, $C' \subseteq G$. If $a \in C'$ then $(ax)^2 = (xa)^2$. Multiplying this by x on the left gives us $x(ax)^2 = x(xa)^2$. Rearranging elements, gives us $xaxax = x(xa)^2$, and that is $(xa)^2x = x(xa)^2$, for every $x \in G$, which means that $C' \subseteq C$. If we take $a, b \in C'$, then, a, b are also in C and $ab \in C$. So it must be that $(ab)x = x(ab)$, for all $x \in G$. Multiplying that by $(ab)x$ gives us $(abx)^2 = (xab)(abx)$. But, $(abx) = (xab)$, so we have $(abx)^2 = (xab)^2$, for all $x \in G$, and therefore such product must be in C'. So C' is closed with respect to multiplication. Now, for the inverses, it must be that if $a \in C'$, then $a \in C$. And, as C is a subgroup of G, it must be that $a^{-1} \in C$, and $a^{-1}x = xa^{-1}$. Multiplying that on the right by $a^{-1}x$ gives us $(a^{-1}x)^2 = (xa^{-1})(a^{-1}x)$. But, again, $(a^{-1}x) = (xa^{-1})$, which yields $(a^{-1}x)^2 = (xa^{-1})^2$, for all $x \in G$, and such expression tells us that a^{-1} must be in C'. So, C' is a subgroup of C and G.

5. *Let G be a finite group, and let S be a nonempty subset of G. Suppose S is closed with respect to multiplication. Prove that S is a subgroup of G.* Suppose $S = \{a_1, \ldots, a_n\}$ and $|S| = n$. Also, $S \subseteq G$, so for every $a, b, c \in S$ they are in G. We have the same operation on S as on G. And, as G is a group, for every $a, b, c \in S \subseteq G$ it holds associativity: $a(bc) = (ab)c$. Now, we will take some $a_i \in S$. As S is closed under multiplication, it must be that every product $a_ia_1, a_ia_2, \ldots, a_ia_n$ is defined and is in S. There are n such products, and every one of them would need to be some $a_j \in S$. Now, we cannot have, by a previos problem, that two such products give the same element, i.e. take $a_ia_1 = a_j$ and $a_ia_2 = a_j$, then $a_ia1 = a_ia_2$ and we would get $a_1 = a_2$ which is a contradiction to our premise that all $a_i \in S$ are distinct (and that order of S is n). Now, if $a_ia_i = a_i$ then, as a_ia_i in S and by that in G, and then $a_ia_i = a_i$ can be multiplied by $a_i^{-1} \in G$, giving $a_i = e$. Now, if $a_ia_i = a_k$ for some k, then a_i must appear as a result of some other product, say a_j, and then $a_ia_j = a_i$ for some j, and, as $a_ia_j \in S \subseteq G$, then it must be that $a_ia_j = a_i \in G$. Then $a_i^{-1} \in G$ and it must be that $a_j = e$. Now, that only shows that a_j is a right neutral element in S. But, if it was that a_ja_i equals some $a_k \in S$, taking a_j^{-1} in G, it would be, as $a_j = e$ in G, that $a_j^{-1} = e^{-1} = e$. That would mean that $a_i = a_j^{-1}a_k$ is actually $a_i = a_k$, which is a contradiction. Therefore, there is a neutral element in S. As there is a neutral element say $a_j = e$. Then, for every product $a_ia_k \in S$, for a fixed a_i, we must have use all the elements and use them only once as a result of a product. And it will happen that $a_ia_k = e$ for some a_k, making a_k the left inverse of a_i. But, as $a_k \in G$, it is also $a_ia_k = e$ in G. If it were that $a_ka_j = e$, then it would mean that $a_ia_k = a_ka_j$. Multiplying this by a_j would give $a_ia_ka_j = a_ka_ja_j$, that is, $a_i = a_ka_ja_j$. But, as $a_ka_j = e$, then $a_i = a_j$, so, a_k must be also both the left and right inverse of a_i, and therefore the inverse of a_i. Same reasoning goes for

every a_i. Thus, S is a subgroup of G.

Comment. Notice that this does not necessarily hold if G is infinite, as there might be no breach of double use in multiplication table (if it can even exist for am infinite group). For example take $(\mathbb{Q}\backslash\{0\}, \cdot)$ which is a (commutative) group. Now, $\mathbb{N} \subset \mathbb{Q}$ and $(\mathbb{N}, \cdot)$ is closed with respect to multiplication, but there are no multiplicative inverses for any $x \in \mathbb{N}$ except when $x = 1$.

6. *Let G be a group and $f : G \to G$ a function. A period of f is any element a in G such that $f(x) = f(ax)$ for every $x \in G$. Prove that the set of all the periods of f is a subgroup of G.* Let $P = \{a \in G : \ f(x) = f(ax), \ \forall x \in G\}$. Obviously $P \subseteq G$. Now, if $a, b \in P$, then $f(x) = f(ax)$ and $f(x) = f(bx)$ for all $x \in G$. Now, obviously $f(x) = f(ax)$. If we take $p = (ax)$, then $f(p) = f(bp)$, for all $x \in G$, that is $f(ax) = f(bax)$, which is in turn equal to $f(x)$, as $f(ax) = f(x)$. That is, $f(x) = f(bax)$, for all $x \in G$ which means that $ba \in G$. Now if we take $a \in P$, we'll check if $a^{-1} \in G$ satisfies conditions of set P. Take $f(a^{-1}x)$. If we substitute $p = (a^{-1}x)$, as $a^{-1}x \in G$ we have $f(p) = f(ap)$, and that is $f(a^{-1}x) = f(aa^{-1}x) = f(x)$, for all $x \in G$. Therefore, $a^{-1} \in P$ and P is a subgroup of G.

7. *Let H be a subgroup of G, and let $K = \{x \in G : \ xax^{-1} \in H \text{ iff } a \in H\}$. Prove:*

   (a) *K is a subgroup of G.* Obviously $K \subseteq G$. Now, we take $x, y \in K$ and check whether their product is in K. Also, we will need some $a \in H$. Because $x \in K$, it must be true that $xax^{-1} \in H$. Now, we see that $xax^{-1} \in H$ and if we take some $y \in K$, then $yxax^{-1}y^{-1} \in H$, i.e. $yxa(yx)^{-1} \in H$. Also, $x, y \in G$ (by definition of K) and so it's $yx \in G$, too. And all that means that $yx \in K$. That is, the product of $x, y \in K$ is again in K. Now, for some $a \in H$ and $x \in K$ it's $xax^{-1} \in H$. As H is a group it means that $x^{-1}a^{-1}x \in H$. That can be written as $x^{-1}a^{-1}(x^{-1})^{-1}$. Note that $x^{-1} \in G$ as H is a subgroup of G. And, as $a^{-1} \in H$ (it's a subgroup, so it's closed with respect to inverses), it means that $x^{-1} \in K$. Therefore K is a subgroup of G.

   (b) *H is a subgroup of K.* We need to show that if $a \in H$ then $a \in K$. Now, for some $x \in K$ it's $xax^{-1} \in H$. As H is a group, and it's closed under multiplication and inverses, it's also $axax^{-1}a^{-1} \in H$. And, as $xax^{-1} \in H$, and a and a^{-1} are also in G (as H is a subgroup), it means that $a \in K$. Therefore $H \subseteq K$. Now, the other two properties have already been shown in a previous problem, they are independent of the now-known fact that H is a subset of K. Therefore H is a subgroup of K.

8. *Let G and H be groups, and $G \times H$ their direct product.*

(a) *Prove that* $\{(x,e):\ x\in G\}$ *is a subgroup of* $G\times H$. Let $S=\{(x,e):\ x\in G\}$ and, as $x\in G$ and $e\in H$, then $S\subseteq G\times H$. Now, take $(x,e),(y,e)\in S$, where $x,y\in G$. Their product is (xy,e). As $x,y\in G$, then also $xy\in G$. In conclusion, $(xy,e)\in S$ and S is closed under multiplication. If we take $(x,e)\in S$, for $x\in G$, then, $(x^{-1},e)\in S$ because $x^{-1}\in G$. We didn't check $e\in H$ specially as, $e^{-1}=e$ and $ee=e$. Therefore, S is closed with respect to inverses. S is a subgroup of $G\times H$.

(b) *Prove that* $\{(x,x):\ x\in G\}$ *is a subgroup of* $G\times G$. Again, let $S=\{(x,x):\ x\in G\}$. Obviously $S\subseteq G\times G$. If we take $(x,x),(y,y)\in S$, then $(xy,xy)\in S$, as, because $x,y\in G$, also $xy\in G$. Therefore, S is closed under multiplication. Now, take $(x,x)\in S$. Obviously $(x^{-1},x^{-1})\in S$, as $x^{-1}\in G$ for every $x\in G$. S is a subgroup of $G\times G$.

Problem. Let G be a group, A it's subgroup and $B\subset G$ such that $A\cap B=\emptyset$. Prove that B cannot be a subgroup of G (in any case).

Solution. As A is a subgroup of G, it is closed with respect to inverses and multiplication. Therefore for every $a\in A$ it follows that $a^{-1}\in A$, and so $aa^{-1}\in A$, which is $aa^{-1}=e\in A\subset G$. As $A\cap B=\emptyset$ it implies that, as $e\in A$, it cannot be that $e\in B$. Set B is missing, therefore, a neutral element, and cannot be closed with respect to multiplication, even if every element in it contained it's inverse. Thus, B cannot be a subgroup.

Remark. A result of a previous problem tells us that, considering family of sets $\{S_i\}_{i\in\lambda}$, where $\lambda\neq\emptyset$, and $S_i\subseteq G$, where G is a group, a necessary condition for all S_i to be subgroups of G is that

$$\bigcap_{i\in\lambda}S_i\neq\emptyset.$$

Problem. Prove that $SO(n)\in\mathbb{R}^{n\times n}$, where $SO(n)$ (special orthogonal group) is the set of all orthogonal matrices with additional property that $\det A=1$, is a subgroup of $O(n)$.

Solution. Obviously $SO(n)\subset O(n)$, by definition. Using the fact that $\det AB=\det A\det B$, we can see that for all $A,B\in SO(n)$ it's $\det A=1$ and $\det B=1$, but also $\det AB=\det A\det B=1\cdot 1=1$. Therefore $AB\in SO(n)$ so it's closed with respect to matrix multiplication. Now, for $A\in SO(n)$ we need to check that $A^T\in SO(n)$. We know that $\det A=1$ and $\det I=1$, so taking $\det AA^T=\det I$, i.e. $\det A\det A^T=\det I$, it must be that $\det A^T=1$. Therefore $A^T\in SO(n)$, which

makes special orthogonal group closed with respect to inverses and by that a subgroup of $O(n)$.

Generators of Groups

Definition. Let G be a group. Now, for some finite $X \subseteq G$, $X \neq \emptyset$, we define a set $S \subseteq G$ which contains all the possible products of $x \in X$ and $x^{-1} \in G$. We say that S is a **subgroup generated by** elements $x \in X \subseteq G$.

Remark. We make a mention-use distinction for the definition above in the analytic way of thought. We said that S is a *subgroup* of G in the *mention-sense* (*subgroup* is just part of a name for S now), but in the following theorem we are going to prove it to be an actual subgroup in the *use-sense* (S is actually a subgroup now).

Theorem. Set S defined as in previous definition, with operation inherited from group G, is a subgroup of G.

Proof. By definition, for finite $X \subseteq G$, S contains all the possible products of elements in X. Now, is $S \subseteq G$? Whatever elements $a_1, \ldots, a_n, a_1^{-1}, \ldots, a_n^{-1} \in X$ we take, their arbitrary product is in S. But, as $X \subseteq G$, then all these elements are in G, and, as G is a group, their arbitrary product is also in G. Then, S is by definition closed under multiplication and inverses. Whatever product we take, we can use the fact that

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}.$$

So, as $S \subseteq G$, and S being closed under multiplication and with respect to inverses, S is a subgroup of G, and by itself, a group.

□

Remark. We can also do the reverse thing, and for some finite $X \subseteq G$ define subgroup S generated by elements from $X \subseteq G$.

Definition. If S is a subgroup generated by a single element $a \in G$, we say that S is a **cyclic subgroup** of G and we say that a is its **generator**. We denote S by $\langle a \rangle$.

Definition. A set of equations, involving only generators and their inverses, are called **defining equations** for G if if these equations completely determine the multiplication table of G.

Problem. List all the cyclic subgroups of $\mathbb{Z}_{10}$.

Solution. Cyclic subgroup must be a subgroup generated by a single $a \in \mathbb{Z}_{10}$. We

have 10 cases (for $0, 1, \ldots, 9$), which we will list. We need not check whether they are really subgroups, the previos theorem guarantees us that they will be subgroups; every subgroup generated by some arbitrary elements in it's overlying group is a subgroup. So, a cyclic subgroup is also a subgroup[14]. The list is (the sets are "sorted" in the way the operation is applied):

- $\langle 0 \rangle = \{0\}$;
- $\langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$;
- $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$;
- $\langle 3 \rangle = \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\}$;
- $\langle 4 \rangle = \{4, 8, 2, 6, 0\}$;
- $\langle 5 \rangle = \{5, 0\}$;
- $\langle 6 \rangle = \{6, 2, 8, 4, 0\}$;
- $\langle 7 \rangle = \{7, 4, 1, 8, 5, 2, 9, 6, 3, 0\}$;
- $\langle 8 \rangle = \{8, 6, 4, 2, 0\}$;
- $\langle 9 \rangle = \{9, 8, 7, 6, 5, 4, 3, 2, 1, 0\}$.

Problem. Show that $\mathbb{Z}_{10}$ is generated by 2 and 5.

Solution. We need to show that every element in $\mathbb{Z}_{10}$ can be obtained by adding 2's and 5's. Now, obviously $5 + 5 = 0$. Then, $2 + 2 + 2 + 5 = 1$. Now, let's denote $a = 2 + 2 + 2 + 5$. Then, every other element can be obtained by adding a with itself. $2 = a + a$, $3 = a + a + a$ and so on. Therefore, $\mathbb{Z}_{10}$ is generated by 2 and 5.

Problem. Describe the subgroup of $\mathbb{Z}_{12}$ generated by 6 and 9.

Solution. First, we have two sets, $\langle 6 \rangle = \{6, 0\}$ and $\langle 9 \rangle = \{9, 6, 3, 0\}$. Combining these elements together, we see that the sum of any two numbers from both sets is already in both sets. Therefore, we have the subgroup with underlying set $\{0, 3, 6, 9\}$.

Problem. Describe the subgroup of $\mathbb{Z}$ generated by 10 and 15.

Solution. All the elements of that subgroup will be of the form $10k + 15l$, where $k, l \in \mathbb{Z}$. That would mean that $5(2k + 3l)$ is the form of all elements; they will all be

[14]Note the *use-mention* distinction of the word subgroup again.

multiples of 5. Also note that $2k + 3l$ ranges through all elements of $\mathbb{Z}$, as, we could take $a = -2 + 3 = 1$ and then generate them all as $a + a = 2$, $a + a + a = 3$, and so on. Same holds for negative numbers, we can take $-a$ and get them all. So, multiplying all elements of $\mathbb{Z}$ by 5 gives us all elements that are divisible by 5. That is the set $S = \{0, 5, -5, 10, -10, \ldots\}$, i.e. $S = \{n \in \mathbb{Z} : \ n = 5k, \ \forall k \in \mathbb{Z}\}$.

Problem. Show that $\mathbb{Z}$ is generated by 5 and 7.

Solution. All the combinations of 5's and 7's will be of the form $5k + 7l$, for all $k, l \in \mathbb{Z}$. Now, taking $a = 3 \cdot 7 + 4 \cdot (-5) = 1$ (best to view multiplication here not as multiplication qua multiplication, but as shortened addition), we can see, again that we can get all the elements by adding a and $-a$ with themselves. Note that $0 = a - a$, or more simply $5 - 5$, $7 - 7$, etc.

Problem. Show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group.

Solution. All it's elements can be generated by $(1, 2) \in \mathbb{Z}_2 \times \mathbb{Z}_3$. That is, $\langle (1, 2) \rangle = \{(1, 2), (0, 1), (1, 0), (0, 2), (1, 1), (0, 0)\}$. We can see that this set is actually equal to the observed set. This group is the subset of $\mathbb{Z} \times \mathbb{Z}$, and as it is cyclic, it's a subgroup of the former and, therefore, a group.

Problem. Show that $\mathbb{Z}_3 \times \mathbb{Z}_4$ is a cyclic group.

Solution. This time, we can take $(1, 1)$ to be generator. We could have also taken $(1, 2)$ and $(2, 3)$. Now,

$$\langle (1, 1) \rangle = \{(1, 1), (2, 2), (0, 3), (1, 0), (2, 1), (0, 2), (1, 3), (2, 0), (0, 1), (1, 2), (2, 3), (0, 0)\}.$$

Notice that we ran through all $3 \cdot 4 = 12$ elements. As $\mathbb{Z}_3 \times \mathbb{Z}_4 \subset \mathbb{Z} \times \mathbb{Z}$, and as $\mathbb{Z}_3 \times \mathbb{Z}_4$ is cyclic, it's a subgroup of $\mathbb{Z}^2$, and then a group by itself.

Problem. Show that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not a cyclic group, but is generated by $(1, 1)$ and $(1, 2)$.

Solution. We see that $\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(0, 0), (1, 0), (0, 1), (1, 1), (0, 2), (1, 2), (0, 3), (1, 3)\}$. Now, it cannot be generated by a single element, as, for potential generators of the form $(0, y)$ we never get a different ordinate (always $0 + 0 = 0$). Now, following the same logic, we cannot also take elements of the form $(x, 0)$, we never get a different abscise. The only ones left are $(1, 1)$, $(1, 2)$ and $(1, 3)$. But, it cannot be generated by $(1, 1)$

only, as we would be getting $(0,2)$, $(1,3)$, $(0,0)$ and $(1,1)$ over and over. Same thing goes for $(1,2)$, as we would have $(0,0)$ and $(1,2)$; for $(1,3)$ we have $(0,2)$, $(1,1)$, $(0,0)$ and then $(1,3)$ again. Therefore $\mathbb{Z}_3 \times \mathbb{Z}_4$ is not a cyclic group (it has to be generated by a *single* element in order to be cyclic). But, we can see that combining $(1,1)$ and $(1,2)$, so that $a = (1,1)+(1,1)+(1,2) = (1,0)$ and $b = (1,2)+(1,1)+(1,1)+(1,1) = (0,1)$, would give us all the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$ (as we run through all ordinates by applying a's and through all absices by applying b's).

Problem. Suppose a group G is generated by two elements a and b. If $ab = ba$, prove that G is Abelian.

Solution. Now, let's take some $c, d \in G$ such that c and d are combinations of products and inverses of a and b. If c were of the form $c = a^n b^m a^p b^q$, we could rearrange elements using $ab = ba$ to get c of the form $c = a^u b^v$. The same can be done with $d = a^t b^s$. Now, the product can also be rearranged so that $cd = a^u b^v a^t b^s = a^t b^s a^u b^v = dc$. Therefore, G is Abelian.

Problem. Let G be the group $\{e, a, b, b^2, ab, ab^2\}$ whose generators satisfy $a^2 = e$, $b^3 = e$, $ba = ab^2$. Write the table of G.

Solution. We will only present the finished table (be reminded that we can use the helpful fact that every element must appear only once in a row):

$\cdot$	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ba	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

Problem. Let G be the group $\{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ whose generators satisfy $a^2 = e$, $b^4 = e$, $ba = ab^3$. Write the table of G[15].

Solution. The finished table is:

[15]This group is called *dihedral group* D_4.

$\cdot$	e	a	b	b^2	b^3	ab	ab^2	ab^3
e	e	a	b	b^2	b^3	ab	ab^2	ab^3
a	a	e	ab	ab^2	ab^3	b	b^2	b^3
b	b	ab^3	b^2	b^3	e	a	ab	ab^2
b^2	b^2	ab^2	b^3	e	b	ab^3	a	ab
b^3	b^3	ab	e	b	b^2	ab^2	ab^3	a
ab	ab	b^3	ab^2	ab^3	a	e	b	b^2
ab^2	ab^2	b^2	ab^3	a	ab	b^3	e	b
ab^3	ab^3	b	a	ab	ab^2	b^2	b^3	e

Problem. Let G be the group $\{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ whose generators satisfy $a^4 = e$, $a^2 = b^2$, $ba = ab^3$. Write the table of group[16] G.

Solution. The table is:

$\cdot$	e	a	b	b^2	b^3	ab	ab^2	ab^3
e	e	a	b	b^2	b^3	ab	ab^2	ab^3
a	a	b^2	ab	ab^2	ab^3	b^3	e	b
b	b	ab^3	b^2	b^3	e	a	ab	ab^2
b^2	b^2	ab^2	b^3	e	b	ab^3	a	ab
b^3	b^3	ab	e	b	b^2	ab^2	ab^3	a
ab	ab	b	ab^2	ab^3	a	b^2	b^3	e
ab^2	ab^2	e	ab^3	a	ab	b	b^2	b^3
ab^3	ab^3	b^3	a	ab	ab^2	e	b	b^2

Problem. Let G be the *commutative* group $\{e, a, b, c, ab, bc, ac, abc\}$ whose generators satisfy $a^2 = b^2 = c^2 = e$. Write the table of G.

Solution. The table is as follows:

$\cdot$	e	a	b	c	ab	bc	ac	abc
e	e	a	b	c	ab	bc	ac	abc
a	a	e	ab	ac	b	abc	c	bc
b	b	ab	e	bc	a	c	abc	ac
c	c	ac	bc	e	abc	b	a	ab
ab	ab	b	a	abc	e	ac	bc	c
bc	bc	abc	c	b	ac	e	ab	a
ac	ac	c	abc	a	bc	ab	e	b
abc	abc	bc	ac	ab	c	a	b	e

[16] This group is called the *quaternion group*.

Functions

Definition. Let A and B be sets. A **function**[17] from set A to set B is an ordered triple (f, A, B), where f is a rule which *for each* element of A assigns *a unique* (one and only one) element in B. We denote the function by $f : A \to B$. We call set A **domain** and B **codomain**.

Definition. We say that a function $f : A \to B$ is **injective**[18] if each element of B is the image of exactly one element in A.

Definition. Let $f : A \to B$ be a function. The set

$$\operatorname{ran}(f) = \{y \in B : \ (\exists x \in A)\,(y = f(x))\}$$

is called the **image** (or range) of the function $f : A \to B$. We say that the function $f : A \to B$ is **surjective**[19] if $\operatorname{ran}(f) = B$.

Lemma. Let $f : A \to B$ be a function. Then, $\operatorname{ran}(f) \subseteq B$.

Proof. By definition, $\operatorname{ran}(f) = \{y \in B : \ (\exists x \in A)\,(y = f(x))\}$. So, if we take $y \in \operatorname{ran}(f)$, then $y \in B$ and from that $\operatorname{ran}(f) \subseteq B$.

□

Lemma. Let $f : A \to B$ be a function. Then,

$$\{f(x) : \ x \in A\} = \{y \in B : \ (\exists x \in A)\,(y = f(x))\}.$$

Proof. Let $R = \{f(x) : \ x \in A\}$ and $R' = \{y \in B : \ (\exists x \in A)\,(y = f(x))\}$. If we take

[17] In FOL, these two rules can be written as:

1. $(\forall x \in A)(\exists y \in B)(y = f(x))$;
2. $(\forall x_1, x_2 \in A)(x_1 = x_2 \to f(x_1) = f(x_2))$.

[18] That is, for each element in B there is exactly one element in A:

$$(\forall x_1, x_2 \in A)(f(x_1) = f(x_2) \to x_1 = x_2).$$

[19] I.e. the codomain of function $f : A \to B$ is equal to it's image; for every element $y \in B$ there is an element in A such that $f(x) = y$; in FOL:

$$(\forall y \in B)(\exists x \in A)(f(x) = y).$$

$y \in R$, then $y = f(x)$, for some $x \in A$, i.e. there exists $x \in A$ such that $y = f(x)$. That implies $y \in R'$ and $R \subseteq R'$. Take $y \in R'$. Then there exists $x \in A$ such that $y = f(x)$. As y is of the form $y = f(x)$, for some $x \in A$, then $y \in R$ and $R' \subseteq R$. That implies $R = R'$.

□

Proposition. Let $f : A \to B$ be a function. Then, $\text{ran}\,(f) = B$ if and only if for all $y \in B$ there exists $x \in A$ such that $y = f(x)$.

Proof. *Necessity.* Let $\text{ran}\,(f) = B$. As $\text{ran}\,(f) = \{f(x) : \ x \in A\}$, then if $y \in B = \text{ran}\,(f)$, there must exist $x \in A$ such that $f(x) = y$. *Sufficiency.* Let for all $y \in B$ exist $x \in A$ such that $y = f(x)$. By a previous proposition we have $\text{ran}\,(f) \subseteq B$. If we take $y \in B$, then there exists $x \in A$ such that $f(x) = y$, so $y \in \text{ran}\,(f)$ and $B \subseteq \text{ran}\,(f)$. That implies $\text{ran}\,(f) = B$.

□

Definition. We say that a function is **bijective** if it's both surjective and injective.

Remark. From now on, we will write only f when we're refering to a function $f : A \to B$ (but make sure to get the distinction between the rule f and the function (f, A, B) which is an ordered triple containing the rule with both domain and codomain).

Definition. Let $f : A \to B$ and $g : B \to C$ be functions. The **composite function** denoted by $g \circ f$ is a function from A to C defined as follows:

$$[f \circ g](x) = f(g(x)), \ \forall x \in A.$$

Theorem. Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions. Then:

$$[h \circ [g \circ f]](x) = [[h \circ g] \circ f](x), \ \forall x \in A,$$

that is, function composition is associative.

Proof. The proof follows directly from definition. We will show that both expressions equal $h(g(f(x)))$. We have:

$$[h \circ [g \circ f]](x) = h([g \circ f](x)) = h(g(f(x))).$$

On the other side, we have:

$$[[h \circ g] \circ f](x) = [h \circ g](f(x)) = h(g(f(x))).$$

□

Theorem. Let $f : A \to B$ and $g : B \to C$ be functions. Then the following statements are true:

1. If f and g are injective, then $g \circ f$ is injective.
2. If f and g are surjective, then $g \circ f$ is surjective.
3. If f and g are bijective, then $g \circ f$ is bijective.

Proof.

1. *If f and g are injective, then $g \circ f$ is injective.* Taking some elements $x_1, x_2 \in A$, such that, as $g \circ f$ is a function, holds $g(f(x_1)) = g(f(x_2))$, then from injectivity of g we have $f(x_1) = f(x_2)$. Then, from injectivity of f we have $x_1 = x_2$. Summing up, for arbitrary $x_1, x_2 \in A$ we had that from $g(f(x_1)) = g(f(x_2))$ follows $x_1 = x_2$. Thus, $g \circ f$ is injective.
2. *If f and g are surjective, then $g \circ f$ is surjective.* As f is surjective, for all $x \in A$ we have $z \in B$ such that $f(x) = z$. And, as g is surjective, then for all $f(x) = z \in B$ we have $y \in C$ such that $g(z) = y$. But, $z = f(x)$, so $g(z) = g(f(x))$ and therefore we have $y = g(f(x))$. Summing up, for all $x \in A$ we have $y \in C$ such that $g(f(x)) = y$. Concluding, $g \circ f$ is surjective.
3. *If f and g are bijective, then $g \circ f$ is bijective.* Trivially, if f and g are injective, then so is $g \circ f$; if f and g are surjective, then so is $g \circ f$. As $g \circ f$ is, then, surjective and injective, it follows that $g \circ f$ is bijective.

□

Theorem. Let $f : A \to B$ and $g : B \to C$ be functions. Then:

1. If $g \circ f$ is injective, then g is injective.
2. If $g \circ f$ is injective, then f is not necessarily injective.
3. If $g \circ f$ is surjective, then f is surjective.
4. If $g \circ f$ is surjective, then g is not neccesarily surjective.

Proof.

1. *If $g \circ f$ is injective, then g is injective.* For all $x_1, x_2 \in A$, as $g \circ f$ injective, $g(f(x_1)) = g(f(x_2))$ implies $x_1 = x_2$. Now, suppose that g is not injective and that would mean that for some $y_1, y_2 \in B$ (where $y_1 = f(x_1)$ and $y_2 = f(x_2)$, because f is a function) it's true that $g(y_1) = g(y_2)$ and $y_1 \neq y_2$. But, as $y_1 = f(x_1)$ and $y_2 = f(x_2)$, that would mean that $g(f(x_1)) = g(f(x_2))$ and $f(x_1) \neq f(x_2)$. As f is a function, then from $f(x_1) \neq f(x_2)$ follows that $x_1 \neq x_2$. That is a contradiction with our assumption that $g \circ f$ is injective.

2. *If $g \circ f$ is injective, then f is not necessarily injective.* Proof by counterexample. Take $g : \mathbb{R}^+ \to \mathbb{R}$, and $g(x) = \ln x$. Now, take $f : \mathbb{R}\{0\} \to \mathbb{R}^+$ as $f(x) = x^2$. Obviously f is not injective, while g is. If we take $g(f(x)) = \ln(x^2) = 2 \ln x$, it's injective, as, taking $g(f(x_1)) = g(f(x_2))$ implies $2 \ln x_1 = 2 \ln x_2$. Now, dividing by two gets us $\ln x_1 = \ln x_2$. Taking[20] the $g^{-1} : \mathbb{R} \to \mathbb{R}^+$, where $g^{-1}(x) = e^x$ gives us $\exp \ln x_1 = \exp \ln x_2$, i.e. $x_1 = x_2$. Therefore, $g \circ f$ is injective, while f is not.

3. *If $g \circ f$ is surjective, then g is surjective.* As $g \circ f$ is surjective, then $(\forall x \in A)(\exists z \in C)(z = g(f(x)))$. Also, as f is function, then $(\forall x \in A)(\exists y \in B)(y = f(x))$. If g were not surjective then it would mean that for some $y \in B$ there does not exist $z \in C$ such that $g(y) = z$. But, as $y = f(x)$ for all $x \in A$, then it would mean that for some $f(x) = y \in B$ does not exist $z \in C$ such that $g(f(x)) = z$. That is a contradiction to our assumption.

4. *If $g \circ f$ is surjective, then f is not neccesarily surjective.* Proof by counterexample. Take $A = \{a_1\}$, $B = \{b_1, b_2\}$ and $C = \{c_1\}$. Now, define $f(a_1) = b_1$, $g(b_1) = g(b_2) = c_1$. Then, obviously $g(f(a_1)) = g(b_1) = c_1$ (that is for all elements in A) completely defines composition $g \circ f$. Now, $g \circ f$ is surjective, but f is not.

□

Remark. In order to complete, rigorously, the proof of the following theorem, we will need to define functions in the set-theoretic sense, and for that we will need some short notes on relations.

Definition. Let A and B be sets. Then any $\mathcal{R} \subseteq A \times B$ is called a **relation** of A to B. The fact that $x \in A$ and $y \in B$ are in relation $\mathcal{R}$, we denote by $x\mathcal{R}y$. We call A domain of $\mathcal{R}$ and B codomain of $\mathcal{R}$.

Definition. We say that a relation $\mathcal{R} \subseteq A \times B$ is a **partial function** if it satisfies the following condition:

[20] We will now make the assumption that the reader is familiar with the concept of inverse function at least at an intuitive level.

$$(\forall x \in A)(\forall y_1, y_2 \in B)((x, y_1), (x, y_2) \in \mathcal{R} \to y_1 = y_2).$$

Remark. In this way we can define function $f : A \to B$ as a partial function which further satisfies (that is, it's **left-total**)

$$(\forall x \in A)(\exists y \in B)((x, y) \in f).$$

Definition. If, for $y \in B$, there exists $x \in A$ such that $f(x) = y$, we write $f^{-1}(y) = x$ and call it *preimage* of y. The set, denoted ambiguously, $f^{-1}(y) = \{x \in A : \ y = f(x)\}$, for $y \in B$, containing all preimages of y is called the *fiber* of y.

Remark. Note that, if x is unique, we will write $f^{-1}(y) = x$, as we will mean that exact element; on the other hand, if $S = \{x \in A : y = f(x)\}$ and $|S| > 1$, then we will write $f^{-1}(y) = S$, meaning S as the fiber of y.

Definition. Function $i_S : S \to S$ defined with $i_S(x) = x$, for all $x \in S$ is called *identity* on S.

Remark. Note that i_S is indeed well defined and is a function. It is defined for all $x \in S$ and returns a unique $x \in S$, for each $x \in S$.

Definition. Let $f : A \to B$ be a function. We say that f has a **left inverse** if there exists $g : B \to A$ such that $[g \circ f] = i_A$. We say that f has a **right inverse** if there exists $g : B \to A$ such that $[f \circ g] = i_B$.

Definition. We say that $f : A \to B$ has an **inverse** if there is a function $f^{-1} : B \to A$ such that $y = f(x)$ if and only if $f^{-1}(y) = x$, for every $x \in A$ and $y \in B$.

Remark. In the set theoretic sense, this can be written as $f^{-1} = \{(y, x) : (x, y) \in f\}$, with of course, the two forementioned properties of functions.

Proposition. Identity is bijective and its own inverse.

Proof. Let $i_S : S \to S$ with $i_S(x) = x$, for all $x \in S$. *Injectivity.* If we take $i_S(x_1) = i_S(x_2)$, by definition we get $x_1 = x_2$. *Surjectivity.* If we take $y \in S$, then there exists $x \in S$, such that $x = y$. As $i_S(x) = x$, then $i_S(x) = y$. Thus, i_S is a bijection. It is obvious that for all $x, y \in S$, $i_S(x) = y$ if and only if $i_S(y) = x$ (if $i_S(x) = y$, then $x = y$ and $i_S(y) = y = x$; conversely, if $i_S(y) = x$, then $y = x$ and $i_S(x) = x = y$) and i_S is the inverse of i_S

□

Theorem. A function $f : A \to B$ has an inverse $f^{-1} : B \to A$ if and only if it has a left inverse $f_L : B \to A$ and a right inverse $f_R : B \to A$ such that $f_L = f_R$.

Proof. Let $f : A \to B$ be a function. *Necessity.* Let f have an inverse $f^{-1} : B \to A$. Then, for all $x \in A$ and $y \in B$, $f(x) = y$ if and only if $x = f^{-1}(y)$, where $f^{-1} : B \to A$. Then, $[f^{-1} \circ f](x) = f^{-1}(f(x))$. But, $f(x) = y$ and $f^{-1}(y) = x$, so $f^{-1}(f(x)) = f^{-1}(y) = x$. As $[f^{-1} \circ f] : A \to A$, with $[f^{-1} \circ f](x) = x$, we have $[f^{-1} \circ f] = i_A$ and f has a left inverse. Similarly, $[f \circ f^{-1}](y) = f(f^{-1}(y)) = f(x) = y$, for all $x \in A$ and $y \in B$, so $[f \circ f^{-1}] = i_B$ and f has a right inverse. *Sufficiency.* Let f have a left inverse and a right inverse. Then there exist $f_L : B \to A$ and $f_R : B \to A$, such that $[f_L \circ f] = i_A$ and $[f \circ f_R] = i_B$. Let $x \in A$ and $y \in B$. As f has a left inverse we have $f_L(f(x)) = x$, for all $x \in A$. But, as f is a function, for all $x \in A$ there exists $y \in B$ such that $f(x) = y$, so we have $f_L(y) = x$. Then, as f has a right inverse, we have $f(f_R(y)) = y$, for all $y \in B$. As f_R is a function, for all $y \in B$, there exists $x \in A$ such that $f_R(y) = x$. Then, $f(x) = y$. As $f_L = f_R$, we have that for all $x \in A$ there exists $y \in B$ such that $f(x) = y$ and that for all $y \in B$ there exists $x \in B$ such that $f_L(y) = x$. That is equivalent to $f(x) = y$ if and only if $f_L(y) = x$, for all $x \in A$ and $y \in B$, which means that, by definition f_L is an inverse of f.

□

Lemma. Inverse of injection is a partial function.

Proof. Suppose $f : A \to B$ is an injection. We define a relation

$$f^{-1} = \{(y, x) \in B \times A : (x, y) \in f\}.$$

Now, as f is injective, it follows that

$$(\forall x_1, x_2 \in A)(f(x_1) = f(x_2) \to x_1 = x_2).$$

Now, we'll write down the fact that $f(x_1) = y$ as $(x_1, y) \in f$. That means that

$$(\forall y \in B)(\forall x_1, x_2 \in A)((x_1, y), (x_2, y) \in f \to x_1 = x_2).$$

But, if $(x_1, y) \in f$, that means that $(y, x_1) \in f^{-1}$. So, we can say:

$$(\forall y \in B)(\forall x_1, x_2 \in A)((y, x_1), (y, x_2) \in f^{-1} \to x_1 = x_2).$$

That means that f^{-1} is a partial function.

□

Theorem. A function $f : A \to B$ has an inverse if and only if it is bijective. In that case, the inverse f^{-1} is a bijective function from B to A.

Proof. *Necessity.* Suppose $f : A \to B$ has an inverse $f^{-1} : B \to A$. That means that $y = f(x)$ if and only if $f^{-1}(y) = x$, for all $x \in A$ and $y \in B$. If f were not injective that would mean that there exists some $x_1, x_2 \in A$ such that $f(x_1) = f(x_2) = y$ and $x_1 \neq x_2$. That would mean that $f^{-1}(y) = x_1$ and $f^{-1}(y) = x_2$, where $x_1 \neq x_2$ i.e. for some $y \in B$ (domain of f^{-1}) we have two different values in A (codomain of f^{-1}), which is a contradiction to the assumption that f^{-1} is a function. Therefore, f must be injective. Now, suppose that f is not surjective. That would mean that for some $y \in B$ there does not exist $x \in A$ such that $y = f(x)$. But, we have, for all $x \in A$ and $y \in B$ that $f^{-1}(y) = x$; that would be again contradict the assumption that f^{-1} is a function, as we would have some x in domain of f^{-1} that does not have it's image, y, in codomain of f^{-1}. Therefore, f must also be surjective. As f is surjective and injective, it is bijective.

Sufficiency. We define first the relation $f^{-1} = \{(y, x) : (x, y) \in f\}$. Now, as f is injective, from the following lemma, it follows that f^{-1} is a partial function. But, as f is also surjective it holds that:

$$(\forall y \in B)(\exists x \in A)(y = f(x)),$$

that is, in set-theoretic view:

$$(\forall y \in B)(\exists x \in A)((x, y) \in f),$$

Now, as we have that if $(x, y) \in f$ implies $(y, x) \in f^{-1}$, then

$$(\forall y \in B)(\exists x \in A)((y, x) \in f^{-1}).$$

By definition that means that f^{-1} is also left-total. That, combined with the fact that it is a partial function, tells us that f^{-1} is a function for which holds $f^{-1} = \{(y, x) : (x, y) \in f\}$, which can be written as $(y, x) \in f^{-1}$ if and only if $(x, y) \in f$, i.e. $x = f^{-1}(y)$ if and only if $y = f(x)$, for all $x \in A$ and $y \in B$, which means that it's inverse of f.

□

Lemma. Let A be a finite set and $f : A \to B$ a function. Then, $\text{ran}\,(f)$ is finite and $|\text{ran}\,(f)| \leq |\text{dom}\,(f)|$.

Proof. Let $A = \{a_1, a_2, \ldots, a_m\}$ with $m \in \mathbb{Z}^+$. Then, $\text{dom}\,(f) = A$. By definition $\text{ran}\,(f) = \{f(x) : \ x \in A\} = \{f(a_1), f(a_2), \ldots, f(a_m)\}$, so $\text{ran}\,(f)$ is finite. As f is a function, each $f(a_i)$ will equal only one $y \in B$, so we can denote $f(a_i) = b_i$, for $i \in \{1, \ldots, m\}$. Yet, we have no guarantee that $b_i \neq b_j$, i.e. $f(a_i) \neq f(a_j)$ for all $i, j \in \{1, \ldots, m\}$, $i \neq j$, and it must be that $|\text{ran}\,(f)\,| \leq m = |A|$.

□

Lemma. Let S and T be finite sets such that $S \subseteq T$ and $|S| = |T|$. Then, $S = T$.

Proof. If $|S| = |T| = 1$, then, $S = \{s\}$ and $T = \{t\}$. But, as $S \subseteq T$, for all $x \in S$, there exists some $y \in T$ such that $x = y$. But that is only $s = t$ and it must be $S = T$. Suppose the statement is true for some $k \in \mathbb{Z}^+$, i.e. $S \subseteq T$, $|S| = |T| = k$ implies $S = T$. Let us prove it is true for $k + 1 \in \mathbb{Z}$. So, if $S = \{s_1, \ldots, s_k, s_{k+1}\}$ and $T = \{t_1, \ldots, t_k, t_{k+1}\}$, with $S \subseteq T$, then we need to show that $S = T$. Notice that we can write $S = S' \cup \{s_{k+1}\}$. As $s_{k+1} \in S$ and $S \subseteq T$, then also $s_{k+1} \in T$ (without loss of generality assume that $t_{k+1} = s_{k+1}$). Then, we can write $T = T' \cup \{t_{k+1}\} = T' \cup \{s_{k+1}\}$. Now, notice that $|S'| = (k + 1) - 1$ and $|T'| = (k + 1) - 1 = k$. So, $|S'| = |T'| = k$. If we take $s_i \in S'$, then $S' \subseteq S \subseteq T$ implies $s_i \in T$. But, $s_{k+1} \neq t_{k+1}$, then there exists $t_j \in T - \{t_{k+1}\}$ such that $s_i = t_j$. Therefore, $S' \subseteq T - \{t_{k+1}\}$, i.e. $S' \subseteq T'$. With $|S'| = |T'| = k$, that implies $S' = T'$ and we get $T = T' \cup \{s_{k+1}\} = S' \cup \{s_{k+1}\} = S$.

□

Theorem. Let $f : A \to B$ a function. Then,

1. Function f has a right inverse if and only if f is surjective.
2. Function f has a left inverse if and only if f is injective.

Proof. *Ad* 1. *Necessity.* Suppose f has a right inverse. Then there exists $f_R : B \to A$ such that $f \circ f_R = i_B$. That means that $f(f_R(y)) = y$, for all $y \in B$. Then, $f_R : B \to A$ is a well-defined function and for all $y \in B$ there exists $x \in A$ such that $f_R(y) = x$. But, if $f_R(y) = x$ and $x \in A$, then $f_R(y) \in A$, and we have $f(f_R(y)) = y$, i.e. $f(x) = y$. Therefore, f is a surjection. *Sufficiency.* Suppose that f is surjective. Then, for all $y \in B$ there exists $x \in A$ such that $f(x) = y$. Let us define $g : B \to A$ so that $g(y) = f^{-1}(y)$, for all $y \in B$ for which exists $x \in A$ such that $f(x) = y$. But, as f is surjective, that condition is satisfied for all $y \in B$ and g is well-defined. We can see

that, if we take $y \in B$ we have $f(g(y)) = f(f^{-1}(y))$. As for $y \in B$ there exists $a \in A$ such that $f(a) = y$, we have $f^{-1}(y) = a$. Then, $f(g(y)) = f(a)$. But, $f(a) = y$ and $f(g(y)) = y$. Thus, f has a right inverse and it is g.

Ad 2. *Necessity.* Suppose f has a left inverse. Then, there exists $f_L : B \to A$ such that $[f_L \circ f](x) = x$, for all $x \in A$. Let $x_1, x_2 \in A$. Then, there exist $y_1, y_2 \in B$ such that $f(x_1) = y_1$ and $f(x_2) = y_2$. As f_L is a well defined function, then for all $y_1, y_2 \in B$, if $y_1 = y_2$, it must be $f_L(y_1) = f_L(y_2)$ (uniqueness). In other words, for all $f(x_1), f(x_2) \in B$, if $f(x_1) = f(x_2)$ it must be $f_L(f(x_1)) = f_L(f(x_2))$. But, $f_L(f(x)) = x$, for all $x \in A$, so we have $x_1 = x_2$. As our choice of x_1 and x_2 was arbitrary the statement is true for all $x_1, x_2 \in A$ and f is, by that, injective. *Sufficiency.* If f is injective, then for all $x_1, x_2 \in A$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Let $g : B \to A$ be a function such that $g(y) = f^{-1}(y)$ for all $y \in B$ for which exists $x \in A$ such that $f(x) = y$. Also, for $y \in B$ for which does not exist $x \in A$ such that $f(x) = y$, let $g(y) = a$, for some $a \in A$. So, g is defined for all $y \in B$. Take $y_1, y_2 \in B$ and assume $y_1 = y_2$. We have that there exist $x_1, x_2 \in A$ such that $y_1 = f(x_1)$ and $y_2 = f(x_2)$. Therefore, we have $f(x_1) = f(x_2)$. By injectivity of f, we have $x_1 = x_2$. As f is defined for all $x \in A$, i.e. for all $x \in A$ there exists $y \in B$ such that $f(x) = y$, then it must be that for all $x \in A$, there exists $y \in B$ such that $x = f^{-1}(y)$, i.e. $x = g(y)$. So, for $x_1, x_2 \in A$, there exists $z_1, z_2 \in B$ such that $g(z_1) = x_1$ and $g(z_2) = x_2$. But, $g(z_1) = f^{-1}(z_1) = x_1$ and $f^{-1}(z_1) = x_1$ implies $z_1 = f(x_1$, i.e. $z_1 = y_1$. Similarly, $z_2 = y_2$. From that we have $g(y_1) = x_1 = x_2 = g(y_2)$, i.e. $g(x_1) = g(x_2)$. Thus, g is a well defined function. If we take $x \in A$, there exists $y \in B$ such that $f(x) = y$. Now, for $y \in B$ such that there exists $x \in A$ and $f(x) = y$, then $g(y) = x$. But, that means that $g(f(x)) = x$, i.e. g is a left inverse of f.

□

Theorem. Let A and B be finite sets and $f : A \to B$ a function. Then the following holds:

1. If $|\mathrm{dom}\,(f)\,| < |\mathrm{cod}\,(f)\,|$, then f cannot be a surjection.
2. If $|\mathrm{dom}\,(f)\,| > |\mathrm{cod}\,(f)\,|$, then f cannot be an injection[21].
3. If $|\mathrm{dom}\,(f)\,| = |\mathrm{cod}\,(f)\,|$, then f is an injection iff it is a surjection.

Proof. *Ad* 1. Let $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$ such that $m < n$. Assume $\mathrm{ran}\,(f) = B$, i.e. f is surjective. From that follows $|\mathrm{ran}\,(f)\,| = |B|$, that is $|\mathrm{ran}\,(f)\,| = n$. But, by a previous lemma, as A and B are finite we have $|\mathrm{ran}\,(f)\,| \leq m$. In other words, $n \leq m$. But, by assumption also $m < n$, so we have $n \leq m < n$ and from that $n < n$, which is impossible. Therefore, f cannot be surjective.

[21] Actually another form of the **pigeonhole principle**.

Ad 2. Let $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$ such that $m > n$. Let us denote $A_n = \{a_{n+1}, \ldots, a_m\}$. Notice that $A - A_n \neq \emptyset$, as $m = n + k$, where $k \in \mathbb{Z}^+$. If there exist $a_i, a_j \in A - A_n$, $i \neq j$ and $i, j \in \{1, \ldots, n\}$, such that $f(a_i) = f(a_j)$, then f is not an injection and we are done. Assume that for all $a_i, a_j \in A - A_n$, we have that $a_i \neq a_j$ (sufficient to say $i \neq j$) implies $f(a_i) \neq f(a_j)$. If we denote $f(a_i) = b_i$, for all $i \in \{1, \ldots, n\}$ then, $\text{ran}\,(f) = \{b_1, \ldots, b_n\}$. All elements are different by assumption, so $|\text{ran}\,(f)| = n$. From $\text{ran}\,(f) \subseteq B$ and latter result, we have $\text{ran}\,(f) = B$, i.e. f is a surjection. Also, $\text{ran}\,(f) = \{b_1, \ldots, b_n\}$. As $A_n \neq \emptyset$, there exists $a_{n+r} \in A_n$, for some $r \in \mathbb{Z}^+$, such that $n < n + r \leq m$. As f is a function, then there exists $b_i \in B = \text{ran}\,(f)$ such that $f(a_{n+r}) = b_p$, where $p \in \{1, \ldots, n\}$. But, also, $f(a_p) = b_p$, impliying $f(a_p) = f(a_{n+r})$. Now, clearly $a_{n+r} \neq a_p$ (contradicting this would imply $n + r = p$, but $p \leq n$, so it must be $n + r \neq p$), that implies that it is not the case that $f(a_p) = f(a_{n+r})$ implies $a_{n+r} = a_p$, i.e. f is not an injection.

Ad 3. Let $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_m\}$. *Necessity.* Let f be an injection. Then, by a previous proposition $|\text{ran}\,(f)| = |A| = m$. As $|B| = m$, we have $|\text{ran}\,(f)\,| = |B|$. Furthermore, as $\text{ran}\,(f) \subseteq B$ it follows that $\text{ran}\,(f) = B$, i.e. f is a surjection. *Sufficiency.* Let f be a surjection. Then, $\text{ran}\,(f) = B$ and from that $|\text{ran}\,(f)\,| = |B| = m$. We can say $\text{ran}\,(f) = \{f(a_1), \ldots, f(a_m)\}$ and all $f(a_i) \neq f(a_j)$, for $i \neq j$, i.e. $a_i \neq a_j$, so f is an injection. $b_p = b_r = b$,

□

Remark. The third case in theorem above actually tells us that if $f : A \to B$, where A and B are finite and with equal number of elements, is injection or a surjection then it is necessarily a bijection. A problem below tells us, that, if sets are not finite, the analogues to the cases above don't have to be true.

Problem. Let $A, B \subseteq \mathbb{R}$ be sets such that $B \subset A$. Show that there exists a bijection $f : A \to B$.

Solution. Let $A = [a, b]$, $B = [c, d]$ with $c \neq d$. Take two points $X(a, c)$ and $Y(b, d)$ in $\mathbb{R}^2$. If we take a line defined by those points, we get the equation:

$$y - c = \frac{d - c}{b - a}(x - a).$$

Simplifying that expression gives us:

$$y = \frac{d - c}{b - a}x + \frac{-a(d - c) + c(b - a)}{b - a}.$$

So, we will take that to be:

$$f(x) = \frac{d-c}{b-a}x - \frac{a(d-c) - c(b-a)}{b-a}.$$

Linear function is obviously injective, and so is the above instantiation. We can see that from the coefficient next to x, $f'(x) = \frac{d-c}{b-a}$ is strictly greater than zero (as $d > c$ and $b > a$), making it a monotonously rising function and therefore injective. Let's take $f(a)$. That is obviously:

$$f(a) = \frac{a(d-c)}{b-a} - \frac{a(d-c) - c(b-a)}{b-a} = \frac{c(b-a)}{b-a} = c.$$

Now, for $f(b)$ we have:

$$f(b) = \frac{b(d-c)}{b-a} - \frac{a(d-c) - c(b-a)}{b-a} = \frac{bd-ad}{b-a} = d.$$

So, $f([a,b]) = [f(a), f(b)] = [c,d]$, that is $\mathrm{Im}(f) = B$, making f surjective and by that bijective.

Problem. Let $\mathcal{F}_b(\mathbb{R})$ be the set of all bijective functions of the form $f : \mathbb{R} \to \mathbb{R}$. Prove that $(\mathcal{F}_b(\mathbb{R}), \circ)$ (i.e. the set of all bijective functions of the formerly described form with function composition as respective operation) is a group.

Solution. By previously proven theorem, function composition is associative (for functions of any type). There is a neutral element $\mathrm{id} : \mathbb{R} \to \mathbb{R}$ defined as $id(x) = x$ (because $[f \circ \mathrm{id}](x) = f(\mathrm{id}(x)) = f(x)$ and $[\mathrm{id} \circ f](x) = \mathrm{id}(f(x)) = f(x)$ for every $x \in \mathbb{R}$). By previosly proven theorem, every bijective function has an inverse, and in this case that would be $f^{-1} : \mathbb{R} \to \mathbb{R}$. Composition is, however, not commutative. We could take, e.g. $f(x) = x + 1$ and $g(x) = 2x$. Obviously, $[f \circ g](x) = f(g(x)) = 2x + 1$, while $[g \circ f](x) = g(f(x)) = 2(x + 1)$. Therefore $(\mathcal{F}_b(\mathbb{R}), \circ)$ is a group.

Problem. Let A and B be finite non-empty sets where $|A| = n$ and $|B| = m$. What is the number of:

1. functions $f : A \to B$;
2. injections $f : A \to B$;
3. bijections $f : A \to A$?

Solution. We will determine the number of:

1. *functions* $f : A \to B$. Now, f will be a set of all ordered pairs $(x, y) \in A \times B$ with conditions that each $x \in A$ must appear only once (so it will be many-to-one) and every $x \in A$ must be contained in some ordered pair (so it will be left-total). For every $y \in B$ we can either choose many $x \in A$ or none at all. One example, for $f \subseteq \{x_1, x_2, x_3\} \times \{y_1, y_2, y_3\}$, would be:

$$f = \{(x_1, y_1), (x_2, y_1), (x_3, y_2)\}.$$

In general, for $A = \{x_1, \ldots, x_n\}$ we have:

$$f = \{(x_1, \cdot), (x_2, \cdot), \ldots, (x_n, \cdot)\}.$$

That way, every $x \in A$ appears and appears only once. For each $x \in A$ we can choose m different $y \in B = \{y_1, \ldots, y_m\}$. So, for every ordered pair we have m choices, as we can take multiple $y \in B$ for one $x \in A$. For n ordered pairs the number of different choices is $\underbrace{m \cdot m \cdots m}_{n \text{ times}} = m^n$. The number of different functions from A to B is $|B|^{|A|}$; more general:

$$|\mathrm{cod} f|^{|\mathrm{dom} f|}.$$

2. *injections* $f : A \to B$. We take all the conditions from the previous problem, adding that every $y \in B$ must appear only once. Therefore, for first ordered pair we have m choices, for second $m - 1$, for third $m - 2$, etc. As we have n ordered pairs, that is $m(m-1)(m-2)\cdots(m-(n-1)) = \frac{m!}{(m-n)!}$. The number of different injections from A to B is then $\frac{|B|!}{(|B|-|A|)!}$; more general:

$$\frac{|\mathrm{cod} f|!}{(|\mathrm{cod} f| - |\mathrm{dom} f|)!}.$$

3. *bijections* $f : A \to A$. Taking all conditions from the previous example, we add the condition that $B = A$ and therefore $|B| = |A|$. Using the fact that $0! = 1$ we have that the number of bijections from A to A is $|A|!$, or:

$$|\mathrm{dom} f|!.$$

Definition. We define a function (in the mention-sense) called *Iverson brackets* of the form $[\cdot] : \Phi \to \{1, 0\}$, where Φ is the set of all propositions of the form $P(x)$.

Then, Iverson brackets is defined by a rule: $[P(x)] = 1$ if and only if $P(x)$ is true, and $[P(x)] = 0$ otherwise.

Problem. We have said that Iverson brackets is a function, but only in the mention-sense. Prove that it really *is* a function.

Solution. By definition of a proposition, it is any judgment to which we can assign a truth value (true or false). So, Iverson brackets is defined for every proposition, satisfying the first axiom; and as every proposition can be, according to law of non-contradiction, true or false, no proposition can take more than one value in $\{1, 0\}$. Therefore, Iverson brackets is a function.

Remark. As a special case of Iverson brackets we can consider indicator function $I_S : S \to \{1, 0\}$, where S is a non-empty set, defined as:

$$I_S(x) = [x \in S].$$

Remark. By using Iverson brackets, we can construct functions using logical connectives in a more analytic fashion. For example, disjunction can be then defined using the operation of addition modulo[22] 2 (denoted by $+_2$):

$$I(P(x) \vee Q(x)) = \mathcal{B}\left([P(x)] +_2 [Q(x)]\right),$$

where $\mathcal{B} : \{0, 1\} \to \{\bot, \top\}$ such that $\mathcal{B}(0) = \bot$ and $\mathcal{B}(1) = \top$ (it's obvious that this is a bijection; its inverse is trivial). Also, $I : \Phi \to \{\bot, \top\}$ is an interpretation. Conjunction can be defined in the similar sense using multiplication:

$$I(P(x) \wedge Q(x)) = \mathcal{B}\left([P(x)] \cdot [Q(x)]\right).$$

Problem. Determine whether each of the following functions $f \in \mathcal{F}(\mathbb{R})$ is or is not injective and is or is not surjective:

1. $f(x) = xI_{\mathbb{Q}}(x) + 2xI_{\mathbb{I}}(x)$;
2. $f(x) = 2xI_{\mathbb{Z}}(x) + xI_{\mathbb{R}\setminus\mathbb{Z}}(x)$;
3. $f : A \times B \to A$, defined by $f(x, y) = x$;
4. $f : A \times B \to B \times A$, defined by $f(x, y) = (y, x)$;

[22] Notice that, if the propositions are taken as sets, as it is in the second-order logic, if the sets are disjunct we can take only simple addition: they are never going to be both true.

5. $f : A \to A \times B$, defined by $f(x) = (x, b)$, $b \in B$;

6. G is a group, $a \in G$, and $f : G \to G$ is defined by $f(x) = ax$;

7. G is a group and $f : G \to G$ is defined by $f(x) = x^{-1}$;

8. G is a group and $f : G \to G$ is defined by $f(x) = x^2$.

Solution.

1. $f(x) = xI_{\mathbb{Q}}(x) + 2xI_{\mathbb{I}}(x)$. Take $f(a) = f(b)$, that means that $aI_{\mathbb{Q}}(a) + 2aI_{\mathbb{I}}(a) = bI_{\mathbb{Q}}(b) + 2bI_{\mathbb{I}}(b)$, i.e. that a and b are both rational or both irrational. If they are both rational, then the second members on every side of equation go to zero, and we only have $a = b$. If they are both irrational, then it's the reverse case and we have $2a = 2b$, that is, $a = b$. Therefore, $f(x)$ is injective. Now, obviously if we take some $y \in \mathbb{Q}$, then, there exists such $x \in \mathbb{Q}$ that $f(x) = y$ and that is x. If we take $y \in \mathbb{I}$, then there exists $x \in \mathbb{I}$ such that $f(x) = y$ and that is $\frac{1}{2}x$, which is again irrational. And, as $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$, we have exhausted all elements in codomain of f, so f is surjective.

   Now, as $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$, f is defined for all $x \in \mathbb{R}$, thus f is surjective. Also, f is bijective.

2. $f(x) = 2xI_{\mathbb{Z}}(x) + xI_{\mathbb{R}\setminus\mathbb{Z}}(x)$. If we take $f(a) = f(b)$, that is, $2aI_{\mathbb{Z}}(a) + aI_{\mathbb{R}\setminus\mathbb{Z}}(a) = 2bI_{\mathbb{Z}}(b) + bI_{\mathbb{R}\setminus\mathbb{Z}}(b)$, that means that a and b are either both integers or are both in $\mathbb{R}\setminus\mathbb{Z}$. So, if they are both integers, the second members of addition on each side of equation go to zero and we have $2a = 2b$. In the otherwise-case, we have $a = b$, so f is injective. Can $f(x) = 1$? If that is so, then $1 = 2xI_{\mathbb{Z}}(x) + xI_{\mathbb{R}\setminus\mathbb{Z}}(x)$. If $x \in \mathbb{Z}$ then we can only have even numbers, as $2x$ is even for all $x \in \mathbb{Z}$. It cannot be 1. If $x \notin \mathbb{Z}$, then $f(x) = x$, so x must be 1, but $1 \in \mathbb{Z}$, and that cannot be. So we don't have at least one element, that is $1 \in \mathbb{R}$ that has a preimage in $\mathbb{R}$. This function is not surjective.

3. $f : A \times B \to A$, *defined by* $f(x, y) = x$. Take $(a, b), (c, d) \in (A \times B)$. Then, $f(a, b) = f(c, d)$ means that $a = c$, but not necessarily $(a, b) = (c, d)$. E.g. $(a_1, b_1) \neq (a_1, b_2)$, such that $b_1 \neq b_2$. Then, $f(a_1, b_1) = a_1$ and $f(a_1, b_2) = a_1$ (i.e. two different elements in domain have the same element a_1 in codomain). Therefore, f is not injective. Now, f is surjective as, if we take $z \in A$, there is $(z, y) \in (A \times B)$ such that $f(z, y) = z$.

4. $f : A \times B \to B \times A$, *defined by* $f(x, y) = (y, x)$. If $f(a, b) = f(c, d)$ that means that $(b, a) = (d, c)$ and that $b = d$ and $a = c$, which is the same as saying $(a, b) = (c, d)$, therefore f is injective. Now, take some $(y, x) \in B \times A$. There exists $(x, y) \in A \times B$ such that $f(x, y) = (y, x)$. Obviously f is surjective and by that bijective.

5. $f : A \to A \times B$, *defined by* $f(x) = (x, b)$, $b \in B$. If $f(z) = f(w)$ then $(z, b) = (w, b)$, which implies that $z = w$. So, f is injective. Yet, f is not surjective as $\mathrm{Im(f)} = (A \times \{b\}) \subset (A \times B)$.

6. G *is a group,* $a \in G$, *and* $f : G \to G$ *is defined by* $f(x) = ax$. Take $x, y \in G$. Then $f(x) = f(y)$ implies $ax = ay$. By cancellation law for groups (in this case, multiplying by a^{-1} on the left), we have $x = y$. Thus, f is injective. Now, if we take some $y \in G$, does there exist such $x \in G$ so that $f(x) = y$, i.e. $ax = y$?. Well, obviously, if $a \in G$, then $a^{-1} \in G$, so we have $x = a^{-1}y$; function f is surjective and therefore bijective.

7. G *is a group and* $f : G \to G$ *is defined by* $f(x) = x^{-1}$. If $f(a) = f(b)$, then $a^{-1} = b^{-1}$. Multipliying by a on the left and b on the right, we have $b = a$, therefore f is injective. Now, taking $y \in G$, does there exist $x \in G$ such that $f(x) = y$, i.e. $x^{-1} = y$? Multiplying by x on the right we have $e = yx$, and then, multiplying by y^{-1} (y has an inverse in G), we have $x = y^{-1}$. So, f is surjective, and then bijective.

8. G *is a group and* $f : G \to G$ *is defined by* $f(x) = x^2$. Now, if $f(a) = f(b)$, then $a^2 = b^2$. But, as we have previously shown, from this does not necessarily follow that $a = b$, e.g. $\mathbb{R}\backslash\{0\}$ with multiplication as respective operation is a group and we have $(-2)^2 = 2^2$, but $-2 \neq 2$. So, f is not necessarily injective. But f is also not necessarily surjective as for arbitrary $y \in G$ there does not have to exist $x \in G$ such that $f(x) = y$, e.g. $\mathbb{R}\backslash\{0\}$ with multiplication is a group and for $-1 \in \mathbb{R}\backslash\{0\}$ there does not exist such $x \in \mathbb{R}\backslash\{0\}$ that $x^2 = -1$. Thus, f is neither necessarily injective nor necessarily injective.

Theorem[23]**.** Let $(G, \oplus, \odot)$ be a ring and $A, B \subseteq G$, such that $A \cap B = \emptyset$ and $A \cup B = G$. Let $u : A \to A$ and $v : B \to B$ be bijective functions. We define function of the form $f : G \to G$ defined as

$$f(x) = u(x) \odot I_A(x) \oplus v(x) \odot I_B(x),$$

where indicator function I_S is defined by Iverson brackets, such that:

$$I_S(x) = [x \in S],$$

and $[\cdot] : \Phi \to \{e_\oplus, e_\odot\}$, defined such that $[P(x)] = e_\oplus$ if and only if $P(x)$ is true; $[P(x)] = e_\odot$ otherwise; $e_\odot$ is neutral element for $\odot$ operation and $e_\oplus$ a neutral element for $\oplus$ operation. Then, f is bijective.

[23]Generalization of the first two problems in previous excercises. For advanced readers!

Proof. Now, as u, v are bijective and each being defined with domain and codomain on A and B, respectively, it cannot be that $u(x) = v(x)$, as $A \cap B = \emptyset$. If it were that $u(x) = v(x)$, that would mean that $u(x) \in A$ (as u is a function) and $v(x) \in B$ (as v is a function). But then, it would mean that $u(x) = v(x) \in B$, i.e. $u(x) \in A$ and $u(x) \in B$, which would be a contradiction to our assumtion that $A \cap B = \emptyset$. So, if we take $f(x) = f(y)$, that means that $u(x) \odot I_A(x) \oplus v(x) \odot I_B(x) = u(y) \odot I_A(y) \oplus v(y) \odot I_B(y)$. And if it were that x were in A and y were in B, it would mean that $u(x) = v(x)$, which could not be (same thing for $x \in B$ and $y \in A$). Therefore either $x, y \in A$ or $x, y \in B$. So, it would mean that $u(x) = u(y)$ or $v(x) = v(y)$, but u, v are bijective, so $x = y$ follows from both. Thus, f is also injective. If we take $y \in G$ does there exist $x \in G$ such that $f(x) = y$? Obviously, $A \cup B = G$, and they are disjunct, so, suppose $y \in A$. That would mean that it was $y = f(x) = u(x)$. If it were that $f(x) = v(x)$, then $y = f(x) = v(x) \in B$, which would be a contradiction. Therefore it was that $y = u(x)$. But, $u(x)$ is surjective, so there exists $x \in B$ such that $y = u(x)$. Same proof goes for $y \in B$. Thus, f is surjective, and by that also bijective. We will only make a comment that, as we're dealing with a commutative ring, neutral element $e_\oplus$ acts as a zero and $e_\odot$ as one, so we can view the operations in function f as addition and multiplication in $\mathbb{R}$ without, for now, entouring into more deeper analysis.

□

Problem. If $f : A \to B$ is injective and $g : B \to C$ surjective, is then $g \circ f : A \to C$ necessarily bijective?

Solution. We can take $f : \mathbb{R} \to \mathbb{R}$ to be $f(x) = x$, which is obviously injective, and $g : \mathbb{R} \to [-1, 1]$ to be $g(x) = \sin x$, which is surjective. But, $g \circ f : \mathbb{R} \to [-1, 1]$ with $g(f(x)) = \sin x$ is not injective and therefore not bijective.

Problem. Each of the following functions is bijective. Describe its inverse:

1. $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = 2xI_{\mathbb{Q}}(x) + 3xI_{\mathbb{I}(x)}$;
2. $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4\}$ and $f : A \to B$ is given by:

$$f = \begin{pmatrix} a & b & c & d \\ 3 & 1 & 2 & 4 \end{pmatrix};$$

3. G is a group, $a \in G$, and $f : G \to G$ is defined by $f(x) = ax$.

Solution.

1. $f : \mathbb{R} \to \mathbb{R}$, *defined by* $f(x) = 2xI_{\mathbb{Q}}(x) + 3xI_{\mathbb{I}(x)}$. Now, if we have $f(x)$ of the form $3x$, then we know that x is irrational. If, however, we have $f(x)$ of the form $2x$, we know that x is rational. Therefore $f^{-1}(x)$ is a rational number if x is divisible by 2 and irrational if it's divisible by 3, $(2|x \to f^{-1}(x) \in \mathbb{Q}) \wedge (3|x \to f^{-1}(x) \in \mathbb{I})$, $f^{-1} : \mathbb{R} \to \mathbb{R}$.

2. $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4\}$ *and* $f : A \to B$ *is given by:*

$$f = \begin{pmatrix} a & b & c & d \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

   Obviously, $f^{-1} : B \to A$ and:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ b & c & a & d \end{pmatrix}.$$

3. G *is a group,* $a \in G$, *and* $f : G \to G$ *is defined by* $f(x) = ax$. If we take $x \in G$, then we want to find the original $y \in G$, such that $x = ay$. As G is a group, and $a \in G$, we can take the inverse of $a^{-1} \in G$ and multiply the equation on the left with the former to get $a^{-1}x = y$. Taking $f^{-1}(x) = y$, we have $f^{-1} : G \to G$ with $f^{-1}(x) = a^{-1}x$.

Permutations

Definition. Let A be a non-empty set. Then, any bijection of the form $f : A \to A$ is called a **permutation**.

Remark. (i) Note that permutations are a subset of bijective functions, by definition. As for $f : A \to A$ and $g : A \to A$ it's $f \circ g : A \to A$ and $g \circ f : A \to A$ and as $f^{-1} : A \to A$, obviously permutations form a group by being a subgroup of bijective functions with function composition as respective operation (we have also shown previously that function composition is associative). (ii) Note that the number of permutations from A to A, with $|A| = n$, as previously shown for bijective functions, is $n!$. (iii) Also, we will denote the neutral element for group of permutations with ϵ and define it as $\epsilon : A \to A$ with rule $\epsilon(x) = x$. The other permutations are denoted with small greek letters and defined through tables, exempli gratia (one permutation of A, where $|A| = 4$):

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Definition. For any set A, the group[24] of all permutations of A is called the **symmetric group** on A and is represented by symbol S_A.

Remark. For $A = \{1, \ldots, n\}$, the group of all permutations of A is called symmetric group on n elements and is denoted by S_n.

Definition. For every $n \in \mathbb{N}\backslash\{1, 2\}$, the regular polygon with n sides has a group of symmetries symbolized by D_n. These groups are called **dihedral groups.**

Problem. Consider the following permutations $f, g, h \in S_6$:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix},$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 4 & 5 & 2 \end{pmatrix}.$$

Compute the following:

1. f^{-1}, g^{-1}, h^{-1}, $f \circ g$, $g \circ f$;

[24] Actually shown in the previous remark.

2. $f \circ (g \circ h)$;

3. $g \circ h^{-1}$;

4. $h \circ g^{-1} \circ f^{-1}$;

5. $g \circ g \circ g$.

Solution. *Ad* 1*:*

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix}, \qquad g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix},$$

$$h^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix},$$

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 2 & 4 & 5 \end{pmatrix}, \qquad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 5 & 6 & 3 \end{pmatrix}.$$

Ad 2*:*

$$g \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 5 & 3 \end{pmatrix}, \qquad f \circ (g \circ h) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

Ad 3*:*

$$g \circ h^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 6 & 5 & 1 \end{pmatrix}.$$

Ad 4*:*

$$g^{-1} \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 5 & 6 & 3 \end{pmatrix}, \qquad h \circ g^{-1} \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 5 & 6 \end{pmatrix}.$$

Ad 5*:*

$$g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix}, \qquad g \circ g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}.$$

Problem. List the elements of the cyclic subgroup of S_6 generated by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}.$$

Solution. We also need to find f^{-1} and then all the possible compositions of f with or without f^{-1} and reverse. Now:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}.$$

We venture further by finding:

$$f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix}.$$

Following the same line of reasoning:

$$f \circ f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}.$$

Notice that $f \circ f \circ f = f^{-1}$ and therefore $f \circ f \circ f \circ f = f \circ f^{-1} = \epsilon$. Then we would be geting $\epsilon \circ f = f$ and the same sequence all over again. Therefore $\langle f \rangle = \{\epsilon, f, f^{-1}, f \circ f\}$.

Problem. Let G be the subset of S_4 consisting of the permutations:

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \qquad f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Show that G is a group of permutations, and write its table.

Solution. In order to show that $G = \{\epsilon, f, g, h\}$ is a group of permutations, we need to show that each $x \in G$ is a permutation and that G is a group. We can show that G is a group by using the fact that $G \subseteq S_4$ and that S_4 is a symmetric group on 4 elements (there are $4! = 24$ permutations). We have already shown in a previous remark that a set endowed with composition and containing all permutations of some set will form a group. Therefore, it is sufficient to show that G is a subgroup of S_4. We need to find

compositions $f \circ f$, $g \circ g$, $h \circ h$, $f \circ g$, $g \circ f$, $f \circ h$, $h \circ f$, $g \circ h$ and $h \circ g$. The compositions with ϵ are trivial as $\epsilon \circ x = x \circ \epsilon = x$, for all $x \in G$ (and $x \in S_4$ also!).

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \qquad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$f \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \qquad h \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$

$$g \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \qquad h \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

We can see that $f \circ g = g \circ f = h$, then, $f \circ h = h \circ f = g$ and $g \circ h = h \circ g = f$. Now, it can easily be verified that $f \circ f = g \circ g = h \circ h = \epsilon$. The table is:

$\circ$	ϵ	f	g	h
ϵ	ϵ	f	g	h
f	f	ϵ	h	g
g	g	h	ϵ	f
h	h	g	f	ϵ

Notice that G is also an Abelian group.

Theorem. Denote σ_S to represent a permutation of a set S. Let $A = \{a_1, \ldots, a_n\}$, $n \in \mathbb{N}$. Then, let S_A be group of all permutations of the set A and G an Abelian subgroup of S_A. Now, let $B = \{b_1, \ldots, b_m\}$, $m \in \mathbb{N}$, be a set disjoint from A and $S_{A \cup B}$ group of all permutations of $A \cup B$. Now, for every $\sigma_A \in G$ define $\sigma_{A \cup B} \in S_{A \cup B}$ such that[25]

$$(\forall x \in A \cup B)(\sigma_{A \cup B}(x) = \sigma_A(x)\mathcal{I}_A(x) + x\mathcal{I}_B(x)).$$

Then the set H, containing such defined $\sigma_{A \cup B}$, is an Abelian subgroup of $S_{A \cup B}$.

Proof. Let $A = \{a_1, \ldots, a_n\}$ be a set, S_A group of permutations of A and G an Abelian subgroup of G. Take $\sigma_A, \rho_A \in G$. That means that $[\sigma_A \circ \rho_A](x) = [\rho_A \circ \sigma_A](x)$, for all $x \in A$. Now take $B = \{b_1, \ldots, b_m\}$ and define $A \cup B = \{a_1, \ldots, a_n, b_1, \ldots, b_m\}$ and H as

[25] Take the plus sign to be just a delimiter as this operation will never be executed; for mathematical rigour we should define this in the context of a ring.

a group of all permutations of $A \cup B$. For every $\sigma_A \in G$ define $\sigma_{A\cup B} \in S_{A\cup B}$ as described in the theorem. We need to show that $S_{A\cup B}$ is an Abelian subgroup of H. Obviously, $H \subseteq S_{A\cup B}$, as $\sigma_{A\cup B} \in S_{A\cup B}$ is defined as $\sigma_{A\cup B} : A \cup B \to A \cup B$, i.e. it's a permutation of $A \cup B$ and therefore contained in H. Take $\sigma_{A\cup B}, \rho_{A\cup B} \in H$. Their composition $\sigma_{A\cup B} \circ \rho_{A\cup B}$ is also in H: as $\sigma_{A\cup B}(x) = \sigma_A(x)$, for some $\sigma_A \in G$, for all $x \in A$ and as $\rho_{A\cup B}(x) = \rho A(x)$, for some $\rho_A \in G$, for all $x \in A$, then, as G is a subgroup, it's also true that $\sigma_A \circ \rho_A \in G$; therefore $[\sigma_{A\cup B} \circ \rho_{A\cup B}](x) = [\sigma_A \circ \rho_A](x)$, for all $x \in A$. Obviosly all the other $x \in B$ take values $[\sigma_{A\cup B} \circ \rho_{A\cup B}](x) = \sigma_{A\cup B}(\rho_{A\cup B}(x)) = \sigma_{A\cup B}(x) = x$. Now, if $\sigma_{A\cup B} \in H$ is then $\sigma^{-1}_{A\cup B} \in H$? Well, if $\sigma_{A\cup B}(x) = \sigma_A(x)$, for all $x \in A$ and for some $\sigma_A \in G$, then, also $\sigma^{-1}_A \in G$. So define $\sigma^{-1}_{A\cup B}(x) = \sigma^{-1}_A(x)$, for all $x \in A$ and $\sigma^{-1}_{A\cup B}(x) = x$, for all $x \in B$ (identity part is its own inverse here). So, H is closed with respect to inverses. Now, take $\sigma_{A\cup B}, \rho_{A\cup B} \in S_{A\cup B}$. We have $[\sigma_{A\cup B} \circ \rho_{A\cup B}](x) = [\sigma_A \circ \rho_A](x)$, for all $x \in A$ and for some $\sigma_A, \rho_A \in G$. But, G is an Abelian subgroup so, $\sigma_A \circ \rho_A = \rho_A \circ \sigma_A$. We have that $[\sigma_{A\cup B} \circ \rho_{A\cup B}](x) = [\rho_A \circ \sigma_A](x) = [\rho_{A\cup B} \circ \sigma_{A\cup B}](x)$, for all $x \in A$. Now, for all $x \in B$, $[\sigma_{A\cup B} \circ \rho_{A\cup B}](x) = x$, but also $[\rho_{A\cup B} \circ \sigma_{A\cup B}](x) = x$. So, $[\sigma_{A\cup B} \circ \rho_{A\cup B}](x) = [\rho_{A\cup B} \circ \sigma_{A\cup B}](x)$, for all $x \in B$. Therefore H is an Abelian subgroup of $S_{A\cup B}$.

□

Problem. Find a four-element Abelian subgroup of S_5. Write its table.

Solution. The construction of such group can be taken from previous problem by using previous theorem. We can take:

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \qquad f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix},$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}.$$

It's easy to see that the following table is then valid for these permutations:

$\circ$	ϵ	f	g	h
ϵ	ϵ	f	g	h
f	f	ϵ	h	g
g	g	h	ϵ	f
h	h	g	f	ϵ

With that in mind, it's easy to see that group $\{\epsilon, f, g, h\}$ is an Abelian subgroup of S_5.

Problem. The subgroup of S_5 generated by

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix},$$

has six elements. List them, then write the table of this group.

Solution. First, we will find g^{-1} and h^{-1}. That is:

$$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}, \quad h^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}.$$

Notice that $g = g^{-1}$, that is, g is its own inverse. Therefore, $g \circ g = \epsilon$. Now, to find the rest, we have:

$$g \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}, \qquad h \circ g \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}.$$

$$g \circ h \circ g \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix},$$

Notice that $g \circ h \circ g \circ h = h^{-1}$, we can try and see what happens when we compose this further with g. But notice also that we did not verify $g \circ g \circ h$, as due to associativity, and the fact that g is its own inverse it's true that $g \circ (g \circ h) = (g \circ g) \circ h = \epsilon \circ h = h$. Further:

$$g \circ h^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}.$$

This is $g \circ h^{-1} = h \circ g \circ h$. Now, finally (we need not chech $h^{-1} \circ g^{-1}$ or the other way round as $g = g^{-1}$):

$$h^{-1} \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix},$$

which is $h^{-1} \circ g = h \circ g \circ h$. We will denote $g = g^{-1}$, then $g \circ h = f$, then $h \circ g \circ h = i$ and $h^{-1} = j$. Also:

$$h \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix},$$

that is, $h \circ g = g \circ h = f$. Now, we need $h \circ h$:

$$h \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix},$$

which is really $h^{-1} = j$. The multiplication table is:

$\circ$	ϵ	f	g	h	i	j
ϵ	ϵ	f	g	h	i	j
f	f	j	h	i	ϵ	g
g	g	h	ϵ	f	j	i
h	h	i	f	j	g	ϵ
i	i	ϵ	j	g	h	f
j	j	g	i	ϵ	f	h

Problem. In each of the following, A is the subset of $\mathbb{R}$ and G is a set of permutations of A. Show that G is a subgroup of S_A, and write the table of G.

1. A is the set of all $x \in \mathbb{R}$ such that $x \neq 0, 1$. $G = \{\epsilon, f, g\}$, where $f(x) = \frac{1}{1-x}$ and $g(x) = \frac{x-1}{x}$;

2. A is the set of all the nonzero real numbers. $G = \{\epsilon, f, g, h\}$, where $f(x) = \frac{1}{x}$, $g(x) = -x$ and $h(x) = -\frac{1}{x}$;

3. A is the set of all the real numbers $x \neq 0, 1$. $G = \{\epsilon, f, g, h, j, k\}$, where $f(x) = 1 - x$, $g(x) = \frac{1}{x}$, $h(x) = \frac{1}{1-x}$, $j(x) = \frac{x-1}{x}$ and $k(x) = \frac{x}{x-1}$;

Solution.

1. *A is the set of all $x \in \mathbb{R}$ such that $x \neq 0, 1$. $G = \{\epsilon, f, g\}$, where $f(x) = \frac{1}{1-x}$ and $g(x) = \frac{x-1}{x}$.* It's obvious that $f : A \to A$ and $g : A \to A$, so they are permutations of A and therefore in S_A. So, $G \subset S_A$. Now, to find the compositions:

$$[g \circ f](x) = \frac{\frac{1}{1-x} - 1}{\frac{1}{1-x}} = \frac{\frac{x}{1-x}}{\frac{1}{1-x}} = x.$$

Obviously $f \circ g = \epsilon$. Further:

$$[f \circ g](x) = \frac{1}{1 - \frac{x-1}{x}} = \frac{1}{\frac{1}{x}} = x.$$

So, $f \circ g = g \circ f = \epsilon$. This means that G is closed with respect to inverses. Last,

$$[f \circ f](x) = \frac{1}{1 - \frac{1}{1-x}} = \frac{1}{\frac{-x}{1-x}} = \frac{x-1}{x} = g(x),$$

$$[g \circ g](x) = \frac{\frac{x-1}{x} - 1}{\frac{x-1}{x}} = \frac{\frac{-1}{x}}{\frac{x-1}{x}} = \frac{1}{1-x} = f(x).$$

So, G is closed under composition and, in conclusion, G is a subgroup of S_A. Table:

$\circ$	ϵ	f	g
ϵ	ϵ	f	g
f	f	g	ϵ
g	g	ϵ	f

2. *A is the set of all the nonzero real numbers. $G = \{\epsilon, f, g, h\}$, where $f(x) = \frac{1}{x}$, $g(x) = -x$ and $h(x) = -\frac{1}{x}$.* As in previous example it's obvious that f, g and h are permutations of A. Now, $f(g(x)) = g(f(x)) = -\frac{1}{x} = h(x)$. Also, $h(f(x)) = f(h(x)) = -x = g(x)$. Then, $g(h(x)) = h(g(x)) = \frac{1}{x} = f(x)$. So, G is closed under composition. Now, $g(g(x)) = x$, $f(f(x)) = x$ and $h(h(x)) = x$, i.e. every element in G is its own inverse. Thus, G is a subgroup of S_A. Table:

$\circ$	ϵ	f	g	h
ϵ	ϵ	f	g	h
f	f	ϵ	h	g
g	g	h	ϵ	f
h	h	g	f	ϵ

3. *A is the set of all the real numbers $x \neq 0, 1$. $G = \{\epsilon, f, g, h, j, k\}$, where $f(x) = 1 - x$, $g(x) = \frac{1}{x}$, $h(x) = \frac{1}{1-x}$, $j(x) = \frac{x-1}{x}$ and $k(x) = \frac{x}{x-1}$.* Obviously, f, g, h and j are permutations of A. The following calculations will explicitly give us the table and show that closure under composition is valid, as well as that every element has an inverse:

$$\begin{aligned}
[g \circ f](x) &= g(f(x)) = g(1-x) = \frac{1}{1-x} = h(x), \\
[f \circ g](x) &= 1 - \frac{1}{x} = \frac{x-1}{x} = j(x), \\
[h \circ f](x) &= \frac{1}{1-1+x} = \frac{1}{x} = g(x), \\
[f \circ h](x) &= 1 - \frac{1}{1-x} = \frac{x}{x-1} = k(x),
\end{aligned}$$

$$
\begin{aligned}
[h \circ g](x) &= \frac{1}{1-\frac{1}{x}} = \frac{1}{\frac{x-1}{x}} = \frac{x}{x-1} = k(x), \\
[g \circ h](x) &= \frac{1}{\frac{1}{1-x}} = 1-x = f(x), \\
[j \circ f](x) &= \frac{1-x-1}{1-x} = \frac{x}{x-1} = k(x), \\
[f \circ j](x) &= 1-\frac{x-1}{x} = \frac{x-x+1}{x} = \frac{1}{x} = g(x),
\end{aligned}
$$

$$
\begin{aligned}
[g \circ j](x) &= \frac{x}{x-1} = k(x), \\
[j \circ g](x) &= \frac{\frac{1}{x}-1}{\frac{1}{x}} = \frac{\frac{1-x}{x}}{\frac{1}{x}} = 1-x = f(x), \\
[h \circ j](x) &= \frac{1}{1-\frac{x-1}{x}} = \frac{1}{\frac{1}{x}} = x = \epsilon(x), \\
[j \circ h](x) &= \frac{\frac{1}{1-x}-1}{\frac{1}{1-x}} = \frac{\frac{x}{1-x}}{\frac{1}{1-x}} = x = \epsilon(x),
\end{aligned}
$$

$$
\begin{aligned}
[f \circ k](x) &= 1-\frac{x}{x-1} = \frac{1}{1-x} = h(x), \\
[k \circ f](x) &= \frac{x-1}{x} = j(x), \\
[g \circ k](x) &= \frac{x-1}{x} = j(x), \\
[k \circ g](x) &= \frac{\frac{1}{x}}{\frac{1}{x}-1} = \frac{\frac{1}{x}}{\frac{1-x}{x}} = \frac{1}{1-x} = h(x),
\end{aligned}
$$

$$
\begin{aligned}
[h \circ k](x) &= \frac{1}{1-\frac{x}{x-1}} = \frac{1}{\frac{1}{1-x}} = 1-x = f(x), \\
[k \circ h](x) &= \frac{\frac{1}{1-x}}{\frac{1}{1-x}-1} = \frac{\frac{1}{1-x}}{\frac{x}{1-x}} = \frac{1}{x} = g(x), \\
[j \circ k](x) &= \frac{\frac{x}{x-1}-1}{\frac{x}{x-1}} = \frac{\frac{1}{x-1}}{\frac{x}{x-1}} = \frac{1}{x} = g(x), \\
[k \circ j](x) &= \frac{\frac{x-1}{x}}{\frac{x-1}{x}-1} = \frac{\frac{1-x}{x}}{\frac{1}{x}} = 1-x = f(x),
\end{aligned}
$$

$$
\begin{aligned}
[f \circ f](x) &= 1-(1-x) = x = \epsilon(x),\\
[g \circ g](x) &= \frac{1}{\frac{1}{x}} = x = \epsilon(x),\\
[h \circ h](x) &= \frac{1}{1-\frac{1}{1-x}} = \frac{1}{\frac{x}{x-1}} = \frac{x-1}{x} = j(x),\\
[j \circ j](x) &= \frac{\frac{x-1}{x}-1}{\frac{x-1}{x}} = \frac{\frac{1}{x}}{\frac{1-x}{x}} = \frac{1}{1-x} = h(x),\\
[k \circ k](x) &= \frac{\frac{x}{x-1}}{\frac{x}{x-1}-1} = \frac{\frac{x}{x-1}}{\frac{1}{x-1}} = x = \epsilon(x).
\end{aligned}
$$

It is evident now that G is a subgroup of S_A with the following table:

$\circ$	ϵ	f	g	h	j	k
ϵ	ϵ	f	g	h	j	k
f	f	ϵ	j	k	g	h
g	g	h	ϵ	f	k	j
h	h	g	k	j	ϵ	f
j	j	k	f	ϵ	h	g
k	k	j	h	g	f	ϵ

Problem. For each integer n, define f_n by $f_n(x) = x + n$.

1. Prove that for each integer n, f_n is a permutation of $\mathbb{R}$, that is, $f_n \in S_{\mathbb{R}}$;
2. Prove that $f_n \circ f_m = f_{n+m}$ and $f^{-1} = f_{-n}$;
3. Let $G = \{f_n : \ n \in \mathbb{Z}\}$. Prove that G is a subgroup of $S_{\mathbb{R}}$;
4. Prove that G is cyclic. (Indicate a generator of G.)

Solution.

1. *Prove that for each integer n, $f_n(x) = x + n$ is a permutation of $\mathbb{R}$, that is, $f_n \in S_{\mathbb{R}}$.* We need to show that f_n is a bijection of the form $f_n : \mathbb{R} \to \mathbb{R}$. Obviously, $\mathrm{Im} f = \mathbb{R}$ as addition is closed in the set of real numbers, i.e. if we take $y \in R$ then there is $x \in \mathbb{R}$, $x = y - n$ so that $y = x + n$, makin f_n surjective. If we take $f_n(a) = f_n(b)$, then $a + n = b + n$, which implies $a = b$. Thus, f_n is injective and therefore, because it is also surjective, it is bijective. As it's domain is the same as its codomain, that is $\mathbb{R}$, it is a permutation of $\mathbb{R}$, by definition.

2. *Prove that $f_n \circ f_m = f_{n+m}$ and $f^{-1} = f_{-n}$.* See that $[f_n \circ f_m](x) = (x+m)+n = x + (m+n) = f_{m+n}(x)$. Then, as in previous problem we had $x = y - n$, then $f^{-1}(x) = x - n$; we can chech that by $[f \circ f^{-1}](x) = (x - n) + n = x$ and $[f^{-1} \circ f](x) = (x + n) - n = x$. Thus, $f^{-1}(x) = x - n = x + (-n) = f_{-n}(x)$.

3. *Let $G = \{f_n : \ n \in \mathbb{Z}\}$. Prove that G is a subgroup of $S_\mathbb{R}$.* We have already proved that f_n is a permutation for every $n \in \mathbb{Z}$, so $G \subset S_\mathbb{R}$. Then, if we take $f_n, f_m \in G$, from the second problem, it follows that its composition f_{n+m} is in G, as $n+m \in \mathbb{Z}$, for every $n, m \in \mathbb{Z}$. From the third problem we have that there is an inverse for every $f_n \in G$ and that is f_{-n} and if $n \in \mathbb{Z}$, then $-n \in \mathbb{Z}$. In conclusion, G is a subgroup of $S_\mathbb{R}$.

4. *Prove that G is cyclic.* We can take $\langle f_1 \rangle$ as the generator of G. Then, it must also contain it's inverse f_{-1}. Obviously we can get a neutral element by $f_1 \circ f_{-1}$ and $f_{-1} \circ f_1$. Now, for every $n \in \mathbb{N}$, we can have f_{-n} by taking $\underbrace{f_{-1} \circ \ldots \circ f_{-1}}_{n \text{ times}}$ which can be shown to be valid by mathematical induction. We take $n = 1$ for a base and then we have just f_{-1}. Suppose that for some n we have f_{-n} by the forementioned line of reasoning. Then we need to prove that for $(n+1)$ we have $f_{-(n+1)}$. See that $f_{-1} \circ f_{-n} = (x + (-n)) + (-1) = x + (-(n+1)) = f_{-(n+1)}$. As, by assumption of induction we got f_{-n} by applying composition of f_{-1} n times, we got $f_{-(n+1)}$ by applying f_{-1} one more time and that is $(n+1)$ times. By the same reasoning we prove that we have f_n by composing f_1 with itself n times (actually $n-1$ times, if we want to be rigorous about the linguistic part of what the author is trying to say, but the point is clear). Therefore, G is cyclic and $G = \langle f_1 \rangle$.

Problem. For any pair of real numbers $a \neq 0$ and b, define a function $f_{a,b}$ as follows: $f_{a,b}(x) = ax + b$.

1. Prove that $f_{a,b}$ is a permutation of $\mathbb{R}$, that is, $f_{a,b} \in S_\mathbb{R}$;
2. Prove that $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$;
3. Prove that $f_{a,b}^{-1} = f_{\frac{1}{a},-\frac{b}{a}}$;
4. Let $G = \{f_{a,b} : \ a, b \in \mathbb{R}, \ a \neq 0\}$. Show that G is a subgroup of $S_\mathbb{R}$.

Solution.

1. *Prove that $f_{a,b} = ax + b$ is a permutation of $\mathbb{R}$, that is, $f_{a,b} \in S_\mathbb{R}$.* We're dealing with a linear function here, we know it to be of the form $f_{a,b} : \mathbb{R} \to \mathbb{R}$ and that it is bijective. Therefore $f_{a,b} \in S\mathbb{R}$ (the reader can easily check it the same way as in previous problem).

2. *Prove that $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$.* See that $[f_{a,b} \circ f_{c,d}](x) = a(cx + d) + b = (ac)x + (ad + b) = f_{ac,ad+b}(x)$.

3. *Prove that* $f_{a,b}^{-1} = f_{\frac{1}{a},-\frac{b}{a}}$. Take $x \in \mathrm{cod} f = \mathbb{R}$. We need to find such $y \in \mathrm{dom} f = \mathbb{R}$ so that $x = f(y)$. We have $x = ay + b$ and that is $x - b = ay$, i.e. $y = \frac{1}{a}x - \frac{b}{a}$. We can take $f_{a,b}^{-1}(x) = y$ and then it is $f_{a,b}^{-1} = \frac{1}{a}x - \frac{b}{a} = f_{\frac{1}{a},-\frac{b}{a}}$. Obviously, by previous problem $f_{a,b} \circ f_{\frac{1}{a},-\frac{b}{a}} = f_{a\circ\frac{1}{a},-a\frac{b}{a}+b} = f_{1,0}$, which is a neutral element, as $f_{1,0}(x) = x$, obviously an identity function.

4. *Let* $G = \{f_{a,b} : \ a, b \in \mathbb{R}, \ a \neq 0\}$. *Show that* G *is a subgroup of* $S_{\mathbb{R}}$. From the first problem, we proved that if $f_{a,b} \in G$, then $f_{a,b} \in S_{\mathbb{R}}$, so $G \subset S_{\mathbb{R}}$. Then, the second problem tells us that G is closed with respect to composition and the third that it's closed with respect to inverses. Therefore, G is a subgroup of $S_{\mathbb{R}}$.

Definition. The **symmetries of a polynomial** p are all the permutations of the subscripts which leave p unchanged. They form a group of permutations.

Problem. List the symmetries of each of the following polynomials, and write their group table.

1. $p = x_1x_2 + x_2x_3$;
2. $p = (x_1 - x_2)(x_2 - x_3)(x_1 - x_3)$;
3. $p = x_1x_2 + x_2x_3 + x_1x_3$;
4. $p = (x_1 - x_2)(x_3 - x_4)$.

Solution.

1. $p = x_1x_2 + x_2x_3$. The polynomial remains unchanged if we switch x_1 with x_3:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Obviously we have the identity ϵ and the inverse of f which is, easy to see, f itself. Therefore the table is:

$\circ$	ϵ	f
ϵ	ϵ	f
f	f	ϵ

2. $p = (x_1 - x_2)(x_2 - x_3)(x_1 - x_3)$. One can easily see that the polynomial remains equal for even commutations of members in the brackets. Notice that, for odd commutations, it will be of opposite sign, e.g. $p \neq -(x_2 - x_1)(x_2 - x_3)(x_1 - x_3)$. But, to analyze the first case, we change the order of subtraction in the first

and third brackets. We have $p = (x_2 - x_1)(x_2 - x_3)(x_3 - x_1)$. Notice that we can put these into correspondence with the first polynomial by permuting the order of bracket multiplication (notice that x_1 appears in first and last brackets twice as first member, and in the second polynomial it's the same with x_2), i.e. $p = (x_2 - x_1)(x_3 - x_1)(x_2 - x_3)$. Now, we notice that it still differs from the first polynomial (considering notation) as in the original, x_3 appears twice in second and third brackets as the second member. So we permute again, but only the first and third in our new polynomial to obtain $p = (x_2 - x_3)(x_3 - x_1)(x_2 - x_1)$. It's easy to see that now we can put indices in correspondence by:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Now, by the same reasoning we can obtain $p = (x_1 - x_2)(x_3 - x_2)(x_3 - x_1)$ (by switching members in second and third parentheses). We permute the brackets to correspond with original and get $p = (x_3 - x_1)(x_1 - x_2)(x_3 - x_2)$. Now we see that indices can be put into correspondence by

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

By careful examination, one can see that, by interchanging members in first and second parentheses, there is no way that indices of $p = (x_2 - x_1)(x_3 - x_2)(x_1 - x_3)$ can be put into correspondence (by means of permutation, at least) with the indices of the original. Therefore, we are only left with f and g. It's now easy to see that $fg = gf = \epsilon$, $ff = g$ and $gg = f$. So, we have a table:

$\circ$	ϵ	f	g
ϵ	ϵ	f	g
f	f	g	ϵ
g	g	ϵ	f

3. $p = x_1x_2 + x_2x_3 + x_1x_3$. Polynomial $p = x_3x_1 + x_1x_2 + x_3x_2$ is equal to the forementioned one and can be obtained by permutation:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Furthermore, polynomial $p = x_2x_1 + x_1x_3 + x_2x_3$ can be obtained by:

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Polynomial $p = x_2x_3 + x_3x_1 + x_2x_1$ is obtained from the first one by permutation:

$$h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Now, we have $p = x_1x_3 + x_3x_2 + x_1x_2$ by:

$$j = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Finally, exempting a trivial neutral element we have $p = x_3x_2 + x_2x_1 + x_3x_1$ obtained by permutation:

$$k = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Multiplication table is as follows:

$\circ$	ϵ	f	g	h	j	k
ϵ	ϵ	f	g	h	j	k
f	f	h	j	ϵ	k	g
g	g	k	ϵ	j	h	f
h	h	ϵ	k	f	g	j
j	j	g	f	k	ϵ	h
k	k	j	h	g	f	ϵ

4. $p = (x_1 - x_2)(x_3 - x_4)$. If we switch x_1 and x_4, we also have to switch x_2 and x_3 so we have $p = (x_4 - x_3)(x_2 - x_1)$ (obviously equal to our initial polynomial as we did an even number of permutations on operation of subtraction). That corresponds to:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Also, we can exchange x_1 with x_2 and x_3 with x_4 to get $p = (x_2 - x_1)(x_4 - x_3)$ (it's equal to the initial polynomial for the same reason as in previous permutation). So we have:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Furthermore, we can permute indices so that we have $p = (x_3 - x_4)(x_1 - x_2)$ which is represented by:

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Note that $f^{-1} = f$, $g^{-1} = g$ and $h^{-1} = h$. Also, $fg = gf = h$, $fh = hf = g$ and $gh = hg = f$, so we have the following table of multiplication:

$\circ$	ϵ	f	g	h
ϵ	ϵ	f	g	h
f	f	ϵ	h	g
g	g	h	ϵ	f
h	h	g	f	ϵ

Problem. Let A be a set and $a \in A$. Let G be the subset of S_A consisting of all the permutations f of A such that $f(a) = a$. Prove that G is a subgroup of S_A.

Solution. It's true that $G \subseteq S_A$, so we first have to prove that for some $f, g \in G$ it's true that $fg \in G$. Now, as $f, g \in G$, then $f(a) = a$ and $g(a) = a$ for some $a \in A$. But, $f(g(a)) = f(a) = a$, and as G contains all permutations in S_A with this property, it must contain fg, i.e. $fg \in G$. If $f \in G$, then $f(a) = a$. As S_A is a group there is $f^{-1} \in S_A$, such that $ff^{-1} = f^{-1}f = \epsilon$, i.e. $f(f^{-1}(x)) = f^{-1}(f(x)) = x$, for all $x \in A$. Therefore, from $f(a) = a$ we have $f^{-1}(f(a)) = f^{-1}(a)$, that is $a = f^{-1}(a)$. As this is true, then $f^{-1} \in G$ and by that it follows that G is a subgroup of S_A.

Problem. If f is a permutation of A and $a \in A$, we say that f *moves* a if $f(a) \neq a$. Let A be an infinite set, and let G be the subset of S_A which consists of all the permutations f of A which move only a finite number of elements of A. Prove that G is a subgroup of S_A.

Solution. Obviously, $G \subset S_A$. Let P_n denote the set $\{p_1, \ldots, p_n\}$, for some $n \in \mathbb{N}$. Take $f, g \in G$. We need to show that $fg \in G$. It's true that $f(p_i) \neq p_i$ and $g(p_i) \neq p_i$, for all $i = \{1, \ldots, n\}$. That can be written as $f(p_i), g(p_i) \in A \backslash P_n$. We need to show that $f(g(p_i)) \neq p_i$. As $g(p_i) \neq p_i$, we need to check what happens with $f(a)$ where $a = g(p_i) \in A \backslash P_n$. If $f(a) = p_i$ then it would mean that f moves a and it would be in P_n, leading to a contradiction. Therefore, it must be that $f(a)$ is a, i.e. $f(g(p_i)) = g(p_i) \neq p_i$, for all i. Therefore, $fg \in G$. Now, if we take $f \in G$, we need to check whether $f^{-1} \in G$. As $f(p_i) \neq p_i$, suppose that $f^{-1}(p_i) = p_i$. Then it would mean that $f(f^{-1}(p_i)) = f(p_i)$, i.e. $p_i = f(p_i)$, which is a contradiction to the assumption that f moves all p_i. Therefore, $f^{-1} \in G$ and, by that, G is a subgroup of S_A.

Problem. Let A be a finite set, and B a subset of A. Let G be the subset of S_A consisting of all the permutations f of A such that $f(x) \in B$ for every $x \in B$. Prove that G is a subgroup of S_A. Give an example to show that the conclusion is not necessarily true if A is an infinite set.

Solution. As $G \subseteq S_A$ by definition, we need only check composition. A careful reader should remember that if $G \subset S_A$ and G is closed with respect to composition and finite, then G is a subgroup of S_A. Take $f, g \in G$. Then, $f(x) \in B$ and $g(x) \in B$ for every $x \in B$. It's easy to see that $f(g(x)) \in B$ as $a = g(x) \in B$ for all $x \in B$ and $f(a) \in B$ because $a = g(x) \in B$, for all $x \in B$. Now, if we were to take in consideration inverses, we would be left with vague and unclear expressions. If we were to consider $f^{-1}(f(x)) = x$, we would have that $f(x) \in B$ for all $x \in B$. Now, all information that we have is that always $f^{-1}(f(x)) \in B$ for all $x \in B$. Actually, $f^{-1}(y) \in B$ whenever $y = f(x)$ and $f(x) \in B$, but that leaves a lot of empty spaces for some y that are in B but are not equal to $f(x)$; in other words we don't know how $f(x)$ behaves. So we have to call upon the previous problem, that A is finite (and by that S_A also). Then, without checking inverses, we know that G is a subgroup of S_A only by the fact that it's closed with respect to composition and that $G \subseteq S_A$. *Comment.* Now, we will give a counterexpamle, why G is not a subgroup of S_A if A is infinite. We can take $A = \mathbb{Q}$. Now S_A will contain permutations $f_a : A \to A$ with $f_a = ax$, where $a \in \mathbb{Q}$. Now if we take $B = \mathbb{N}$, presumed group G will contain $f_b : A \to A$ with $f_b = bx$ where $b \in \mathbb{N}$ (it will leave elements in $\mathbb{N}$ fixed and will therefore be in G). It will be closed with respect to multiplication as $[f_a \circ f_b](x) = abx$ and $ab \in \mathbb{N}$, but the inverses will be a problem as $f_b^{-1}(x) = \frac{1}{bx} = \frac{1}{b}x$ and $\frac{1}{b} \notin \mathbb{N}$ unless $b = 1$.

Finite groups of permutations

Definition. Every permutation $f : A \to A$, where A is finite, for which exists some $a \in A$ such that $[f \circ f \circ \cdots \circ f](a) = a$ and $[f \circ f](a) \neq a$ and $[f \circ f](x) = x$, for all $x \in A \backslash \{a\}$, is called a **cycle**.

Example. Following permutation is a cycle:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}.$$

Such permutation can be also written as $f = (2\ 4\ 5)$ to signify that f moves 2 to 4 then 4 to 5 and finally 5 to 2. We can write that fact down also as $2 \to 4 \to 5 \to 2$.

Example. In previous example, f was a cycle. Let's observe a permutation that is not a cycle:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

We can see that $2 \to 4 \to 5 \to 2$, but the other elements do not remain fixed as $1 \to 3 \to 1$. But now, g can be written down as a composition of two disjoint (they share no elements in common while completing a cycle) cycles $g_1 = (2\ 4\ 5)$ and $g_2 = (1\ 3)$ such that $g = g_1 \circ g_2$. We can easily see that it will really produce g (we can write that fact down as $g = (2\ 4\ 5)(1\ 3)$). Now we have a sufficient reason to believe that the following theorem holds and can be proved.

Theorem. Every permutation that is not identity is either a cycle or a composition of disjoint cycles.

Proof. Assume that $f : A \to A$ is not identity, i.e. there are some $x \in A$ for which $f(x) \neq x$. Now we take that x (we will denote it by x_1) and take $f(x_1) = x_2$. If $f(x_2) = x_1$ we have a first cycle. If not, we follow $f(x_2) = x_3$ and so on. We either (as we're dealing with a finite group) exhaust all the elements and thus the permutation is a (single) cycle, or we reach a repetition for x_k in the chain $x_1 \to x_2 \to \cdots \to x_k$, for some $k < |A|$. It's easy to see that it must be $f(x_k) = x_1$, as if it were some other x_i it would follow that $f(x_{i-1}) = x_i$ and $f(x_k) = x_i$ and that would indicate a breach of definition of permutation as an injection and by that as a bijection. Next, we choose another element $y_1 \in A$ for which $f(y_1) \neq y_1$ and do the same line of reasoning. As there is a finite number of elements in A, we have to reach the end sooner or later. Taking composition of those cycles gives the permutation we started with, as they are

all disjoint (if they were not it would mean that some $f(x_i) = y_j$ for some $i, j \leq |A|$, again implicating a breach in definition of permutation as also $f(x_i) = x_{i+1}$).

□

Lemma. Disjoint cycles commute.

Proof. Follows directly from the fact that they are disjoint, e.g. if we take $f = f_1 f_2$ such that $f_1 = (a_1 \dots a_k)$ and $f_2 = (a_{k+1} \dots a_n)$, then, f_2 will permute elements $a_{k+1} \dots a_n$ leaving others unchanged (the ones for f_1). Similarly, if we take f_1 first it will leave elements which f_2 permutes unchanged.

□

Definition. If $f = (a_1 \dots a_n)$ is a cycle, then n is called the **length of the cycle** f.

Theorem. Decomposition of a permutation into cycles is unique up to the order of the cycles.

Proof. Suppose that $f = f_1 f_2 \cdots f_n$ and $f' = g_1 g_2 \cdots g_m$, where f_i, g_j are cycles for all $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, m\}$, where $n < m$. Then $f_1 f_2 \cdots f_n = g_1 g_2 \cdots g_m$. But, as all f_i and g_j are permutations, they are also bijections and have inverse elements. Therefore, we can take $g_1^{-1} f_1 f_2 \cdots f_n = g_2 \cdots g_m$. Now, there must be some f_i that shares some element with g_1^{-1}. If that were not so, that would mean that for f some element remains fixed, while for f' it does not and $f \neq f'$, leading to contradiction. So, suppose that f_1, without loss of generality shares some element in common with g_1^{-1} (by previous lemma they commute). Because cycles are disjoint, no other f_i can have that same element, and due to the fact that permutations are functions and bijections, it must be that $g_1^{-1} f_1 = \epsilon$. Using the same process we arrive at $\epsilon = g_{n+1} \cdots g_m$, meaning that we can disregard $g_{n+1} \cdots g_m$. So it must be that $f = f'$.

□

Problem. Compute each of the following products in S_9:

1. (1 4 5)(3 7)(6 8 2);
2. (1 7)(6 2 8)(9 3 5 4);
3. (7 1 8 2 5)(3 6)(4 9);
4. (1 2)(3 4 7);
5. (1 4 7)(1 6 7 8)(7 4 1 3 2);

6. (6 1 4 8)(2 3 4 5)(1 2 4 9 3).

Solution. We have to remind ourselves that first operations performed are those on the right and observe what happens for every $i \in \{1, 2, \ldots, 9\}$.

1. (1 4 5)(3 7)(6 8 2). First cycle leaves 1 fixed, second one also, but the third one carries it to 4. First cycle carries 2 to 6 and all the others leave 6 fixed. First cycle leaves 3 fixed, second carries it to 7 and third one leaves 7 fixed. Thus reasoning we arrive at:

$$(1\ 4\ 5)(3\ 7)(6\ 8\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 7 & 5 & 1 & 8 & 3 & 2 & 9 \end{pmatrix}.$$

2. (1 7)(6 2 8)(9 3 5 4). We have that:

$$(1\ 7)(6\ 2\ 8)(9\ 3\ 5\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 5 & 9 & 4 & 2 & 1 & 6 & 3 \end{pmatrix}.$$

3. (7 1 8 2 5)(3 6)(4 9). After composition it's:

$$(7\ 1\ 8\ 2\ 5)(3\ 6)(4\ 9) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 6 & 9 & 7 & 3 & 1 & 2 & 4 \end{pmatrix}.$$

4. (1 2)(3 4 7). The result is simply:

$$(1\ 2)(3\ 4\ 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 4 & 7 & 5 & 6 & 3 & 8 & 9 \end{pmatrix}.$$

5. (1 4 7)(1 6 7 8)(7 4 1 3 2). We have:

$$(1\ 4\ 7)(1\ 6\ 7\ 8)(7\ 4\ 1\ 3\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 2 & 6 & 5 & 1 & 7 & 4 & 9 \end{pmatrix}.$$

6. (6 1 4 8)(2 3 4 5)(1 2 4 9 3). After carefully performing compositions, as now they are not disjunct (same as in previos example, actually):

$$(6\ 1\ 4\ 8)(2\ 3\ 4\ 5)(1\ 2\ 4\ 9\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 9 & 2 & 1 & 7 & 6 & 8 \end{pmatrix}.$$

Problem. Write each of the following permutations in S_9 as a product of disjoint cycles:

$$\text{(a)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 2 & 5 & 1 & 7 & 6 & 8 & 3 \end{pmatrix};$$

$$\text{(b)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 9 & 2 & 3 & 8 & 1 & 6 & 5 \end{pmatrix};$$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 5 & 3 & 1 & 2 & 4 & 8 & 6 \end{pmatrix}$;

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix}$.

Solution.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 2 & 5 & 1 & 7 & 6 & 8 & 3 \end{pmatrix} = (1\ 4\ 5)(2\ 9\ 3)(6\ 7).$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 9 & 2 & 3 & 8 & 1 & 6 & 5 \end{pmatrix} = (1\ 7)(2\ 4)(3\ 9\ 5)(6\ 8).$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 5 & 3 & 1 & 2 & 4 & 8 & 6 \end{pmatrix} = (1\ 7\ 4\ 3\ 5)(2\ 9\ 6).$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix} = (1\ 9\ 2\ 8)(3\ 7\ 5).$

Definition. Cycles of length 2 are called **transpositions**.

Theorem. Every cycle can be written down as a composition of transpositions.

Proof. Let $a_1 \to a_2 \to a_3 \to \cdots \to a_n \to a_1$ be a cycle of length n denoted as $(a_1 a_2 \dots a_n)$. We have $f(a_i) = a_{i+1}$ for all $i \in \{1, \dots, n-1\}$ and $f(a_n) = a_1$. If we take composition $(a_1 a_3)(a_1 a_2)$ we have:

$$(a_1 a_3)(a_1 a_2) = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix} = (a_1 a_2 a_3).$$

By the same line of reasoning we see that we will have

$$(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2),$$

as a_1 will be carried to a_2 and a_2 doesn't appear again in the list. But, a_2 is carried to a_1 in the first transposition and to a_3 in the second which does not appear again; a_3 will be carried to a_1 in the second transposition and a_1 to a_4 in the third transposition. Meaning that a_i will be carried to a_{i+1} in i-th transposition, where $i \in \{1, \dots, n-1\}$. Special case, a_n will be carried to a_1 as a_n does not appear anywhere before.

□

Comment. Note that decomposition into transpositions need not be unique (as it is with disjoint cycles). We give a counterexample, and the reader can easily check that $(a_1a_4)(a_1a_3)(a_1a_2) = (a_4a_3)(a_4a_2)(a_4a_1) = (a_1a_2a_3a_4)$.

Problem. Express each of the following as a product of transpositions in S_8:

1. $(1\ 3\ 7\ 4\ 2\ 8)$,
2. $(4\ 1\ 6)\,(8\ 2\ 3\ 5)$,
3. $(1\ 2\ 3)\,(4\ 5\ 6)\,(1\ 5\ 7\ 4)$,
4. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 8 & 7 & 6 & 5 \end{pmatrix}$

Solution. For each of these problems we will fix one element from each cycle and from it develop all the transpositions. Notice that we are always going from right to left, as the rightmost composition gets executed first.

1. $(1\ 3\ 7\ 4\ 2\ 8) = (1\ 8)\,(1\ 2)\,(1\ 4)\,(1\ 7)\,(1\ 3)$.
2. $(4\ 1\ 6)\,(8\ 2\ 3\ 5) = (4\ 6)\,(4\ 1)\,(8\ 5)\,(8\ 3)\,(8\ 2)$.
3. $(1\ 2\ 3)\,(4\ 5\ 6)\,(1\ 5\ 7\ 4) = (1\ 3)\,(1\ 2)\,(4\ 6)\,(4\ 5)\,(1\ 4)\,(1\ 7)\,(1\ 5)$.
4. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 8 & 7 & 6 & 5 \end{pmatrix} = (6\ 7)\,(5\ 8)\,(1\ 2)\,(1\ 4)\,(1\ 3)\,.$

Problem. In S_5, write $(1\ 2\ 3\ 4\ 5)$ in five different ways as a cycle, and in five different ways as a product of transpositions.

Solution. It's easy to see that the cycle $(1\ 2\ 3\ 4\ 5)$ is invariant to rotations of elements, so we have $(2\ 3\ 4\ 5\ 1)$, $(3\ 4\ 5\ 1\ 2)$, $(4\ 5\ 1\ 2\ 3)$ and $(5\ 1\ 2\ 3\ 4)$ (five if we count the starting cycle). Now, as for transpositions, we have five elements to choose for a fixed element. So we have $(1\ 5)(1\ 4)(1\ 3)(1\ 2)$, $(2\ 1)(2\ 5)(2\ 4)(2\ 3)$, $(3\ 2)(3\ 1)(3\ 5)(3\ 4)$, $(4\ 3)(4\ 2)(4\ 1)(4\ 5)$ and $(5\ 4)(5\ 3)(5\ 2)(5\ 1)$.

Problem. In S_5, express each of the following as the square of a cycle: (a) $(1\ 3\ 2)$, (b) $(1\ 2\ 3\ 4\ 5)$, (c) $(1\ 3)(2\ 4)$.

Solution. (a) We have $(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$, so $(1\ 3\ 2) = (1\ 2\ 3)^2$. (b) By wild guess we can take $(1\ 4\ 2\ 5\ 3)(1\ 4\ 2\ 5\ 3) = (1\ 2\ 3\ 4\ 5)$, so $(1\ 2\ 3\ 4\ 5) = (1\ 4\ 2\ 5\ 3)^2$. (c) From the second proposition below it will be easy to see that $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$.

Proposition. Let f be a permutation of a finite set. If $f = (a_1a_2 \ldots a_{n-1}a_n)$, then $f^{-1} = (a_na_{n-1} \ldots a_2a_1)$.

Proof. It is sufficient to show that $ff^{-1} = \epsilon$. Now, applying f^{-1} first, we have $a_i \to a_{i-1}$, for all $i \in \{2, 3, \ldots, n\}$. From f we have $a_{i-1} \to a_i$, for all $i \in \{2, 3, \ldots, n\}$. Whenever we take a_i from f^{-1} it goes to a_{i-1}; then, applying f it goes back to a_i. Therefore, $f\left(f^{-1}(a_i)\right) = a_i$, meaning $ff^{-1} = \epsilon$ (of course, we need to mention that $a_1 \to a_n$ in f^{-1} and $a_n \to a_1$ in f, which obviously satisfies $ff^{-1} = \epsilon$ while composing). Also, if $ff^{-1} = \epsilon$, then it must be that $f^{-1}f = \epsilon$. Suppose we have that $gf = \epsilon$. It would mean that $gff^{-1} = f^{-1}$, giving $g = f^{-1}$ again. From this follows that f is indeed inverse of f^{-1}.

□

Proposition. Let f be a cycle $f = (a_1 a_2 \ldots a_n)$ where $n \in \mathbb{N}$. Then f^m, where $m \in \mathbb{N}$ and $n = km$, for some $k \in \mathbb{N}$, will be a product of m disjoint cycles $f_i = \left(a_i a_{i+m} a_{i+2m} \ldots a_{i+(k-1)m)}\right)$, where $i \in \{1, 2, \ldots, m\}$. Each f_i is of length k.

Proof. First we may consider following example as a motivation for our proof. Take $f = (1\ 2\ 3\ 4\ 5\ 6)$ and $m = 3$. Taking for $m = 2$ first and then for $m = 3$ we have:

$$\begin{aligned} f^2 &= (1\ 2\ 3\ 4\ 5\ 6)\,(1\ 2\ 3\ 4\ 5\ 6) = (1\ 3\ 5)\,(2\ 4\ 6)\,, \\ f^3 = ff^2 &= (1\ 2\ 3\ 4\ 5\ 6)\,(1\ 3\ 5)\,(2\ 4\ 6) = (1\ 4)\,(2\ 5)\,(3\ 6)\,. \end{aligned}$$

To proceed with the more general proof, we have that $n = km$, where $m, n, k \in \mathbb{N}$. So f can be written down as:

$$f = (a_1 a_2 \ldots a_{n-1} a_n) = (a_1 a_2 a_3 \ldots a_{km-1} a_{km})\,.$$

Before we continue, notice that $a_{i+n} = a_i$, for all $i \in \{1, 2, \ldots, n\}$. Observe what happens with a_1 when we take f^m. For $m = 2$, a_1 goes to a_2; for $m = 3$, a_1 goes to a_2 and then to a_3. Continuing in this way, we may conclude that for some m, a_1 will go to a_{1+m} when taking f^m. In other words, we skip m elements for every step. When we reach $a_{1+(k-1)m}$, we have reached the end. Due to the fact that $n = mk$, we have that $a_{1+(k-1)m} = a_{1+km-m} = a_{1+n-m}$ will go to a_{1+n} and that is a_1. That way, we complete one cycle and can do the rest for a_2, a_3 and all up to a_m (notice that there will be m of them) and they will be disjoint. Naturally, for a_m we'll be having $a_{m+(k-1)m}$ as the last element and that is a_n. As for each cycle i we had elements a_i, a_{i+m} ranging to $a_{i+(k-1)m}$, we have $\frac{i+(k-1)m-i}{m} + 1$ of them (e.g. from $2, 4, 6, 8, 10$ we have $\frac{10-2}{2} + 1 = 5$), and that is $\frac{(k-1)m}{m} + 1 = (k-1) + 1 = k$; in other words, length of each cycle is k.

□

Proposition. Let f be a cycle $f = (a_1 a_2 \dots a_p)$, where p is a prime number. Then every power of f is a cycle.

Proof. We will observe the case when $f = (a_1\ a_2\ a_3)$ and take $n = 2$. We will construct a sequence by repeating elements from f (preserving their order) n times. That way we obtain $a_1, a_2, a_3, a_1, a_2, a_3, a_1$. From that we construct a new sequence $A_1 = a_1$, $A_2 = a_2$, $A_3 = a_3$, $A_4 = a_1$ (notice that $A_4 = A_{1+3} = a_1$), $A_5 = a_2$ (see that $A_5 = A_{1+2\cdot 2}$, $A_6 = a_3$, $A_7 = a_1$; also, notice that $A_7 = A_{2\cdot 3+1}$). Now, as we take steps while composing permutations with itself, we always skip one member (when taking a power of 2), that is from A_1 we get to A_3 then to A_5 and then to A_7 which is a_1. This way, we enclosed a cycle using all elements from f.

Now we will prove this for f^n when $n \in \mathbb{N}$ and p (length of f) is prime. We construct a sequence such that $A_{i+kp} = a_i$, for $i \in \{1, 2, \dots, p\}$ and $k \in \{0, 1, 2, \dots, n-1\}$, and $A_{np+1} = a_1$. Now, when taking a power of n, we skip every n members in the sequence, that is, we start from A_1, get to A_{1+n} then to A_{1+2n} and so on (always of the form A_{1+mn}, where $m \in \mathbb{N}$). We can see that we will arrive at A_{np+1-n} as it's $A_{np+1-n} = A_{1+(p-1)n}$ (here $m = p-1$). In the next step we will complete the cycle as we will have $A_{1+(p-1)n+n} = A_{1+pn-n+n} = A_{1+pn} = a_1$. The whole sequence is of length $np + 1$. And for skipping n steps (and disregarding the last $A_{np+1} = a_1$), obviously, length of the subsequence (disregarding, again, the last one) is $\frac{np}{n} = p$. The new sequence is $A_1, A_{1+n}, A_{1+2n}, \dots, A_{1+(p-1)n}$. Suppose two of those elements are equal, i.e. $A_{1+m_1 n} = A_{1+m_2 n}$, but $m_1 \neq m_2$. Take $A_{1+m_1 n} = A_{i+k_1 p}$ and $A_{1+m_2 n} = A_{i+k_2 p}$. Now, from $m_1 n = i - 1 + k_1 p$ (and $1 \leq i \leq p$, i.e. $0 \leq i - 1 \leq p - 1 < p$) we have that $m_1 n$ divided by p yields $i - 1$ as a remainder. Same thing goes for $m_2 n$. That would mean that $m_1 n = m_2 n + pq$ for some $q \in \mathbb{Z}$, i.e. $m_1 \equiv m_2 \pmod{p}$. That would be possible for $m_2 = m_1 + pt$, where $t \in \mathbb{Z}$, but m_1 and m_2 are both positive and less than p, so there does not exist such t. We have a contradiction to our statement that there exist two equal a_i in our subsequence of length p. So it must be that all a_i are used and create one cycle.

□

Problem. If $\alpha = (3\ 7\ 1\ 4)$, $\beta = (1\ 2\ 3)$, and $\gamma = (2\ 4\ 1\ 3\ 5)$ in S_7, express each of the following as a product of disjoint cycles: (a) $\alpha^{-1}\beta$, (b) $\gamma^{-1}\alpha$, (c) $\alpha^2\beta$, (d) $\beta^2\alpha\gamma$, (e) γ^4, (f) $\gamma^3\alpha^{-1}$, (g) $\beta^{-1}\gamma$, (h) $\alpha^{-1}\gamma^2\alpha$.

Solution. Using previous propositions it will be easier to solve these problems.

(a) $\alpha^{-1}\beta = (4\ 1\ 7\ 3)\,(1\ 2\ 3) = (3\ 7)\,(1\ 2\ 4)$.

(b) $\gamma^{-1}\alpha = (5\ 3\ 1\ 4\ 2)\,(3\ 7\ 1\ 4) = (1\ 2\ 5\ 3\ 7\ 4)$.

(c) $\alpha^2\beta = (3\ 1)\,(7\ 4)\,(1\ 2\ 3) = (1\ 2\ 3)\,(7\ 4)$.

(d) $\beta^2\alpha\gamma = (1\ 3\ 2)\,(3\ 7\ 1\ 4)\,(2\ 4\ 1\ 3\ 5) = (1\ 7\ 3\ 5)$.

(e) $\gamma^4 = (\gamma^2)^2 = (1\ 5\ 4\ 3\ 2)^2 = (1\ 4\ 2\ 5\ 3)$.

(f) $\gamma^3\alpha^{-1} = \gamma^2\gamma\alpha^{-1} = (1\ 2\ 3\ 4\ 5)\,(4\ 1\ 7\ 3) = (1\ 7\ 4\ 2\ 3\ 5)$.

(g) $\beta^{-1}\gamma = (3\ 2\ 1)\,(2\ 4\ 1\ 3\ 5) = (1\ 2\ 4\ 3\ 5)$.

(h) $\alpha^{-1}\gamma^2\alpha = (4\ 1\ 7\ 3)\,(1\ 5\ 4\ 3\ 2)\,(3\ 7\ 1\ 4) = (1\ 4\ 2\ 7\ 5)$.

Problem. Compute α^{-1}, α^2, α^3, α^4 and α^5 where: (a) $\alpha = (1\ 2\ 3)$, (b) $\alpha = (1\ 2\ 3\ 4)$, (c) $\alpha = (1\ 2\ 3\ 4\ 5\ 6)$.

Solution. (a) $\alpha^{-1} = (3\ 2\ 1)$, $\alpha^2 = (1\ 3\ 2) = (3\ 2\ 1) = \alpha^{-1}$, $\alpha^3 = \alpha^2\alpha = \alpha^{-1}\alpha = \epsilon$, $\alpha^4 = \alpha^3\alpha = \epsilon\alpha = \alpha$, $\alpha^5 = \alpha^4\alpha = \alpha\alpha = \alpha^2 = \alpha^{-1}$. (b) $\alpha^1 = (4\ 3\ 2\ 1)$, $\alpha^2 = (1\ 3)\,(2\ 4)$, $\alpha^3 = \alpha^2\alpha = (1\ 3)\,(2\ 4)\,(1\ 2\ 3\ 4) = (1\ 4\ 3\ 2) = (4\ 3\ 2\ 1) = \alpha^{-1}$, $\alpha^4 = \alpha^3\alpha = \alpha^{-1}\alpha = \epsilon$, $\alpha^5 = \alpha^4\alpha = \epsilon\alpha = \alpha$. (c) $\alpha^{-1} = (6\ 5\ 4\ 3\ 2\ 1)$, $\alpha^2 = (1\ 3\ 5)\,(2\ 4\ 6)$, $\alpha^3 = (1\ 4)\,(2\ 5)\,(3\ 6)$, $\alpha^4 = \alpha^3\alpha = (1\ 4)\,(2\ 5)\,(3\ 6)\,(1\ 2\ 3\ 4\ 5\ 6) = (1\ 5\ 3)\,(2\ 6\ 4)$, $\alpha^5 = \alpha^4\alpha = (1\ 5\ 3)\,(2\ 6\ 4)\,(1\ 2\ 3\ 4\ 5\ 6) = (1\ 6\ 5\ 4\ 3\ 2\ 1) = \alpha^{-1}$.

Problem. Let α be a cycle of length s, say $\alpha = (a_1 a_2 \ldots a_s)$. Prove each of the following:

1. There are s distinct powers of α.
2. $\alpha^{s-1} = \alpha^{-1}$.
3. α^2 is a cycle if and only if s is odd.
4. $\alpha^{s+1} = \alpha$.
5. If s is odd, α is the square of some cycle of length s.
6. If s is even, say $s = 2t$, then α^2 is the product of two cycles of length t. (Find them.)

Solution.

1. *There are s distinct powers of α.* First we have $\alpha^0 = \epsilon$ then α itself. Taking α^2 will create a cycle that will carry a_1 to a_2 and then to a_3, i.e. we always skip 2 elements. Now, we can do that for all α^i, when $1 < i < s$ and it will be that, for

each i, a_1 goes to a_{1+i} so they will be distinct. We can do that until we reach α^s as α^{s-1} will carry a_1 to a_s. So, α^s will carry a_1 to next one after a_s and that is a_1, i.e. $\alpha^s = \epsilon = \alpha^0$. From there, the process repeats itself. So, counting ϵ, α and all i between 1 and s it will be $(s-1) - 1 + 2 = s$ distinct powers of α.

2. $\alpha^{s-1} = \alpha^{-1}$. We have $\alpha^{s-1} = \alpha^s\alpha^{-1}$. Now, $\alpha^s = \epsilon$, as for each i we have that a_i goes to a_{i+s} and that is again a_i. Therefore, $\alpha^{s-1} = \epsilon\alpha^{-1} = \alpha^{-1}$.

3. α^2 *is a cycle if and only if* s *is odd. Necessity.* Let α^2 be a cycle. We have to prove that the length of α is odd. Suppose the length s was even. By a previous theorem, as then $2|s$ we have that α^2 is a product of two disjoint cycles of length $\frac{s}{2}$. That is a contradiction to our assumption that α^2 is a cycle, so s has to be odd. *Sufficiency.* Let s, i.e. length of α be odd. We have to show that α^2 is a cycle. If we start from a_1 it will carry to a_3 and all the odd-numbered indices (up to a_s). But, then it will skip a_1 and carry to a_2 and then to a_4 until we exhaust all even-numbered indices (up to a_{s-1}). Finally, a_{s-1} will skip a_s and carry to a_1, thus finishing the cycle and using all elements (as we had all odd and all even indices).

4. $\alpha^{s+1} = \alpha$. Follows from the fact that $\alpha^s = \epsilon$. We have $\alpha^{s+1} = \alpha^s\alpha = \epsilon\alpha = \alpha$.

5. *If* s *is odd,* α *is the square of some cycle of length* s. Let s be odd, i.e. length of α is odd. If we take:

$$\beta = \left(a_1 a_{\frac{s+1}{2}} a_2 a_{\frac{s+3}{2}} \dots a_{s-1} a_{\frac{s-3}{2}} a_s a_{\frac{s-1}{2}}\right).$$

If we take β^2 then a_1 goes to a_2 which will go to a_3 and so on up to $\frac{s-1}{2}$. Obviously this sequence will have $\frac{s-1}{2}$ elements. Then, as we have reached the end, we continue to $\frac{s+1}{2}$, then to $\frac{s+3}{2}$ to a_{s-1} to a_s. In this second sequence we have $s - \frac{s+1}{2} + 1 = \frac{2s-s-1+2}{2} = \frac{s+1}{2}$ elements, totaling $\frac{s-1}{2} + \frac{s+1}{2} = \frac{2s}{2} = s$ elements. This can be done only if s is odd as we would not get natural numbers for e.g. $\frac{s+1}{2}$, $\frac{s-1}{2}$, et cetera. It's easy to see that, by this reasoning $\beta^2 = \alpha$.

6. *If* s *is even, say* $s = 2t$*, then* α^2 *is the product of two cycles of length* t*. (Find them.)* As $2|s$, from previous proposition we have that α is a product of two disjoint cycles of length $\frac{s}{2} = t$. It's easy to verify that

$$(a_1 a_3 \dots a_{s-3} a_{s-1})(a_2 a_4 \dots a_{s-2} a_s) = (a_1 a_2 \dots a_{s-1} a_s)^2.$$

Length of first cycle is $\frac{s-1-1}{2} + 1 = \frac{s-2+2}{2} = t$ and of the second one $\frac{s-2}{2} + 1 = \frac{s-2+2}{2} = t$.

Lemma. No matter how ϵ is written as a composition of transpositions, the number of transpositions is always even.

Proof. Suppose that ϵ can be written as a product of m transpositions such that $\epsilon = t_1 t_2 \cdots t_m$. Let x be an element whose last appearence is in k-th transposition, $t_k = (xa)$ where a is some other element. We observe t_{k-1}. Now, t_{k-1} can contain x and a and then it would be $t_{k-1}t_k = (xa)(xa)$ which is identity and can be removed - now we have $m-2$ transpositions. If t_{k-1} contains x but not a, i.e. some element b which differs from x and a then $t_{k-1}t_k = (xb)(xa) = (xa)(ab)$, therefore x appears last in one place further to the left. If t_{k-1} contains a but not x (some b instead) we have $t_{k-1} = (ab)(xa) = (xb)(ab)$ and again x appears last one place further to the left. If t_{k-1} contains neither x nor a, but some b and c different from x and a we have $t_{k-1} = (bc)(xa) = (xa)(bc)$ and here x appears last one place further to the left. Now, either we have always $m-2$ elements or x gets pushed one place to the left. Therefore, if we reach the end we cannot have only $t_1 = (xa)$ as then $\epsilon(x) = a$ which is a contradiction (it must be that $\epsilon(x) = x$). Therefore, m must be even. And for those elements after k, we can fix some other element, see when it appears last and do the same thing again.

□

Theorem. If a permutation can be written in an even number of transpositions then it cannot be written in an odd number of transpositions.

Proof. Let f be a permutation and f^{-1} its inverse. If f can be written in an even and an odd number of transpositions, the same goes for f^{-1}. Also, we have that $ff^{-1} = \epsilon$. From previous lemma we have that ϵ can be written only in an even number of transpositions. Therefore, if f can be written in an even number of transpositions and f^{-1} in odd number of transpositions, then ϵ would have to be odd. Same thing if f is odd and f^{-1} even, ϵ would have to be odd. Therefore, it can only be that f is either even or odd.

□

Problem. Determine which of the following permutations is even, and which is odd: (a) (7 1 8 6 4), (b) (1 2)(7 6)(3 4 5), (c) (1 2 7 6)(3 2 4 1)(7 8 1 2), (d) (1 2 3)(2 3 4 5)(1 3 5 7),

$$\text{(e) } \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 1 & 5 & 6 & 2 & 3 & 9 \end{pmatrix}$$

Solution. (a) (7 1 8 6 4), (b) (1 2)(7 6)(3 4 5), (c) (1 2 7 6)(3 2 4 1)(7 8 1 2), (d) (1 2 3)(2 3 4 5)(1 3 5 7),

$$\text{(e) } \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 1 & 5 & 6 & 2 & 3 & 9 \end{pmatrix}$$

Problem. Prove each of the following:

1. The product of two even permutations is even.
2. The product of two odd permutations is even.
3. The product of an even permutation and an odd permutation is odd.
4. A cycle of length l is even if l is odd.
5. A cycle of length l is odd if l is even.
6. If α and β are cycles of length l and m, respectively, then $\alpha\beta$ is even or odd depending on whether $l + m - 2$ is even or odd.
7. If $\pi = \beta_1 \cdots \beta_r$ where each β_i is a cycle of length l_i, then π is even or odd depending on whether $l_1 + l_2 + \cdots + l_r - r$ is even or odd.

Solution.

1. *The product of two even permutations is even.* Let α and β be even permutations, i.e. α can be written as a product of $2n$ and β as a product of $2m$ transpositions, where $m, n \in \mathbb{N}$. Then $\alpha\beta$ can be written as product of $2n + 2m = 2(n + m)$ transpositions which is an even number again and it is therefore an even permutation.
2. *The product of two odd permutations is even.* Let α and β be odd permutations, that is α can be written as a product of $2n + 1$ and β as a product of $2m + 1$ transpositions, where $m, n \in \mathbb{N}$. Then $\alpha\beta$ can be written as product of $2n + 1 + 2m + 1 = 2(n + m + 1)$ transpositions which is an even number and it is therefore an even permutation.
3. *The product of an even permutation and an odd permutation is odd.* Let α be an even permutation and β an odd permutations. Then α can be written as a product of $2n$ and β as a product of $2m + 1$ transpositions, where $m, n \in \mathbb{N}$. Then $\alpha\beta$ can be written as product of $2n + 2m + 1 = 2(n + m) + 1$ transpositions which is an odd number and it is therefore an odd permutation.
4. *A cycle of length l is even if l is odd.* Let $\alpha = (a_1 a_2 \dots a_l)$ be a cycle of length l. It can be written as a product of transpositions as

$$\alpha = (a_1 a_l)(a_1 a_{l-1}) \cdots (a_1 a_4)(a_1 a_3)(a_1 a_2).$$

Notice that we have a transposition $(a_1 a_i)$ for every $i \in \{2, \ldots, l\}$. That's $l-1$ transpositions which is even if l is odd. Therefore, cycle of length l is even if l is odd.

5. *A cycle of length l is odd if l is even.* Follows from the same point of reasoning as the previous statement. If l is even then $l-1$ is odd, that is α can be written as $l-1$ transpositions, so it is also odd.

6. *If α and β are cycles of length l and m, respectively, then $\alpha\beta$ is even or odd depending on whether $l+m-2$ is even or odd.* If α is a cycle of length l, then it can be written as a product of $l-1$ transpositions. Same thing goes for β as it can be written as a product of $m-1$ transpositions. Then $\alpha\beta$ can be written as a product of $(l-1)+(m-1) = l+m-2$ transpositions. Therefore, whether $\alpha\beta$ is even or odd will depend on $l+m-2$.

7. *If $\pi = \beta_1 \cdots \beta_r$ where each β_i is a cycle of length l_i, then π is even or odd depending on whether $l_1 + l_2 + \cdots + l_r - r$ is even or odd.* Each cycle β_i can be written as a product of $l_i - 1$ transpositions. Therefore, π can be written as a product of $\sum_{i=1}^{r} l_i - 1 = \sum_{i=1}^{r} l_1 - r$ transpositions. Whether π is even or odd will depend on that sum.

Problem. In each of the following, let α and β be disjoint cycles, say $\alpha = (a_1 a_2 \ldots a_s)$ and $\beta = (b_1 b_2 \ldots b_r)$.

1. For every positive integer n, $(\alpha\beta)^n = \alpha^n \beta^n$.

2. If $\alpha\beta = \epsilon$ then $\alpha = \epsilon$ and $\beta = \epsilon$.

3. If $(\alpha\beta)^t = \epsilon$, then $\alpha^t = \epsilon$ and $\beta^t = \epsilon$.

4. Find a transposition γ such that $\alpha\beta\gamma$ is a cycle.

5. Let γ be the same transposition as in the preceding exercise. Show that $\alpha\gamma\beta$ and $\gamma\alpha\beta$ are cycles.

6. Let α and β be cycles of odd length (not disjoint). Prove that if $\alpha^2 = \beta^2$, then $\alpha = \beta$.

Solution.

1. *For every positive integer n, $(\alpha\beta)^n = \alpha^n \beta^n$.* Disjoint cycles commute (and are associative), as proven previously, so we have $(\alpha\beta)^n = \alpha^n \beta^n$.

2. *If $\alpha\beta = \epsilon$ then $\alpha = \epsilon$ and $\beta = \epsilon$.* We have $(a_1a_2 \dots a_s)(b_1b_2 \dots b_r) = \epsilon$, but α does not influence nor modify β (and reverse) in any way. Therefore, it must be that both α and β are identity.

3. *If $(\alpha\beta)^t = \epsilon$, then $\alpha^t = \epsilon$ and $\beta^t = \epsilon$.* From two previous problems we have that $(\alpha\beta)^t = \alpha^t\beta^t$, so it must be that $\alpha^t = \epsilon$ and $\beta^t = \epsilon$.

4. *Find a transposition γ such that $\alpha\beta\gamma$ is a cycle.* Let $(x_1x_2) = \gamma$. We have $(a_1a_2 \dots a_s)(b_1b_2 \dots b_r)(x_1x_2)$ and we want to find x_1 and x_2 which will "connect" α and β. Say we finish β and want to continue on α. We can take $x_1 = a_s$ and $x_2 = b_r$. Then we have:

$$(a_1a_2 \dots a_s)(b_1b_2 \dots b_r)(a_sb_r) = (a_sb_1b_2 \dots b_ra_1a_2 \dots a_{s-1}) = (b_1b_2 \dots b_ra_1a_2 \dots a_s).$$

5. *Let γ be the same transposition as in the preceding exercise. Show that $\alpha\gamma\beta$ and $\gamma\alpha\beta$ are cycles.* We have $\gamma = (a_sb_r)$. First we shall consider:

$$(a_1a_2 \dots a_s)(a_sb_r)(b_1b_2 \dots b_{r-1}b_r) = (b_1b_2 \dots b_{r-1}a_1a_2 \dots a_sb_r).$$

   We also have:

$$(a_sb_r)(a_1a_2 \dots a_s)(b_1b_2 \dots b_{r-1}b_r) = (b_1b_2 \dots b_{r-1}a_sa_1a_2 \dots a_{s-1}b_r).$$

6. *Let α and β be cycles of odd length (not disjoint). Prove that if $\alpha^2 = \beta^2$, then $\alpha = \beta$.* As α^2 and β^2 are equal cycles (due to length of α and β being odd), they are of the same length n (which is odd) and it must be that $\alpha^2(x_i) = x_{i+2} = \beta^2(x_i)$ for all $i \in \{1, \dots, n-2\}$. Also $\alpha^2(x_{n-1}) = x_2 = \beta^2(x_{n-1})$ and $\alpha^2(x_n) = x_1 = \beta^2(x_n)$. Then, $\alpha x_i = x_{i+1}$, but also $\beta x_i = x_{i+1}$. So, $\alpha x_i = \beta x_i$ for all $i \in \{1, \dots, n-1\}$ and $\alpha x_n = x_1 = \beta x_n$.

Problem. If α is any cycle and π any permutation, $\pi\alpha\pi^{-1}$ is called a *conjugate* of α. In the following parts, let π denote any permutation in S_n. Prove each of the following in S_n:

1. Let $\alpha = (a_1a_2 \dots a_s)$ be a cycle. Then $\pi\alpha\pi^{-1}$ is the cycle $(\pi(a_1), \dots, \pi(a_s))$.

2. Any two cycles of the same length are conjugates of each other.

3. If α and β are disjoint cycles, then $\pi\alpha\pi^{-1}$ and $\pi\beta\pi^{-1}$ are disjoint cycles.

4. Let σ be a product $\alpha_1 \cdots \alpha_t$ of t disjoint cycles of lengths $l_1, \dots, l_t$, respectively. Then $\pi\sigma\pi^{-1}$ is also a product of t disjoint cycles of lengths $l_1, \dots, l_t$.

5. Let α_1 and α_2 be cycles of the same length. Let β_1 and β_2 be cycles of the same length. Let α_1 and β_1 be disjoint, and let α_2 and β_2 be disjoint. There is a permutation $\pi \in S_n$ such that $\alpha_1\beta_1 = \pi\alpha_2\beta_2\pi^{-1}$.

Solution.

1. *Let $\alpha = (a_1a_2 \dots a_s)$ be a cycle. Then $\pi\alpha\pi^{-1}$ is the cycle $(\pi(a_1), \dots, \pi(a_s))$.* Let us denote $\pi' = (\pi(a_1), \dots, \pi(a_s))$. If we take $\pi'(\pi(a_i))$ it has to go to $\pi'(\pi(a_{i+1}))$ by definition of π'. Also, note that $\alpha(a_i) = a_{i+1}$ (except for $\alpha(a_n) = a_1$, which won't influence our examinations for now). Now we have $\pi'(\pi(a_i)) = \pi(\alpha(\pi^{-1}(\pi(a_i)))) = \pi(\alpha(a_i)) = \pi(a_{i+1})$.

2. *Any two cycles of the same length are conjugates of each other.* Let $N = \{1, 2, \dots, n\}$. If β is conjugate of α, then β can be written as $\pi\beta\pi^{-1}$, where $\pi \in S_n$ is some permutation. Conversely, if α is conjugate od β, then α can be written as $\rho\beta\rho^{-1}$, where $\rho \in S_n$ is some other permutation. If $\alpha = (a_1a_2 \dots a_s)$, i.e. $\alpha(a_i) = a_{i+1}$ (with $\alpha(a_s) = a_1$) and $\beta = (b_1b_2 \dots b_s)$, id est $\beta(b_i) = b_{i+1}$ (with $\beta(b_s) = b_1$), then we can take such π that $\pi(b_i) = a_i$, for all $i \in \{1, \dots, s\}$. Obviously, $\pi : N \to N$ is bijection (and a permutation in S_n). Note that $\pi^1(a_i) = b_i$. Then we define:

$$\pi'(a_i) = \pi(\beta(\pi^{-1}(a_i))) = \pi(\beta(b_i)) = \pi(b_{i+1}) = a_{i+1}.$$

Same thing goes for a_s (it goes to a_1; the reader can check for himself). Obviously $\pi' : N \to N$ (as π, π^{-1} and α all stay on N) and $\alpha : N \to N$. Furthermore $\pi'(a_i) = a_{i+1} = \alpha(a_i)$, therefore $\pi' = \alpha$. In conclusion, α is conjugate of β. Same thing goes to prove the other side; we take $\rho(a_i) = b_i$, for all $i \in \{1, \dots, s\}$. Then:

$$\rho'(b_i) = \rho(\alpha(\rho^{-1}(b_i))) = \rho(\alpha(a_i)) = \rho(a_{i+1}) = b_{i+1}.$$

So, by the same reasoning $\rho' = \beta$ and β is conjugate of α. To make a further point we could have taken $\rho = \pi^{-1}$.

3. *If α and β are disjoint cycles, then $\pi\alpha\pi^{-1}$ and $\pi\beta\pi^{-1}$ are disjoint cycles.* If α and β are disjoint, it means that $\alpha(x) \neq \beta(x)$, for all $x \in \mathbb{N}$. Now we have $\pi\alpha\pi^{-1} = (\pi(a_1)\pi(a_2) \dots \pi(a_s))$ and $\pi\beta\pi^{-1} = (\pi(b_1)\pi(b_2) \dots \pi(b_r))$. Suppose for some i it's true that $\pi(a_i) = \pi(b_i)$. But, as π is a permutation and by that a bijection and also an injection, from $\pi(a_i) = \pi(b_i)$ follows that $a_i = b_i$, which is a contradiction to our assumption that α and β are disjoint. Therefore, their conjugates (using the same permutation) must be disjoint also.

4. *Let σ be a product $\alpha_1 \cdots \alpha_t$ of t disjoint cycles of lengths $l_1, \ldots, l_t$, respectively. Then $\pi\sigma\pi^{-1}$ is also a product of t disjoint cycles of lengths $l_1, \ldots, l_t$.* From previous problem we have that all $\pi\alpha_i\pi$ are disjoint cycles, and their lengths are, from the first problem, l_i. If we take the product of all conjugates of α_i we have:

$$\pi\alpha_1\pi^{-1}\pi\alpha_2\pi^{-1}\cdots\pi\alpha_{t-1}\pi^{-1}\pi\alpha_t\pi^{-1}.$$

It's easy to see that all $\pi^{-1}\pi$ cancel each other out and all that remains is:

$$\pi\alpha_1\alpha_2\cdots\alpha_{t-1}\alpha_t\pi^{-1} = \pi\sigma\pi^{-1}.$$

Therefore, $\pi\sigma\pi^{-1}$ was obtained as product of all $\pi\alpha_i\pi^{-1}$, which are disjoint and of the same lengths as α_i. This proves our hypothesis.

5. *Let α_1 and α_2 be cycles of the same length. Let β_1 and β_2 be cycles of the same length. Let α_1 and β_1 be disjoint, and let α_2 and β_2 be disjoint. There is a permutation $\pi \in S_n$ such that $\alpha_1\beta_1 = \pi\alpha_2\beta_2\pi^{-1}$.* If we take some $\pi \in S_n$ (e.g. such that $\pi(a_i') = a_i$ and $\pi(b_i') = b_i$, where a_i is from α_1 and a_i' is from α_2; same thing for β_1 and β_2) it's true that, because they are cycles of the same length, α_1 and α_2 will be conjugates of each other, i.e. $\alpha_1 = \pi\alpha_2\pi^{-1}$ (follows from the second problem). Same thing goes for $\beta_1 = \pi\beta_2\pi^{-1}$. Such permutation will work as a_i and b_i won't mix. We take the product $\alpha_1\beta_1 = \pi\alpha_2\pi^{-1}\pi\beta_2\pi^{-1} = \pi\alpha_2\beta_2\pi^{-1}$ and that concludes this problem.

Problem. If α is any permutation, the least positive integer n such that $\alpha^n = \epsilon$ is called the *order* of α. Prove in S_n:

1. If $\alpha = (a_1 \ldots a_s)$ is a cycle of length s, then $\alpha^s = \epsilon$, $\alpha^{2s} = \epsilon$, and $\alpha^{3s} = \epsilon$. Is $\alpha^k = \epsilon$ for any positive integer $k < s$?

2. If $\alpha = (a_1 \ldots a_s)$ is a cycle of length s, the order of α is s.

Solution.

1. *If $\alpha = (a_1 \ldots a_s)$ is a cycle of length s, then $\alpha^s = \epsilon$, $\alpha^{2s} = \epsilon$, and $\alpha^{3s} = \epsilon$. Is $\alpha^k = \epsilon$ for any positive integer $k < s$?* Each time we raise α to the power of k, we get a_{i+k} from a_i. Therefore, if we take a_1 and take α to the power of s, we will have a_{1+s} which will go to a_1 (as a_s is the last in the cycle and the next is a_1 again). This will, of course work for all powers of the form ks, as we will have a_{1+ks} from a_1. Better said, suppose that it's true, and we will show that $a_{1+(k+1)s}$

will take us to a_1. We have $a_{(1+ks)+s}$. By assumption a_{1+ks} will take us to a_1 and adding s will, by something we have also shown take us to a_1. Thus, by reasoning through mathematical induction, the assumption is valid. Also, suppose $k < s$ and $\alpha^k = \epsilon$. That would mean that a_1 goes to a_{1+k} and that a_1 comes after a_k, but that is contradiction to the fact that a_{k+1} goes after a_k (when $k < s$, of course) and that the cycle is of length k and not s. Therefore, there cannot be any positive integer $k < s$ such that $\alpha^k = \epsilon$.

2. *If $\alpha = (a_1 \dots a_s)$ is a cycle of length s, the order of α is s.* Follows from the reasoning in previous problem. The least number that will take us from a_1 to a_{1+s} is of course s.

Problem. Find the order of each of the following permutations: (a) (1 2)(3 4 5), (b) (1 2)(3 4 5 6), (c) (1 2 3 4)(5 6 7 8 9).

Solution. (a) The permutations is composed of two disjoint cycles of lengths 2 and 3. The cycle of length 2 will be identity for all even powers, and the cycle of length 3 will be identity for 3, 6, etc. If we take the least common multiple of 2 and 3 it's going to be 6. And indeed, when we reach 6 we will have an even permutation, thus putting first cycle to identity. We will also have 6 which will put second cycle to identity. (b) Following the similar reasoning as in previous problem, the cycles will both be identity when taken to the power of 4. (c) As lengths of cycles are 4 and 5, the first time they meet and form identity is at power of 20.

Problem. What is the order of $\alpha\beta$, if α and β are disjoint cycles of lengths 4 and 6, respectively? Explain, what is the order of $\alpha\beta$, if α and β are disjoint cycles of lengths r and s?

Solution. As disjoint cycles commute, we have that $(\alpha\beta)^n = \alpha^n\beta^n$. Thus, we seek k_1 and k_2 such that $\alpha^{4k_1}\beta^{6k_2} = \epsilon$ and that $4k_1 = 6k_2$. The least such (positive natural) numbers will be $k_1 = 3$ and $k_2 = 2$. So:

$$(\alpha\beta)^1 2 = \alpha^1 2 \beta^1 2 = \alpha^{4\cdot 3}\beta^{6\cdot 2} = \epsilon\epsilon = \epsilon.$$

We can assume form this reasoning that for two disjoint cycles of lengths r and s, order of their product will be least common multiple of r and s.

Definition. The set of all the even permutations in S_n is denoted by A_n and is called the **alternating group**[26] on n symbols.

[26] For now in the mention-sense.

Problem. Prove each of the following in S_n:

1. Let $\alpha_1, \ldots, \alpha_r$ be distinct even permutations, and β an odd permutation. Then $\alpha_1\beta, \ldots, \alpha_r\beta$ are r *distinct* odd permutations.

2. If $\beta_1, \ldots, \beta_r$ are distinct odd permutations, then $\beta_1\beta_1, \beta_1\beta_2, \ldots, \beta_1\beta_r$ are r *distinct* even permutations.

3. In S_n, there are the same number of odd permutations as even permutations.

4. The set of all the even permutations (alternating group) is a subgroup of S_n.

5. Let H be any subgroup of S_n. H either contains only even permutations, or H contains the same number of odd as even permutations.

Solution.

1. *Let $\alpha_1, \ldots, \alpha_r$ be distinct even permutations, and β an odd permutation. Then $\alpha_1\beta, \ldots, \alpha_r\beta$ are r distinct odd permutations.* Suppose $\alpha_i\beta = \alpha_j\beta$ for some $i \neq j$ and $i, j \in \{1, \ldots, r\}$. That would mean that, after multiplying with β^{-1} on the right. Then we would have that $\alpha_i = \alpha_j$ which is a contradiction to assumption that all α_i are distinct permutations. Furthermore, as α_i are even and β odd, then by previous problem, $\alpha_i\beta$ are odd.

2. *If $\beta_1, \ldots, \beta_r$ are distinct odd permutations, then $\beta_1\beta_1, \beta_1\beta_2, \ldots, \beta_1\beta_r$ are r distinct even permutations.* Suppose $\beta_1\beta_i = \beta_1\beta_j$ for some $i \neq j$ where $i, j \in \{1, \ldots, r\}$. Then, taking left inverse, β_1^{-1} and multiplying equality on the left yields $\beta_i = \beta_j$, which is contradiction to assumption that all β_i are distinct. Furthermore, as β_1 is odd and β_i are odd then $\beta_1\beta_i$ are even permutations.

3. *In S_n, there are the same number of odd permutations as even permutations.* Suppose there are d (distinct) odd permutations and v (distinct) even permutations. First we will show that there are more odd permutations then even permutations. We have that for all even permutations $\alpha_1, \ldots, \alpha_v$ there are v distinct odd permutations $\alpha_i\beta$ for one odd permutation β. Now, as there are d odd permutations we have $\alpha_i\beta_j$, where $i \in \{1, \ldots, v\}$ and $j \in \{1, \ldots, d\}$, distinct odd permutations. That is dv distinct odd permutations. Obviously $dv \geq v$, so there are more odd permutations than even permutations. Furthermore, as we have d distinct odd permutations, we have distinct even permutations $\alpha_1\alpha_i$ (for $i \in \{1, \ldots, d\}$) and there are d of them. But we can do that not only for α_1, but for all α_j, that is $\alpha_i\alpha_j$ (for $i, j \in \{1, \ldots, d\}$). So there are d^2 even permutations. And, as $d^2 \geq d$ we have more even permutations than odd permutations. If we have both more (or equal) number of odd permutations than even permutations

and, conversely, more (or equal) number of even permutations than odd permutations, our conclusion is that there is the same number of odd permutations as even permutation.

4. *The set of all the even permutations (alternating group) is a subgroup of S_n.* Let us denote A_n as alternating group on n symbols. Any even permutation is a permutation and it belongs in S_n, therefore, obviously, $A_n \subset S_n$ (we can use a stronger statement as we have proved that there is the same number of odd as even permutations, so there must be some other elements in S_n that are not in A_n). If we take two even permutations $f, g \in A_n$, their product is an even permutation again and $fg, gf \in A_n$. Also, if $f \in A_n$ is an even permutation, it's inverse is an even permutation and $f^{-1} \in A_n$ (follows from $ff^{-1} = \epsilon$ and ϵ is an even permutation). Therefore A_n is subgroup of S_n.

5. *Let H be any subgroup of S_n. H either contains only even permutations, or H contains the same number of odd as even permutations.* If H is subgroup of S_n, then it's true that $H \subseteq S_n$, it's closed under composition and with respect to inverses. For one thing, H must contain ϵ or else it could not be closed under multiplication and with respect to inverses (as $ff^{-1} = \epsilon$). But, ϵ is an even permutation. Therefore H cannot contain only odd permutations. As $\{\epsilon\}$ is a trivial group (with respect to composition, of course) then it is possible that H contains only even permutations (even if that is only one). But, if we add one even permutation, it's inverse would be even and composition with other even permutations would be even. Now, suppose we had more odd than even permutations. That is an impossibility as for each two odd permutations their product is an even permutation, i.e. if there are d (distinct) odd then, there must be d^2 (distinct) even permutations. Suppose there are more even than odd permutations. For one odd permutation and all even permutation their products are all odd, therefore, for each odd permutation there are as many odd as there are even permutations so that is an imposibility. Therefore their numbers must equal.

Problem. Remember that in any group G, a set S of elements of G is said to *generate* G if every element of G can be expressed as a product of elements in S and inverses of elements in S. Prove:

1. The set T of all the transpositions in S_n generates S_n.

2. The set $T_1 = \{(1\ 2), (1\ 3), \ldots, (1\ n)\}$ generates S_n.

3. Every even permutation is a product of one or more cycles of length 3. Conclude that the set U of all cycles of length 3 generates A_n.

4. The set $U_1 = \{(1\ 2\ 3), (1\ 2\ 4), \ldots, (1\ 2\ n)\}$ generates A_n.

5. The pair of cycles $(1\ 2)$ and $(1\ 2\ \cdots\ n)$ generates S_n.

Solution.

1. *The set T of all the transpositions in S_n generates S_n.* Set T contains all transpositions, i.e. all cycles of the form $(i\ j)$ where $i, j\{1, \ldots, n\}$ and $i \neq j$. Every permutation can be written down as a product of disjoint cycles. Suppose we had $\pi \in S_n$ such that:

$$\pi = \left(x_1^{(1)} x_2^{(1)} \ldots x_{p_1}^{(1)}\right) \left(x_1^{(2)} x_2^{(2)} \ldots x_{p_2}^{(2)}\right) \cdots \left(x_1^{(m)} x_2^{(m)} \ldots x_{p_m}^{(m)}\right).$$

   It can be shown as a product of transpositions so that:

$$\pi = \left(x_1^{(1)} x_{p_1}^{(1)}\right) \cdots \left(x_1^{(1)} x_3^{(1)}\right) \left(x_1^{(1)} x_2^{(1)}\right) \cdots \left(x_1^{(m)} x_{p_m}^{(m)}\right) \cdots \left(x_1^{(m)} x_2^{(m)}\right).$$

   Also, let us just note that identity can be expressed as $\epsilon = (1\ 2)(2\ 1)$ (and in many other ways). Therefore, as every permutation can be written as a product of transpositions, set T generates S_n.

2. *The set $T_1 = \{(1\ 2), (1\ 3), \ldots, (1\ n)\}$ generates S_n.* In previous problem we have shown *how* a permutation can be written as a product of transpositions. Now, any transposition of the form $(i\ j)$ where $i, j \in \{1, \ldots, n\}$ and $i \neq j$ can be written as $(i\ j) = (j\ 1)(1\ i)(1\ j)$. Therefore, T_1 generates S_n.

3. *Every even permutation is a product of one or more cycles of length 3. Conclude that the set U of all cycles of length 3 generates A_n.* Let $(i\ j)$ and $(k\ l)$ (where $i, j, k, l \in \{1, \ldots, n\}$ and $i \neq j$ and $k \neq l$) be two transpositions. Their product can be written as $(i\ j)(k\ l) = (l\ k\ j)(i\ k\ j)$. If we have $(i\ j)(i\ k) = (i\ k\ j)$ (additional condition that $i \neq k$). Therefore, every even permutation is a product of one or more cycles of length 3. The product of even permutations is even, therefore the set U generates A_n (as every even permutation can be written as a product of elements in U).

4. *The set $U_1 = \{(1\ 2\ 3), (1\ 2\ 4), \ldots, (1\ 2\ n)\}$ generates A_n.* Every cycle of length 3 can be written as:

$$(i\ j)(k\ l) = (1\ 2\ k)(1\ 2\ i)(1\ 2\ l)(1\ 2\ j)(1\ 2\ k)(1\ 2\ i).$$

Also, we have:

$$(i\ j)(i\ k) = (i\ k\ j) = (1\ 2\ j)(1\ 2\ i)(1\ 2\ k)(1\ 2\ j)(1\ 2\ i).$$

The last condition is sufficient, and therefore, every even permutation can be written as product of elements in U_1; in other words, U_1 generates A_n.

5. *The pair of cycles* $(1\ 2)$ *and* $(1\ 2\ \cdots\ n)$ *generates* S_n. Every transposition of the form $(1\ i)$ (where $i \in \{2, \ldots, n\}$) can be written as:

$$(n-(i-2)\ n-(i-1)) = (1\ 2\ \cdots\ n)^{-i}(1\ 2)(1\ 2\ \cdots\ n)^{i}.$$

This way we can obtain all $(k\ k+1)$, where $k \in \{1, \ldots, n-1\}$, by taking $i = n-k+2$. We can see that the only elements not left to identity will be the ones leading to 2 and 1. And which ones will lead to 1 and 2? Well, as $n \to 1$ for $i = 1$ we have $n-1 \to 1$ for $i = 2$ and (following the same reasoning) we have $n-(i-1) \to 1$. Also, $n \to 2$ for $i = 2$, $n-1 \to 2$ for $i = 3$ and we may conclude that $n-(i-2) \to 2$ in general. Now, what happens in the second cycle is that $1 \to 2$ and $2 \to 1$. Finally, when taking inverse, we are asking ourselves, where will 1 and 2 go? Obviously, $1 \to n$ for $i = -1$, $1 \to n-1$ for $i = -2$ and generally $1 \to n-(i-1)$. Similarly, $2 \to n$ for $i = -2$, $2 \to n-1$ for $i = -3$ and generally $2 \to n-(i-2)$. Therefore we have that $n-(i-1) \to n-(i-2)$ and $n-(i-2) \to n-(i-1)$. We also have that:

$$(1\ i) = (1\ 2)(2\ 3)\cdots(i-1\ i-2)(i-1\ i)(i-1\ i-2)\cdots(3\ 2)(2\ 1).$$

It is obvious that all elements $1 < k < i$ will go to $k+1$ and then to k again. But, 1 will go to 2, then to 3, all up to i and then stop (as there is no more i on the left). Same thing for i, as it will go to $i-1$ then to $i-2$ all up to 1. And, all such transpositions are those containted in T_1 and T_1 generates S_n, then the pair of cycles $(1\ 2)$ and $(1\ 2\ \cdots\ n)$ also generates S_n.

Isomorphism

Definition. Let G_1 and G_2 be groups. A bijective function $f : G_1 \to G_2$ with the property that for any two elements a and b in G_1

$$f(ab) = f(a)f(b)$$

is called an **isomorphism** from G_1 to G_2. If there exists an isomorphism from G_1 to G_2, we say that G_1 is **isomorphic** to G_2 and symbolize this fact by writing:

$$G_1 \cong G_2.$$

Proposition. Isomorphism is an equivalence relation.

Proof. (a) *Reflexivity.* Every group is isomorphic to itself as we can take $\epsilon : G \to G$ such that $\epsilon(x) = x$, for all $x \in G$. It's obviously a bijection and $\epsilon(ab) = ab = \epsilon(a)\epsilon(b)$, for all $a, b \in G$. Therefore, $G \cong G$. (b) *Symmetry.* If we have $G_1 \cong G_2$ then there exists isomorphism $f : G_1 \to G_2$. As isomorphism is a bijection it's inverse $f^{-1} : G_2 \to G_1$ is also a bijection. Furthermore, as we have $f(ab) = f(a)f(b)$ for $a, b \in G_1$, then $f^{-1}(f(ab)) = f^{-1}(f(a)f(b))$. That is, $f^{-1}(f(a)f(b)) = ab$, for $f(a), f(b) \in G_2$. But, as $f^{-1}(f(a)) = a$ and $f^{-1}(f(b)) = b$, we have $f^{-1}(f(a)f(b)) = f^{-1}(f(a))f^{-1}(f(b))$, where $f(a), f(b) \in G_2$. We could rename $a' := f(a)$ and $b' := f(b)$ so that we have $f^{-1}(a'b') = f^{-1}(a')f^{-1}(b')$ for all $a', b' \in G_2$. Therefore f^{-1} is also an isomoprhism and we have that $G_1 \cong G_2$ implies $G_2 \cong G_1$. (c) *Transitivity.* Suppose we have $G_1 \cong G_2$ and $G_2 \cong G_3$. We have to show that $G_1 \cong G_3$. As $G_1 \cong G_2$, there exists isomorphism $f : G_1 \to G_2$ such that $f(ab) = f(a)f(b)$, for all $a, b \in G_1$. Also, as $G_2 \cong G_3$, there exists an isomorphism $g : G_2 \to G_3$ such that $g(ab) = g(a)g(b)$, for all $a, b \in G_2$. As isomorphism is bijection by definition then composition $g \circ f : G_1 \to G_3$ is also a bijection. Furthermore we have that $g(f(ab)) = g(f(a)f(b))$, for all $a, b \in G_1$. As $f(ab) \in G_2$ and $f(a), f(b) \in G_2$, then $g(f(a)f(b)) = g(f(a))g(f(b))$. So we have $[g \circ f](ab) = [g \circ f](a)[g \circ f](b)$, for all $a, b \in G_1$. Therefore, $g \circ f$ is an isomorphism from G_1 to G_3, so $G_1 \cong G_2$ and $G_2 \cong G_3$ implies $G_1 \cong G_3$.

□

We will first exemplify our motivation for the following theorem. Indeed, proof of a theorem by itself is worth nothing, if it does not shed more light on the theorem itself. It has not only to reveal something extraordinary, but it has to show why the theorem works and will always work. Proving it in a simple way is by no means an advantage. Proving it in a way that will reveal (or at least allow us a glimpse at) all the machinery

behind it. Let us first define group $V := (V, \cdot)$ where $V = \{1, i, -1, -i\}$. When we're dealing with "small" finite groups, showing isomorphism between them will be just a matter of table-checking. Now, let us take another group $\mathbb{Z}_4 := (\mathbb{Z}_4, +_4)$. We will show that $V \cong \mathbb{Z}_4$. If we construct tables for V and $\mathbb{Z}_4$, respectively, we will have:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	$\mathbf{-1}$	$\mathbf{1}$
$-i$	$-i$	i	$\mathbf{1}$	$\mathbf{-1}$

$+_4$	0	1	2	3
0	0	1	2	3
1	$\mathit{1}$	$\mathbf{2}$	$\mathit{3}$	$\mathbf{0}$
2	2	3	0	1
3	$\mathit{3}$	$\mathbf{0}$	$\mathit{1}$	$\mathbf{2}$

Now, an obvious thing is to look for the identity and then seek out patterns. Obviously, identity for V is 1 (as we're dealing with multiplication of complex numbers; actually $(V, \cdot)$ is a subgroup of $(\mathbb{C}\backslash\{0\}, \cdot)$). Identity in $\mathbb{Z}_4$ is 0 (we're dealing with addition). We will start constructing isomorphism $f : V \to \mathbb{Z}_4$. We have $f(1) = 0$. Good thing is to start looking for blocks of subtables (such as one marked in bold) with few tips: rows have to match, i.e. we cannot have a subtable containing elements that don't correspond to ones that define rows in one, and in other have such elements appear in the subtable. Such is the logical choice for the subtable in $\mathbb{Z}_4$ that corresponds to the subtable in V. They both contain neutral elements on the diagonal and they both have other element that is different from the ones defining rows (i.e. in V we have -1 appearing in i and $-i$ rows and in $\mathbb{Z}_4$ we have 2 appearing in 1 and 3 rows). So, we may assume that $f(-1) = 2$. Also, $2 +_4 2 = 0$ and $-1 \cdot -1 = 1$ (they are inverses of themselves which is by itself a good guiding point). We may further guess that $f(i) = 1$ (as actually i means "rotate by π and logical order is $1, i, -1, -i$, therefore i acts as an increment, as does 1 in $\mathbb{Z}_4$). Then, $f(-i) = 3$ as $-i \cdot i = 1$. So it leaves us with:

$$f = \begin{pmatrix} 1 & i & -1 & -i \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

We have to check if $f(ab) = f(a)f(b)$ for all $a, b \in V$. E.g. we have $f(i \cdot -1) = f(-i) = 3 = 1 +_4 2$. Both groups are commutative so we need not check all possibilities. By pure reason we shall assume that this is indeed correct (and the reader can check himself by going through the table one more time). But, now, we want to define functions $\pi_a : V \to V$ of the type $\pi_a(x) = ax$, for all $a \in V$. Permutation π_1 is identity as $\pi_1(x) = 1 \cdot x = x$. Therefore $\pi_1 = \epsilon$. To go further, we have $\pi_i(x) = ix$ which will have the following table:

$$\pi_i = \begin{pmatrix} 1 & i & -1 & -i \\ i & -1 & -i & 1 \end{pmatrix}.$$

In the same fashion we construct $\pi_{-1} = -x$ and $\pi_{-i} = -ix$:

$$\pi_{-1} = \begin{pmatrix} 1 & i & -1 & -i \\ -1 & -i & 1 & i \end{pmatrix}, \quad \pi_{-i} = \begin{pmatrix} 1 & i & -1 & -i \\ -i & 1 & i & -1 \end{pmatrix}.$$

We can see that we have here the following table of multiplication for these permutations (a helpful fact is that $\pi_i = (1\ i\ -1\ -i)$, $\pi_{-1} = (-1\ 1)\,(-i\ i)$ and $\pi_{-i} = (-i\ -1\ i\ 1)$):

$\circ$	π_1	π_i	π_{-1}	π_{-i}
π_1	π_1	π_i	π_{-1}	π_{-i}
π_i	π_i	π_{-1}	π_{-i}	π_1
π_{-1}	π_{-1}	π_{-i}	π_1	π_i
π_{-i}	π_{-i}	π_1	π_i	π_{-1}

Set of permutations $\{\pi_1, \pi_i, \pi_{-1}, \pi_{-i}\}$ (with composition) is obviously isomorphic to group V. The following theorem will be proved generaly, by constructing such permutations over some group and proving the existence of isomorphism. Yet, we have forgotten something that was implicitly understood here: we had to prove that $\pi_a : V \to V$ is actually a permutation, for all $a \in V$. As forementioned, here the case was trivial, but when we're dealing with something larger and unknown we have to go step by step and prove that π_a is a function and such function for which $\mathrm{dom}(f) = \mathrm{cod}(f)$ and such function that is bijective. Also, we have to prove that the set of such permutations is also a group (and that will be done easier by proving it to be a subgroup of S_n).

Theorem (Cayley). Every group is isomorphic to a group of permutations.

Proof. Let G be a group. We define a function $\pi_a : G \to G$, as in previous (motivational) example, such that $\pi_a(x) = ax$, where $a \in G$. First we will show that this is indeed a permutation. A function it surely is, taking ax, where $a, x \in G$ will, due to group G being closed with respect to multiplication, yield $ax \in G$. Such ax will also be unique as group G satisfies axioms of totality. As its domain and codomain are the same, it is a permutation (providing we prove it's also bijective).

Furthermore we have to prove that it is injective and surjective. If we take $\pi_a(x) = \pi_b(y)$ we have $ax = ay$. As $a \in G$ and G is group, i.e. closed with respect to inverses among other things, we also have $a^{-1} \in G$ such that $a^{-1}a = e$, where $e \in G$ is identity (neutral element). Therefore, multiplying $ax = ay$ on the left with a^{-1} gives us $a^{-1}ax = a^{-1}ay$ which actually implies that $ex = ey$, and by that $x = y$. Thus, π_a is injective for all $a \in G$. Now, for surjectivity, we take some $y \in G$. There has to exist original $x \in G$ such that $y = \pi_a(x)$ and that is $y = ax$. Taking the inverse and multiplying on the left gives us $a^{-1}y = x$. As inverse exists, there exists such $x \in G$. Thus, π_a is a bijection and, taking former conditions into consideration, a permutation.

We now take the set $G^* = \{\pi_a : \ a \in G\}$, which will contain one such permutation for each $a \in G$. Let S_G denote the group[27] of all permutations on G. We will show that G^* is a subgroup of S_G. First, G^* is a subset of S_G, as π_a is a permutation and contained in S_G (which contains all permutations on G). If we take $\pi_a, \pi_b \in G^*$, then $\pi_a(\pi_b(x)) = \pi_a(bx) = a(bx) = (ab)x$. As $ab \in G$ (G is closed under multiplication), then $\pi_{ab} = (ab)x$ is in G^* (ab is in G so by definition of G^* permutation π_{ab} is contained in G^*). If we take $\pi_a \in G^*$, then we have to show that $\pi_a^{-1} \in G^*$. We have $\pi_a(x) = ax$ and it's inverse[28] is $\pi_a^{-1}(x) = a^{-1}x$. Group G is closed with respect to inverses so a^{-1} is in G, and by that $\pi_{a^{-1}}$ is in G^*. Therefore, G^* is a subgroup of S_G, and by that, a group by itself.

Now we take function $f : G \to G^*$ such that $f(a) = \pi_a$. Such function is defined for all a, and all π_a are unique for each a. Also, f is injective as $f(a) = f(b)$ implies $\pi_a = \pi_b$. That implies $ax = bx$, so taking the inverse of x (we can do that as $x \in G$ and $x^{-1} \in G$) and multiplying with it the equation on the right gives us $a = b$. Thus, f is injective. If we take $\pi_a \in G^*$ there exists $a \in G$ such that $\pi_a = f(a)$ and f is surjective. By that, it is also bijective. Now, we have to show that $f(ab) = f(a)f(b)$. It's easy to see[29] that $f(ab) = \pi_{ab} = \pi_a\pi_b = f(a)f(b)$. Thus, f is an isomorphism from G to G^* and we have just proved that $G \cong G^*$. In other words, a weaker statement, G is isomorphic to some group of permutations.

□

Definition. Let G be a group and $G^* = \{\pi_a : \ a \in G\}$, where $\pi_a : G \to G$ is a permutation on G. We say that G^* is:

- **left regular representation** of G if $\pi_a(x) = ax$;
- **right regular representation** of G if $\pi_a(x) = xa$;
- **regular representation** of G if G is commutative.

Problem. Find the right and left regular representation of each of the following groups, and compute their tables. (If the group is Abelian, find its regular representation.) (a) $\mathbb{Z}_3$; (b) P_2, the group of subsets of a two-element set; (c) $\mathbb{Z}_4$.

Solution. (a) The multiplication table for $\mathbb{Z}_3$ is as follows:

[27] S_G is the subgroup of the group of all bijections from G to G. If we take two $f, g \in S_G$, then fg is also a bijection from G to G, and if we take inverse f^{-1} of $f \in S_G$ it is also in S_G as inverse of bijection is a bijection and, again, it goes from G to G.

[28] As $\pi_a(\pi_a^{-1}(x)) = a(a^{-1})x = x$ and $\pi_a^{-1}(\pi_a(x)) = a^{-1}(ax) = x$.

[29] Note that $\pi_{ab} = \pi_a\pi_b$ as $\pi_{ab}(x) = (ab)x = a(bx) = \pi_a(\pi_b(x))$.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

The table for $\mathbb{Z}_3$ is symmetric so the group is commutative. It will have a regular representation. We define $G^* = \{\pi_0, \pi_1, \pi_2\}$. Then, taking into consideration that $\pi_0 = \epsilon$, we have:

$$\pi_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \qquad \pi_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}.$$

Note that $\pi_1 = (0\ 1\ 2)$ and $\pi_2 = (0\ 2\ 1)$.

(b) Let $\{a, b\}$ be a two-element set. Then $P_2 = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. The table of P_2 (taking symmetric difference as operation on P_2) is:

Δ	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a, b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\emptyset$	$\{a\}$
$\{a, b\}$	$\{a, b\}$	$\{b\}$	$\{a\}$	$\emptyset$

Again, P_2 is commutative (as set union is commutative) so it has a regular representation. We have $P_2^* = \left\{\pi_\emptyset, \pi_{\{a\}}, \pi_{\{b\}}, \pi_{\{a,b\}}\right\}$, where (taking that $\pi_\emptyset = \epsilon$):

$$\pi_{\{a\}} = \begin{pmatrix} \emptyset & \{a\} & \{b\} & \{a, b\} \\ \{a\} & \emptyset & \{a, b\} & \{b\} \end{pmatrix} = (\emptyset\ \{a\})(\{b\}\ \{a, b\}),$$

$$\pi_{\{b\}} = \begin{pmatrix} \emptyset & \{a\} & \{b\} & \{a, b\} \\ \{b\} & \{a, b\} & \emptyset & \{a\} \end{pmatrix} = (\emptyset\ \{b\})(\{a\}\ \{a, b\}),$$

$$\pi_{\{a,b\}} = \begin{pmatrix} \emptyset & \{a\} & \{b\} & \{a, b\} \\ \{a, b\} & \{b\} & \{a\} & \emptyset \end{pmatrix} = (\emptyset\ \{a, b\})(\{a\}\ \{b\}).$$

(c) We already have multiplication table for $\mathbb{Z}_4$ (look above). The group is also Abelian, therefore it will have a regular representation. We have $G^* = \{\pi_0, \pi_1, \pi_2, \pi_3\}$, where (notice that $\pi_0 = \epsilon$):

$$\pi_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}, \qquad \pi_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix},$$

$$\pi_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}.$$

Notice that $\pi_1 = (0\ 1\ 2\ 3)$, $\pi_2 = (0\ 2)(1\ 3)$ and $\pi_3 = (3\ 2\ 1\ 0)$.

Problem. Let G_1 and G_2 be groups, and let $f : G_1 \to G_2$ be an isomorphism. Prove the following:

1. If e_1 denotes the neutral element of G_1 and e_2 denotes the neutral element of G_2, prove that $f(e_1) = e_2$.
2. Prove that for each element in a in G_1, $f(a^{-1}) = [f(a)]^{-1}$.
3. If G_1 is a cyclic group with generator a, prove that G_2 is also a cyclic group, with generator $f(a)$.

Solution.

1. *If e_1 denotes the neutral element of G_1 and e_2 denotes the neutral element of G_2, prove that $f(e_1) = e_2$.* Let $f(e_1) = e_2'$, where $e_2' \neq e_2$, i.e. we have that $e_2'(e_2')^{-1} = e_2$. We will show that $e_2' = e_2$. If we take $f^{-1}(e_2) = f^{-1}(e_2'(e_2')^{-1})$, as $f^{-1} : G_1 \to G_2$ is also an isomorphism (symmetry), it follows that $f^{-1}(e_2) = f^{-1}(e_2')f^{-1}((e_2')^{-1})$. But, $f(e_1) = e_2'$, so $f^{-1}(f(e_1)) = f^{-1}(e_2')$, i.e. $e_1 = e_2'$. From that we have $f^{-1}(e_2) = e_1 f^{-1}((e_2')^{-1})$. As e_1 is a neutral element in G_1 (and notice that $f^{-1}((e_2')^{-1}) \in G_1$) we have that $f^{-1}(e_2) = f^{-1}(e_2')^{-1}$. As f^{-1} is a bijection, we have that $e_2 = (e_2')^{-1}$. That means that $e_2'e_2 = e_2$ and from that follows $e_2' = e_2$ (as $e_2'e_2 = e_2'$).

2. *Prove that for each element in a in G_1, $f(a^{-1}) = [f(a)]^{-1}$.* As G_1 is a group, there exists $a^{-1} \in G_1$ such that $aa^{-1} = e_1$, where e_1 is a neutral element in G_1. As $f : G_1 \to G_2$ is an isomorphism, we have that $f(e_1) = f(aa^{-1}) = f(a)f(a^{-1})$. By the previous problem $f(e_1) = e_2$, where e_2 is a neutral element in G_2. Therefore, we have $e_2 = f(a)f(a^{-1})$. Notice that $f(a) \in G_2$ and, as G_2 is a group, it has an inverse[30] $[f(a)]^{-1} \in G_2$. By multiplying $e_2 = f(a)f(a^{-1})$ with $[f(a)]^{-1}$ on the left, we have $[f(a)]^{-1}e_2 = [f(a)]^{-1}f(a)f(a^{-1})$, which is $[f(a)]^{-1} = f(a^{-1})$.

3. *If G_1 is a cyclic group with generator a, prove that G_2 is also a cyclic group, with generator $f(a)$.* As G_1 is a cyclic group with generator a then every element in G_1 is of the form a^n, or a^{-n}, where $n \in \mathbb{N}$. Taking $f(a^n) = f(aa^{n-1}) = f(a)f(a^{n-1})$ and continuing the process, we finally get $f(a^n) = \underbrace{f(a)f(a)\cdots f(a)}_{n \text{ times}} = [f(a)]^n$. Same thing goes for $f(a^{-n}) = \underbrace{f(a^{-1})f(a^{-1})\cdots f(a^{-1})}_{n \text{ times}} = [f(a)]^{-n}$. As f is bijective, every element in G_2 will be of this form (or a neutral element). Therefore $f(a)$ generates G_2.

[30] Note that this is not an inverse function, but an inverse element in G_2; in other words $f^{-1}(a) \neq [f(a)]^{-1}$.

Problem. Let E designate the group of all the even integers, with respect to addition. Prove that $\mathbb{Z} \cong E$.

Solution. We can take the function $f : \mathbb{Z} \to E$ such that $f(x) = 2x$. As this is a linear function, it is a bijection and

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y).$$

Therefore, f is an isomorphism from $\mathbb{Z}$ to E and $\mathbb{Z} \cong E$.

Problem. Let G be the group $\{10^n : \ n \in \mathbb{Z}\}$ with respect to multiplication. Prove[31] that $G \cong \mathbb{Z}$.

Solution. Let $f : G \to \mathbb{Z}$ be a function defined with $f(x) = \log x$. Logarithmic function is a bijection (also, notice that $x > 0$ for all $x \in G$). We have:

$$f(xy) = \log xy = \log x + \log y = f(x) + f(y).$$

To conclude, f is an isomorphism from G to $\mathbb{Z}$ and $G \cong \mathbb{Z}$.

Problem. Prove[32] that $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$.

Solution. If we took $f : \mathbb{C} \to \mathbb{R} \times \mathbb{R}$ such that $f(a + bi) = (a, b)$ we would be on our way of proving this isomorphism. We have to prove that this is a bijection. First, injectivity. If $(a, b) = (c, d)$ then $a = c$ and $b = d$ (as two ordered pairs are equal if and only if values at their respective places are the same). Therefore, $a+bi = c+di$ (as two complex numbers are equal if and only if their real and imaginary values are the same). Surjectivity is trivial. If we took $(a, b) \in \mathbb{R} \times \mathbb{R}$, we can always find $(a + bi) \in \mathbb{C}$ such that $f(a + bi) = (a, b)$. In conclusion, f is a bijection. Now (remember the definition of the direct product) we have:

$$\begin{aligned} f((a + bi) + (c + di)) &= f((a + c) + (b + d)i) = (a + c, b + d) \\ &= (a, b) + (c, d) = f(a + bi) + f(c + di). \end{aligned}$$

Thus, f is an isomorphism from $\mathbb{C}$ to $\mathbb{R} \times \mathbb{R}$ and it follows that $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$.

[31] Notice that when we're talking groups, we're always thinking of $\mathbb{Z}$ with addition; if we took multiplication, $(\mathbb{Z}, \cdot)$ would not be a group (monoid at best).

[32] We're also thinking addition here, as multiplication for complex numbers is defined a bit different than that of the direct product of two groups.

Problem. Prove[33] that $\mathbb{R} \cong \mathbb{R}^+$. Prove that $\mathbb{R} \ncong \mathbb{R}^*$ (remember that $\mathbb{R}^*$ is the group with $\mathbb{R}\backslash\{0\}$ under multiplication).

Solution. One of the functions of the form $f : \mathbb{R} \to \mathbb{R}^+$ is $f(x) = e^x$. Exponential function is a bijection. Furthermore,

$$f(x + y) = e^{x+y} = e^x e^y = f(x)f(y).$$

By that, f is an isomorphism from $\mathbb{R}$ to $\mathbb{R}^+$ and $\mathbb{R} \cong \mathbb{R}^+$. Now, we want to show that $\mathbb{R} \ncong \mathbb{R}^*$. We will prove that by demonstrating that certain pairings are impossible. Suppose we have an isomorphism $f : \mathbb{R} \to \mathbb{R}^*$. As neutral elements must correspond, we have that $f(0) = 1$. Also, elements which are their own inverses must correspond, and as $-1 \cdot (-1) = 1$, we have that -1 is its own inverse in $\mathbb{R}^*$. But, if such element were to exist in $\mathbb{R}$, it would have to be $x + x = 0$. But, then it must be that $x = 0$ and that is the only element that is it's own inverse in $\mathbb{R}$. So, we would have that $f(0) = -1$ and would have a contradiction to necessary condition that $f(0) = 1$. So there does not exist an isomorphism f from $\mathbb{R}$ to $\mathbb{R}^*$ (and reverse) and $\mathbb{R} \ncong \mathbb{R}^*$.

Problem. If we know generators and defining equations for two groups, G and G', and if we are able to match the generators of G with those of G' so that the defining equations are the same, we may conclude that $G \cong G'$. Prove that the following pairs of groups G, G' are isomorphic:

1. G is the subgroup of S_4 generated by (2 4) and (1 2 3 4);
   $G' = \{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ where $a^2 = e$, $b^4 = e$ and $ba = ab^3$;
2. $G = S_3$; $G' = \{e, a, b, ab, aba, abab\}$ where $a^2 = e$, $b^2 = e$, and $bab = aba$;
3. $G = D_4$; $G' = \{e, a, b, ab, aba, (ab)^2, ba, bab\}$ where $a^2 = b^2 = e$ and $(ab)^4 = e$;
4. $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; $G' = \{e, a, b, c, ab, ac, bc, abc\}$ where $a^2 = b^2 = c^2 = e$ and $(ab)^2 = (bc)^2 = (ac)^2 = e$.

Solution.

1. *G is the subgroup of S_4 generated by* (2 4) *and* (1 2 3 4)*;*
   $G' = \{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ where $a^2 = e$, $b^4 = e$ and $ba = ab^3$.
   As (2 4)(2 4) $= \epsilon$ and (1 2 3 4)$^4 = \epsilon$ obviously $f((2\ 4)) = a$ and $f((1\ 2\ 3\ 4)) = b$.

[33] $\mathbb{R}$ is a group of real numbers under addition, as multiplication requires excluding the zero. $\mathbb{R}^+$ is a group of real numbers under multiplication, as we don't have negative numbers to fulfill condition of existence of additive inverses; also, zero is excluded.

Now we have to check whether $(1\ 2\ 3\ 4)(2\ 4) = (2\ 4)(1\ 2\ 3\ 4)^3$. On the left-hand side we have $(2\ 1)(3\ 4)$ and on the right-hand side $(2\ 4)(1\ 4\ 3\ 2) = (1\ 2)(3\ 4)$. Therefore, as we were able to match generators and defining equations, we have that $G \cong G'$.

2. $G = S_3$; $G' = \{e, a, b, ab, aba, abab\}$ *where* $a^2 = e$, $b^2 = e$, *and* $bab = aba$. S_3 is generated (as proved above) by $(1\ 2)$ and $(1\ 3)$. Obviously $(1\ 2)^2 = \epsilon$ and $(1\ 3)^2 = \epsilon$. We make a wild guess and take $f((1\ 2)) = a$ and $f((1\ 3)) = b$ (actually makes no difference as the defining equation is symmetrical). So we have $(1\ 3)(1\ 2)(1\ 3) = (3\ 2)$ and $(1\ 2)(1\ 3)(1\ 2) = (2\ 3)$. Obviously $S_3 \cong G'$.

3. $G = D_4$; $G' = \{e, a, b, ab, aba, (ab)^2, ba, bab\}$ *where* $a^2 = b^2 = e$ *and* $(ab)^4 = e$. Remember that generators of D_4 satisfy $c^2 = e'$, $d^4 = e'$ and $dc = cd^3$. In G' we have $(ab)^4 = e$, so we can confirm our suspicions that $f(d) = (ab)$. Also, if we multiply $dc = cd^3$ on the right with dc, we have $(dc)^2 = e$. We can assume that $f(dc) = a$ and $f(c) = b$. And we can see that then $f(c^2) = f(c)f(c) = bb = b^2 = e = f(e')$. Also, $f((dc)^2) = f(dc)f(dc) = aa = a^2 = e = f(e')$ and $f(d^4) = f(d^2)f(d^2) = [f(d)]^4 = (ab)^4 = e = f(e')$. So $D_4 \cong G'$.

4. $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; $G' = \{e, a, b, c, ab, ac, bc, abc\}$ *where* $a^2 = b^2 = c^2 = e$ *and* $(ab)^2 = (bc)^2 = (ac)^2 = e$. In G we have ordered triples. Neutral element is $(0, 0, 0)$. For one thing, we have that $(0, 0, 1) + (0, 0, 1) = (0, 0, 0)$ and we can try $f(a) = (0, 0, 1)$. Similarly, we can take $f(b) = (0, 1, 0)$ and $f(c) = (1, 0, 0)$. Supposing f is an isomorphism we would have $f((ab)^2) = f(ab) + f(ab) = (0, 1, 1) + (0, 1, 1) = (0, 0, 0) = f(e)$. We would also have $f((bc)^2) = (1, 1, 0) + (1, 1, 0) = (0, 0, 0)$ and $f((ac)^2) = (1, 0, 1) + (1, 0, 1) = (0, 0, 0)$. Thus, $G \cong G'$.

Problem. $G = \{x \in \mathbb{R} : \ x \neq -1\}$ with the operation $x * y = x + y + xy$. Show that $f(x) = x - 1$ is an isomorphism from $\mathbb{R}^*$ to G. Thus, $\mathbb{R}^* \cong G$.

Solution. We have that f is a linear function and is therefore an injection. To prove that it is a surjection, we only need to check what happens when $x = 0$ (as it might copy it somewhere in G and we excluded it). Obviously $f(0) = 0 - 1 = -1$ and $-1 \notin G$. All other elements have their originals. Thus, f is a bijection. Next, we have:

$$\begin{aligned} f(x) * f(y) &= (x-1) * (y-1) = x - 1 + y - 1 + (x-1)(y-1) \\ &= x - 1 + y - 1 + xy - x - y + 1 = xy - 1 = f(xy). \end{aligned}$$

From that follows $f(xy) = f(x) * f(y)$ and from that $\mathbb{R}^* \cong G$.

Problem. G is the set of the real numbers with the operation $x * y = x + y + 1$. Find an isomorphism $f : \mathbb{R} \to G$ and show that it is an isomorphism.

Solution. We can try (after some thinking) $f(x) = x + 2$. Then we have $f(x + y) = x + y + 2 = x + 1 + y + 1 = f(x) * f(y)$. Also, f is a linear function from $\mathbb{R}$ to $\mathbb{R}$ (underlying set of G is $\mathbb{R}$) so it is bijective and $\mathbb{R} \cong G$.

Problem. G is the set of the nonzero real numbers with the operation $x * y = \frac{xy}{2}$. Find an isomorphism from $\mathbb{R}^*$ to G.

Solution. Similarly, after some trying out, we get that the best option is $f : \mathbb{R}^* \to G$ with $f(x) = 2x$ (also a linear function and a bijection; the only thing we need to worry is about zero, but $f(0) = 0$ and zero is neither in $\mathbb{R}$ nor in G). We have $f(xy) = 2xy = \frac{(2x)\cdot(2y)}{2} = f(x) * f(y)$. Thus, $\mathbb{R}^* \cong G$.

Problem. Show that $f(x, y) = (-1)^y x$ is an isomorphism from $\mathbb{R}^+ \times \mathbb{Z}_2$ to $\mathbb{R}^*$. Conclude that $\mathbb{R}^* \cong \mathbb{R}^+ \times \mathbb{Z}_2$.

Solution. First we will show that f is an injection. If $f(x, y) = f(z, w)$ then we have $(-1)^y x = (-1)^z w$. Dividing equality by x (we can do that as $x \in \mathbb{R}^+$) and by $(-1)^z$ (obviously $(-1)^z \neq 0$, for all $z \in \mathbb{Z}_2$) we have $\frac{(-1)^y}{(-1)^z} = \frac{w}{x}$. Notice that the left side will always be either 1 or -1. That can be only if $w = x$. But what if it were $y \neq z$, e.g., without loss of generality, $y = 1$ and $z = 0$? Then, from the starting equality, we would have $-x = w$. But, as $x = w$, it would follow that $-x = x$, meaning x can only be zero. That cannot be as $x \in \mathbb{R}^+$. Therefore, it must be that $y = z$. As we deduced from $f(x, y) = f(z, w)$ that $(x, y) = (z, w)$, f is an injection. As for the surjectivity, we take a non zero number of the form $z = (-1)^y x$. If $z < 0$ then $y = 1$ and if $z > 0$ then $y = 0$ (as x is always positive). So it only remains the problem of picking x. For $z > 0$ we have $z = x$ and for $z < 0$ we have $z = -x$, i.e. $x = -z$. To sum it all up, $x = |z|$. Thus for every $z \in \mathbb{R}^*$ there is an ordered pair $(x, y) \in \mathbb{R}^+ \times \mathbb{Z}_2$ such that $z = (-1)^y x$, and because of that, f is a surjection. Now we only check second condition for isomorphism:

$$f((x, y) \cdot (z, w)) = f(xz, yw) = (-1)^{yw} xz = (-1)^y x (-1)^w z = f(x, y) f(z, w).$$

Therefore, f is an isomorphism from $\mathbb{R}^+ \times \mathbb{Z}_2$ to $\mathbb{R}^*$. From that it follows that $\mathbb{R}^+ \times \mathbb{Z}_2 \cong \mathbb{R}^*$, and because isomorphism is an equivalence relation, we have that $\mathbb{R}^* \cong \mathbb{R}^+ \times \mathbb{Z}_2$ (symmetry).

Problem. Let G and H be groups. Prove that $G \times H \cong H \times G$.

Solution. If we take $f : G \times H \to H \times G$ such that $f(x, y) = (y, x)$ it will be a bijection. If $f(x, y) = f(z, w)$ then $(y, x) = (w, z)$ and from that follows $y = w$ and $x = z$ which is the same as $(x, y) = (z, w)$, thus it is an injection. If we take $(y, x) \in H \times G$, then there exists $(z, w) \in G \times H$ such that $f(z, w) = (y, x)$ and that is $(z, w) = (x, y)$. Furthermore, we have $f((x, y)(z, w)) = f(xz, yw) = (yw, xz) = (y, x)(w, z) = f(x, y)f(z, w)$. In conclusion, f is an isomorphism and $G \times H \cong H \times G$.

Problem. Let G be any group. Prove that G is Abelian if and only if the function[34] $f(x) = x^{-1}$ is an isomorphism from G to G.

Solution. *Necessity.* Let G be Abelian, i.e. $xy = yx$ for all $x, y \in G$. We need to prove that $f(x) = x^{-1}$ is an isomorphism from G to G. We have that f is an injection as from $f(x) = f(y)$, i.e. $x^{-1} = y^{-1}$ follows that, after multiplying equality with x on the left and y on the right, we have $xx^{-1}y = xy^{-1}y$ and that is $y = x$. If $y \in G$ then we need to find $x \in G$ such that $f(x) = y$. But, as G is a group, every element has an inverse, so we take $x = y^{-1}$ and have[35] $f(y^{-1}) = (y^{-1})^{-1} = y$. Thus, f is a surjection. Then we have $f(xy) = (xy)^{-1} = y^{-1}x^{-1}$. But, as G is Abelian, we have $y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$. Therefore, f is an isomorphism from G to G. *Sufficiency.* Let f be an isomorphism from G to G. We need to prove that G is Abelian. We have that f is a bijection and that $f(xy) = f(x)f(y)$ for all $x, y \in G$. That means that $f(x, y) = (xy)^{-1} = x^{-1}y^{-1} = f(x)f(y)$. That is, $y^{-1}x^{-1} = x^{-1}y^{-1}$. Multiplying this equality on the left and right by y, we have $x^{-1}y = yx^{-1}$. Then, multiplying with x on left and right, we have $yx = xy$ (which is valid for all $x, y \in G$, of course). Therefore, G is Abelian.

Problem. Let G be any group, with it operation denoted multiplicatively. Let H be a group with the same set as G and let its operation be defined by $x * y = y \cdot x$ (where $\cdot$ is the operation of G). Prove that $G \cong H$.

Solution. Let f be a mapping from H to G such that $f(x) = x$. As f is identity from the set H (or G) to itself (underlying sets of G and H are the same), it is a bijection. We have:

$$f(x * y) = x * y = y \cdot x = f(y) \cdot f(x) = f(x) * f(y).$$

[34] Not to be confused with the more specific $f(x) = \frac{1}{x}$ function on real numbers (without zero).
[35] Proved at the beginning of the script.

Therefore, f is an isomorphism from H to G and from that fact we have $G \cong H$.

Problem. Let c be a fixed element of G. Let H be a group with the same set as G, and with the operation $x * y = xcy$. Prove that the function $f(x) = c^{-1}x$ is an isomorphism from G to H.

Solution. First we will show that f is a bijection. Let $f(x) = f(y)$. Then $c^{-1}x = c^{-1}y$. As $c \in G$ and G is a group, we can multiply this equation with c on the left to get $x = y$. From this follows that f is an injection. Next, if we take $y \in H$ we need to find $x \in G$ such that $c^{-1}x = y$. And that is $x = cy$. As $y \in H$, it is also in G (underlying sets are same), and the product cy is in G (as G is a group). Such element exists in G and f is a surjection, and by that a bijection. Furthermore, consider:

$$f(xy) = c^{-1}xy = c^{-1}xcc^{-1}y = f(x)cf(y) = f(x) * f(y).$$

Then, f is an isomoprhism from G to H and $G \cong H$.

Definition. If G is a group, an **automorphism** of G is an isomorphism from G to G.

Comment. Since an automorphism is a bijection from G to G it is a permutation of G.

Problem. Prove the following:

1. Permutation $f = (1\ 5)(2\ 4)$ (where $f \in S_6$) is an automorphism of $\mathbb{Z}_6$;
2. Permutations $f_1 = (1\ 2\ 4\ 3)$, $f_2 = (1\ 3\ 4\ 2)$ and $f_3 = (1\ 4)(2\ 3)$ (where $f_i \in S_5$) are all automorphisms of $\mathbb{Z}_5$;
3. If G is any group, and a is any element of G, then $f(x) = axa^{-1}$ is an automorphism of G;
4. The set $\mathrm{Aut}(G)$ of all automorphisms of G is a subgroup of S_G.

Solution.

1. *Permutation $f = (1\ 5)(2\ 4)$ (where $f \in S_6$) is an automorphism of $\mathbb{Z}_6$.* Group $\mathbb{Z}_6$ is a cyclic group generated by 1 with a defining equation $6 \cdot 1 = 0$ (multiplication here is a shorthand for more consecutive additive operations). Now, notice that $\mathbb{Z}_6$ can also be generated by 5 with a defining equation $6 \cdot 5 = 0$. We will see that it is true, as we have $f(0) = 0$, $f(1) = 5$, $f(1 +_6 1) = f(2) = 4 = 5 +_6 5$, $f(2 +_6 1) = f(3) = 3 = 5 +_6 5 +_6 5$, $f(3 +_6 1) = f(4) = 2 = 5 +_6 5 +_6 5 +_6 5$,

$f(4 +_6 1) = f(5) = 1 = 5 +_6 5 +_6 5 +_6 5 +_6 5$ and $f(5 +_6 1) = f(0) = 0$. As generators and defining equations correspond, f is an automorphism of $\mathbb{Z}_6$.

2. *Permutations* $f_1 = (1\ 2\ 4\ 3)$, $f_2 = (1\ 3\ 4\ 2)$ *and* $f_3 = (1\ 4)(2\ 3)$ *(where* $f_i \in S_5$*) are all automorphisms of* $\mathbb{Z}_5$. Elements 2, 3 and 4 all generate $\mathbb{Z}_5$ (as they are relatively prime to 5; reader can easily check this fact). The defining equations are $5 \cdot 2 = 0$, $5 \cdot 3 = 0$ and $5 \cdot 4 = 0$, respectively. Now, for f_1, we have $f_1(1) = 2$, $f_1(2) = 4 = 2 +_5 2$, $f_1(3) = 1 = 2 +_5 2 +_5 2$, $f_1(4) = 3 = 2 +_5 2 +_5 2 +_5 2$ and $f_1(0) = 0$. For f_2, we have $f_2(1) = 3$, $f_2(2) = 1 = 3 +_5 3$, $f_2(3) = 4 = 3 +_5 3 +_5 3$, $f_2(4) = 2 = 3 +_5 3 +_5 3 +_5 3$ and $f_2(0) = 0$. Furthermore, $f_3(1) = 4$, $f_3(2) = 3 = 4 +_5 4$, $f_3(3) = 2 = 4 +_5 4 +_5 4$, $f_3(4) = 1 = 4 +_5 4 +_5 4 +_5 4$ and $f_3(0) = 0$. Therefore, f_1, f_2 and f_3 are automorphisms of $\mathbb{Z}_5$.

3. *If* G *is any group, and* a *is any element of* G*, then* $f(x) = axa^{-1}$ *is an automorphism of* G. First, we will check whether f is bijective. As $f(x) = f(y)$ will, when we multiply the equation $axa^{-1} = aya^{-1}$ with a^{-1} on the left and a on the right, imply $x = y$, function f is injective. Surjectivity will hold as for any $y \in G$ we can find $x \in G$ such that $y = f(x)$; we have $y = axa^{-1}$ and multiplying it with a^{-1} on the left and a on the right will yield $x = a^{-1}ya$. Then, x is obviously in G, as G is a group, closed with respect to inverses and multiplication. Therefore, f is bijective. For now we can say that f is a permutation. But, also:

$$f(xy) = axya^{-1} = axa^{-1}aya^{-1} = f(x)f(y).$$

Therefore, f is an automorphism of G.

4. *The set* $\mathrm{Aut}(G)$ *of all automorphisms of* G *is a subgroup of* S_G. As $f \in \mathrm{Aut}(G)$ implies f is an automorphism, and by that a permutation, then $f \in S_G$. From that we have that $\mathrm{Aut}(G) \subseteq S_G$. If we take $f, g\mathrm{Aut}(G)$, their product fg will be in $\mathrm{Aut}(G)$, as product of two permutations is a permutation, and as $f(xy) = f(x)f(y)$ and $g(xy) = g(x)g(y)$, we have $f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y))$, their product is (an isomorphism and) an automorphism of G. If we take $f \in \mathrm{Aut}(G)$, we have that $f(xy) = f(x)f(y)$. From that, we have $f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(x))f(f^{-1}(y)) = xy$. Then, applying $f^{-1} \in S_G$ on this equation gives us $f^{-1}(x)f^{-1}(y) = f^{-1}(xy)$. Therefore, f^{-1} is an automorphism of G, and $\mathrm{Aut}(G)$ is closed with respect to multiplication and inverses. Thus, $\mathrm{Aut}(G)$ is a subgroup of S_G.

Order of group elements

Definition. Let G be a group, $n \in \mathbb{N}$ and $a \in G$. We define:

$$\begin{aligned} a^n &= \underbrace{a \cdot a \cdots a}_{n \text{ times}}, \\ a^{-n} &= \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ times}}, \\ a^0 &= e, \end{aligned}$$

where $e \in G$ is a neutral element of G and $a^{-1} \in G$ inverse of a.

Proposition. If G is a group, $a \in G$ and $m, n \in \mathbb{Z}$, then the following holds:

1. $a^m a^n = a^{m+n}$,
2. $(a^m)^n = a^{mn}$,
3. $a^{-n} = (a^{-1})^n = (a^n)^{-1}$.

Proof. First we will prove for $m > 0$ and $n > 0$. Ad 1. If $m > 0$ and $n > 0$, we have:

$$a^m a^n = \underbrace{a \cdot a \cdots a}_{m \text{ times}} \underbrace{a \cdot a \cdots a}_{n \text{ times}} = \underbrace{a \cdot a \cdots a}_{m+n \text{ times}} = a^{m+n}.$$

Ad 2. For $m > 0$ (or $m \leq 0$; observe it does not change anything) and $n > 0$:

$$(a^m)^n = \underbrace{a^m \cdot a^m \cdots a^m}_{n \text{ times}} = \underbrace{a \cdot a \cdots a}_{mn \text{ times}}.$$

Ad 3. If we have $n > 0$, then:

$$a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ times}} = \left(a^{-1}\right)^n.$$

Also, we have, by a previous proposition, that:

$$(a^n)^{-1} = \left(\underbrace{a \cdot a \cdots a}_{n \text{ times}}\right)^{-1} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ times}} = (a^{-1})^n = a^{-n}.$$

Now, we will prove other cases. Ad 1. If $m < 0$ and $n > 0$. We will take $k = -m$. That way, $k \in \mathbb{N}$ and we have:

$$a^m a^n = a^{-k} a^n = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{k \text{ times}} \underbrace{a \cdot a \cdots a}_{n \text{ times}}.$$

If $k > n$ then we have n pairs of $a^{-1}a$ and the rest is a^{-1}, and $k-n$ of them. Therefore we have $a^m a^n = (a^{-1})^{k-n}$. As $k > n$ then $k - n$ is positive, and by (3) we have $a^m a^n = (a^{-1})^{k-n} = a^{n-k} = a^{m+n}$. If $k < n$ then we have k pairs of $a^{-1}a$ and the $n - k$ rest is a. Therefore we have again $a^{m+n} = a^{n-k} = a^{m+n}$. The same proof goes when $m > 0$ and $n < 0$. If $m < 0$ and $n < 0$, and we take $p = -m$ and $q = -n$, then p and q are natural numbers. Then, $a^m a^n = a^{-p} a^{-q}$. By definition:

$$a^m a^n = a^{-p} a^{-q} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{p \text{ times}} \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{q \text{ times}}.$$

We have a^{-1} multiplied by itself $p+q$ times, therefore $a^m a^n = (a^{-1})^{p+q}$. As $(p+q) \in \mathbb{N}$, we can use (3) and get:

$$a^m a^n = a^{-(p+q)} = a^{-p+(-q)} = a^{m+n}.$$

If $m = 0$ or $n = 0$ (or both) it's trivial to see that $a^m a^0 = a^m e = a^m = a^{m+0}$, $a^0 a^0 = ee = e = a^0 = a^{0+0}$, et cetera. Ad 2. If $m < 0$ and $n > 0$. Take $m = -p$ and we get, with positive p,

$$(a^m)^n = \left(a^{-p}\right)^n = \left(\underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{p \text{ times}} \right)^n = \left(a^{-1}\right)^{pn}.$$

By using (3) we have $(a^m)^n = a^{-pn} = a^{mn}$. If $m > 0$ and $n < 0$, and we take $n = -q$, then $q \in \mathbb{N}$, and we have:

$$(a^m)^n = (a^m)^{-q} = \underbrace{(a^m) - 1 \cdot (a^m)^{-1} \cdots (a^m)^{-1}}_{q \text{ times}}.$$

As $m > 0$, by using (3), we have $(a^m)^{-1} = a^{-m}$. Furthermore,

$$(a^m)^n = \underbrace{a^{-m} \cdot a^{-m} \cdots a^{-m}}_{q \text{ times}} = \left(a^{-m}\right)^q.$$

Now we have the case we already proved just a moment ago (for $m < 0$ and $n > 0$) and $(a^m)^n = a^{-mq} = a^{mn}$. Now, to prove when $m < 0$ and $n < 0$. We take $m = -p$ and $n = -q$. Then,

$$(a^m)^n = \left(a^{-p}\right)^{-q} = \underbrace{\left(a^{-p}\right)^{-1} \cdot \left(a^{-p}\right)^{-1} \cdots \left(a^{-p}\right)^{-1}}_{q \text{ times}}.$$

Providing we prove that $(a^{-p})^{-1} = a^{-(-p)} = a^p$ (for positive p) we will have:

$$(a^m)^n = \left(a^{-p}\right)^{-q} = \underbrace{a^p \cdot a^p \cdots a^p}_{q \text{ times}} = a^{pq} = a^{(-m)\cdot(-n)} = a^{mn}.$$

If $m = 0$ or $n = 0$ (or both), then the cases are trivial. We have $(a^0)^n = e^n = e = a^0 = a^{n\cdot 0}$, then $(a^m)^0 = e = a^0 = a^{m\cdot 0}$ and $(a^0)^0 = e^0 = e = a^0 = a^{0\cdot 0}$. Ad 3. Now, to justify for $n < 0$, we will take $n = -p$ and have $a^{-n} = a^{-(-p)} = a^p$. As proven previously that $\left(a^{-1}\right)^{-1} = a$, we have:

$$a^{-n} = a^p = \left(\left(a^{-1}\right)^{-1}\right)^p = \left(a^{-1}\right)^{-p} = \left(a^{-1}\right)^n.$$

Similarly, we have:

$$\left(a^{-p}\right)^{-1} = \left(\left(a^{-1}\right)^p\right)^{-1} = \underbrace{\left(a^{-1}\right)^{-1} \cdot \left(a^{-1}\right)^{-1} \cdots \left(a^{-1}\right)^{-1}}_{p \text{ times}} = \underbrace{a \cdot a \cdots a}_{p \text{ times}} = a^p = a^{-n}.$$

Finally, we have $a^{-0} = a^0 = e = e^{-1} = (a^0)^{-1}$ and $a^{-0} = a^0 = e = (a^{-1})^0$.

□

Definition. If there exists $m \in \mathbb{Z}^*$ such that $a^m = e$, then the **order of the element** a is defined to be the least $n \in \mathbb{N}$ such that $a^n = e$, that is:

$$n = \min\left(\{m \in \mathbb{Z}^* : \ a^m = e\} \cap \mathbb{N}\right).$$

Then we write $\operatorname{ord}(a) = n$. If there does not exist $m \in \mathbb{Z}^*$ such that $a^m = e$, we say that a has **order infinity** and we write $\operatorname{ord}(a) = \infty$.

Proposition. Let G be a group. If there exists $m \in \mathbb{Z}^*$ such that $a^m = e$, where $a, e \in G$, then there exists $n \in \mathbb{N}$ such that $a^n = e$.

Proof. If $m > 0$ then $n = m$. If $m < 0$, then we take $m = -n$ and have $a^{-n} = e$. Multiplying by a^n on the right gives us $a^{-n}a^n = ea^n$ and that is $e = a^n$. This concludes the proof.

□

Furthermore, let us remind ourselves of one important theorem (divison with remainder). I will ommit the proof, as I already have it in my work on elementary number theory, discussed in much detail.

Theorem (division with remainder). Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^*$. There exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.

Proof. *Discussed in my work on elementary number theory.*

□

This we shall use to prove the following theorem.

Theorem. Let G be a group and $a \in G$. If $\operatorname{ord}(a) = n$, then there exists $k \in \{0, 1, \ldots, n-1\}$ such that $a^k = a^m$ for all $m \in \mathbb{Z}$. Furthermore $a^i \neq a^j$, for all $i, j \in \{0, 1, \ldots, n-1\}$ and $i \neq j$.

Proof. As $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, id est $n \in \mathbb{Z}^*$ (note that order of a group element is defined as a natural number, and is therefore a positive integer) then, by division with remainder theorem, there exist unique $q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r < |n| = n$. Therefore a^m can be written as a^{nq+r}. By previous proposition, we have that $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$, for all $m, n \in \mathbb{Z}$. Therefore:

$$a^m = a^{nq+r} = a^{nq} a^r = (a^n)^q \, a^r.$$

By definition of order of group element, as we have $\operatorname{ord}(a) = n$, then $a^n = e$. So we have $a^m = e^q a^r = a^r$. But, by division with remainder theorem, we have that $0 \leq r < n$, i.e. $r \in \{0, 1, \ldots, n-1\}$. So we can take $k = r$ and have $a^m = a^k$.

Now suppose that $a^i = a^j$, for some $i, j \in \{0, 1, \ldots, n-1\}$ and $i \neq j$. Also suppose that $i < j$. Note that $i, j < n$. Then we can take some $k \in \mathbb{N}$ such that $j = i + k$. As $j < n$ then $i + k < n$, that is $k < n - i < n$. From that it follows that $a^i = a^{i+k} = a^i a^k$. But, that would mean, if we multiply this expression by a^{-i} on the left, that $e = a^k$. Then the order of a is either $k < n$, which is a contradiction to the assumption that the order is n (that n is the least positive integer such that $a^n = e$), or $k = n$, which would mean that $j = i + n$, contradicting assumption that $j < n$. Thus, it has to be that $a^i \neq a^j$ for all $i, j \in \{0, 1, \ldots, n-1\}$ where $i \neq j$.

□

Proposition. Let G be a group and $a \in G$. If $\operatorname{ord}(a) = \infty$, then all powers of a are different, i.e. $a^i \neq a^j$ for all $i, j \in \mathbb{Z}$ such that $i \neq j$.

Proof. Suppose that $a^i = a^j$ for some $i, j \in \mathbb{Z}$ and $i \neq j$. Suppose that $i < j$. That means that $j = i + k$, where $k \in \mathbb{Z}$. If we multiply the expression $a^i = a^{i+k}$ by a^{-i} on the left, we get $e = a^{-i}a^{i+k}$, that is, $e = a^{i+k}$. But, as $\operatorname{ord}(a) = \infty$, there does not exist $n \in \mathbb{Z}^*$ such that $a^n = e$. Therefore, the only possible option is that $i + k = 0$ so that $e = a^0$. That would mean that $k = -i$ and that $j = i - i = 0$. Then from assumption that $a^i = a^j$ would follow that $a^i = a^0 = e$ and it must be that $a^i = e$. Again, as $\operatorname{ord}(a) = \infty$, it must be that $i = 0$, contradicting our assumption that $i \neq j$. In conclusion, all powers of a are different (if $\operatorname{ord}(a) = \infty$).

□

Proposition. Let G be a group and $a \in G$. If $\operatorname{ord}(a) = n$ and $a^t = e$ for some $t \in \mathbb{Z}$, then $n|t$.

Proof. Suppose that $\operatorname{ord}(a) = n$, $a^t = e$ for some $t \in \mathbb{Z}$, but $n \nmid t$, i.e. by division with remainder theorem, we have that $t = nq + r$, where $q, r \in \mathbb{Z}$ such that $0 \leq r < |n| = n$. That means that $a^{nq+r} = e$. We have $a^{nq}a^r = e$ and from that $(a^n)^q a^r = e$. As $\operatorname{ord}(a) = n$ we have $a^n = e$ and from that $e^q a^r = e$, that is, $a^r = e$. But, n is the least positive number such that $a^n = e$ and $r < n$. Therefore, as r cannot be n, it can only be zero, that is $r = 0$. Then, from $t = nq + r$, we have $t = nq + 0 = nq$. In other words, there exists $q \in \mathbb{Z}$ such that $t = nq$, which means that $n|t$.

□

Proposition. Let G be a group and $a, e \in G$. Then, $\operatorname{ord}(a) = 1$ if and only if $a = e$.

Proof. *Necessity.* If $\operatorname{ord}(a) = 1$ then $a^1 = e$ and that is $a = e$. *Sufficiency.* If $a = e$, i.e. $a^1 = e$, obviously $\operatorname{ord}(a) = 1$, as there is no $n \in \mathbb{N}$ such that $n < 1$ (that is, 1 is the least natural number such that $a^n = e$).

□

Problem. Determine the order of: (a) $10 \in \mathbb{Z}_{25}$, (b) $6 \in \mathbb{Z}_{16}$, (c) $f = (1\ 6\ 4\ 2) \in S_6$, (d) $1 \in \mathbb{R}^*$, (e) $1 \in \mathbb{R}$, (f) $f \in S_A$, where $A = \mathbb{R}\backslash\{0, 1, 2\}$ and $f(x) = \frac{2}{2-x}$.

Solution. (a) $\operatorname{ord}(10) = 5$ as $5 \cdot 10 \equiv 0 \pmod{2)5}$, and it's the smallest one (notice that $5 = \gcd(10, 25)$). (b) $\operatorname{ord}(6) = 8$ as $8 \cdot 6 \equiv 0 \pmod{1)6}$, and it's the smallest one as $\gcd(6, 16) = 48$. (c) For a cycle c of length n we have that $c^n = \epsilon$ (proven previously). As length of f is 4, we have $f^4 = \epsilon$, thus $\operatorname{ord}(f) = 4$. (d) In $\mathbb{R}^*$ neutral element is 1, therefore, by previous proposition, $\operatorname{ord}(1) = 1$. (e) Obviously $\operatorname{ord}(1) = \infty$ as there does not exist $n \in \mathbb{N}$ such that $n \cdot 1 = 0$. (f) We have:

$$
\begin{aligned}
[f \circ f](x) &= \frac{2}{2-\frac{2}{2-x}} = \frac{2}{\frac{2-2x}{2-x}} = \frac{2-x}{1-x}. \\
[f \circ f \circ f](x) &= \frac{2-\frac{2}{2-x}}{1-\frac{2}{2-x}} = \frac{\frac{2-2x}{2-x}}{\frac{-x}{2-x}} = \frac{2x-2}{x}. \\
[f \circ f \circ f \circ f](x) &= \frac{2\cdot\frac{2}{2-x}-2}{\frac{2}{2-x}} = \frac{\frac{2x}{2-x}}{\frac{2}{2-x}} = x.
\end{aligned}
$$

Therefore, $\operatorname{ord}(f) = 4$.

Problem. Can an element of an infinite group have finite order?

Solution. Group $\mathbb{C}^*$ is infinite. It is a group, as associativity holds $z_1(z_2z_3) = (z_1z_2)z_3$, for all $z_1, z_2, z_3 \in \mathbb{C}^*$. Neutral element is $1 \in \mathbb{C}^*$ as $z \cdot 1 = z$, for all $z \in \mathbb{C}^*$. Each element has an inverse, $(a+bi)^{-1} = \frac{a-bi}{a^2+b^2}$, for all $(a+bi) \in \mathbb{C}^*$. But, taking roots of unity $\omega_n^i \in \mathbb{C}^*$, where $i \in \{0, \ldots, n-1\}$ and $n \in \mathbb{N}\backslash\{1\}$, we have that $\omega_n^n = 1$, i.e. $\operatorname{ord}(\omega_n) = n$. Same thing would go for $-1 \in \mathbb{R}^*$, as $(-1)^2 = 1$, that is $\operatorname{ord}(-1) = 2$ (notice that -1 is also a root of unity for $n = 2$).

Problem. In $\mathbb{Z}_{24}$, list all the elements of order (a) 2, (b) 3, (c) 4, (d) 6.

Solution. In order to solve $nx \equiv 0 \pmod{2}4$ for x, where $n \in \{2, 3, 4, 6\}$, we actually have $nx - 0 = 24k$, i.e. $nx = 24k$, where $k \in \mathbb{Z}$. In other words we need to observe only multiples of 24, e.g. 24, 48, 72, 96, 120, etc. (a) We only have $2 \cdot 12 = 24$, there is no other element between 12 and 24 that would yield 24 or 48 when multiplied by 2. So, $\operatorname{ord}(12) = 2$. (b) We have $3 \cdot 8 = 24$ and $3 \cdot 16 = 48$, so $\operatorname{ord}(8) = 3$ and $\operatorname{ord}(16) = 3$. (c) We have $4 \cdot 6 = 24$, $4 \cdot 12 = 48$ (but this one does not count as also $2 \cdot 12 = 24$) and $4 \cdot 18 = 72$, therefore $\operatorname{ord}(6) = 4$ and $\operatorname{ord}(18) = 4$. (d) We have $6 \cdot 4 = 24$, $6 \cdot 8 = 48$ (but this one does not count as $3 \cdot 8 = 24$), then $6 \cdot 12 = 72$ (also does not count as $2 \cdot 12 = 24$), $6 \cdot 16 = 96$ (does not count as $3 \cdot 16 = 48$) and $6 \cdot 20 = 120$. So, $\operatorname{ord}(4) = 6$, $\operatorname{ord}(20) = 6$.

Theorem. Let G be a group and $a_1, \ldots, a_n \in G$. Then, for any $m \in \mathbb{N}$ and $1 < k < n$ we have that

$$(a_1a_2 \cdots a_n)^m = e,$$

implies that

$$(a_k a_{k+1} \cdot a_n a_1 a_2 \dots a_{k-1})^m = e.$$

Proof. We rewrite the first expression as:

$$(a_1 a_2 \cdots a_n)(a_1 a_2 \cdots a_n)^{m-2}(a_1 a_2 \cdots a_n) = e.$$

Multiplying by $(a_1 a_2 \cdots a_{k-1})^{-1}$ on the left and by $(a_1 a_2 \cdots a_{k-1})$ on the right gives us:

$$\begin{aligned} e &= (a_1 a_2 \cdots a_{k-1})^{-1}(a_1 a_2 \cdots a_{k-1} a_k a_{k+1} \cdots a_n)(a_1 a_2 \cdots a_n)^{m-2} \\ &\cdot (a_1 a_2 \cdots a_{k-1} a_k a_{k+1} \cdots a_n)(a_1 a_2 \cdots a_{k-1}). \end{aligned}$$

That leaves us with:

$$(a_k a_{k+1} \cdots a_n)(a_1 a_2 \cdots a_n)^{m-2}(a_1 a_2 \cdots a_{k-1} a_k a_{k+1} \cdot a_n)(a_1 a_2 \cdots a_{k-1}) = e.$$

Using associativity in G, and as the elements are "in the same order", and their numbers are equal, i.e. we have a_i for $1 + m - 2 + 1$ times for $k \leq i \leq n$ and $m - 2 + 1 + 1$ times for $1 \leq i \leq k - 1$, it is obvious that this is equivalent to:

$$(a_k a_{k+1} \cdots a_n a_1 a_2 \cdots a_{k-1})^m = e.$$

□

Problem. Let a, b and c be elements of a group G. Prove the following:

1. If $\operatorname{ord}(a) = n$, then $a^{n-r} = (a^r)^{-1}$;
2. If $a^k = e$ where k is odd, then the order of a is odd;
3. $\operatorname{ord}(a) = \operatorname{ord}(bab^{-1})$;
4. $\operatorname{ord}(a^{-1}) = \operatorname{ord}(a)$;
5. The order of ab is the same as the order of ba;
6. $\operatorname{ord}(abc) = \operatorname{ord}(cab) = \operatorname{ord}(bca)$;
7. Let $x = a_1 a_2 \cdots a_n$, and let $y = a_k a_{k+1} \cdots a_n a_1 \cdots a_{k-1}$, where $1 < k < n$. Then $\operatorname{ord}(x) = \operatorname{ord}(y)$.

Solution.

1. *If* $\operatorname{ord}(a) = n$*, then* $a^{n-r} = (a^r)^{-1}$. Let $\operatorname{ord}(a) = n$. That means that $a^n = e$. If we multiply this by a^{-r} on the right we have $a^n a^{-r} = ea^{-r}$. But, $a^n a^{-r} = a^{n+(-r)} = a^{n-r}$ and $ea^{-r} = a^{-r} = (a^r)^{-1}$, so $a^{n-r} = (a^r)^{-1}$.

2. *If* $a^k = e$ *where* k *is odd, then the order of* a *is odd.* By a previous proposition, if $m = \operatorname{ord}(a)$, then $m|k$. Therefore, there exists $n \in \mathbb{Z}$ such that $k = nm$. If m were even, then whether n were even or odd, k would be even also, contrary to the assumption that k is odd. Therefore $m = \operatorname{ord}(a)$ must be odd.

3. $\operatorname{ord}(a) = \operatorname{ord}(bab^{-1})$. Let $m = \operatorname{ord}(a)$ and $n = \operatorname{ord}(bab^{-1})$. That means that if $a^k = e$, for some $k \in \mathbb{N}$, then $m \leq k$ (order is the least positive integer for which $a^k = e$). The same thing goes if $(bab^{-1})^l = e$, for some $l \in \mathbb{N}$, then $n \leq l$. First, if we take $a^m = e$ and we multiply it by b^{-1} on the right and b on the left, we have $ba^m b^{-1} = bb^{-1}$. Now, we can write that down as:

$$b\underbrace{a \cdot a \cdots a}_{m \text{ times}} b^{-1} = e.$$

   But, between each $a \cdot a$ we can put $e = bb^{-1}$, so that we have string of $ab^{-1}ba = aa$. We will put in $m-1$ of neutral elements written down as $b^{-1}b$. That is (counting in b on the left and b^{-1} on the right):

$$\underbrace{\left(bab^{-1}\right) \cdot \left(bab^{-1}\right) \cdots \left(bab^{-1}\right)}_{m \text{ times}} = e.$$

   But, that means that $(bab^{-1})^m = e$ and by definition of order of bab^{-1}, we have that $n \leq m$. On the other hand, we have $(bab^{-1})^n = e$. That can be written as:

$$\underbrace{\left(bab^{-1}\right) \cdot \left(bab^{-1}\right) \cdots \left(bab^{-1}\right)}_{n \text{ times}} = e.$$

   But, each bb^{-1} can be eliminated as, obviously, $bb^{-1} = e$. All that is left is $ba^n b^{-1} = e$. Multiplying by b^{-1} on the left and b on the right we have $a^n = e$. And, by definition of order of a, we have that $m \leq n$. Combining $m \leq n$ and, previously obtained, $n \leq m$, we have $m = n$. In other words, $\operatorname{ord}(a) = \operatorname{ord}(bab^{-1})$.

4. $\operatorname{ord}(a^{-1}) = \operatorname{ord}(a)$. We can take $m = \operatorname{ord}(a^{-1})$ and $n = \operatorname{ord}(a)$. Then, for all $k \in \mathbb{N}$, if $(a^{-1})^k = e$ then $m \leq k$. Also, for all $l \in \mathbb{N}$, if $a^l = e$, then $n \leq l$. First, let's take a look at $(a^{-1})^m = e$, that is $a^{-m} = e$. If we multiply that by a^m on

the left, we have $a^m a^{-m} = a^m e$, i.e. $a^m = e$. By definition of order of a, we have that $n \leq m$. Now, if we take $a^n = e$, and we multiply it by a^{-n} on the right, we have, $a^n a^{-n} = e a^{-n}$, and that is $e = a^{-n}$. That can be written as $(a^{-1})^n = e$ and by definition of order of a^{-1} we have that $m \leq n$. As we have $m \leq n$ and $n \leq m$, it's $m = n$, i.e. $\operatorname{ord}(a^{-1}) = \operatorname{ord}(a)$.

5. *The order of ab is the same as the order of ba.* Let's take $m = \operatorname{ord}(ab)$ and $n = \operatorname{ord}(ba)$. We need to show that $m = n$. As in previous two excercises, we have $(ab)^m = e$. That is:

$$\underbrace{(ab)(ab)\cdots(ab)}_{m \text{ times}} = e.$$

We can rearrange that to get $a(ba)^{m-1}b = e$. Multiplying that by a^{-1} on the left and by a on the right, we get $(ba)^{m-1}(ba) = e$ and that is $(ba)^m = e$. By definition of order of (ba) we have $n \leq m$. Similarly, we have $(ba)^n = e$, i.e.

$$\underbrace{(ba)(ba)\cdots(ba)}_{n \text{ times}} = e.$$

We can rearrange that to get $b(ab)^{n-1}a = e$. Multiplying by b^{-1} on the left and by b on the right, we have $(ab)^{n-1}(ab) = e$, that is $(ab)^n = e$. By definition of order of (ab) we have $m \leq n$. Combining $m \leq n$ and $n \leq m$ we have $n = m$, which was to be shown.

6. $\operatorname{ord}(abc) = \operatorname{ord}(cab) = \operatorname{ord}(bca)$. Let $p = \operatorname{ord}(abc)$, $q = \operatorname{ord}(cab)$ and $r = \operatorname{ord}(bca)$. From first expression we have that $(abc)^p = e$. That is:

$$(abc)(abc)^{p-2}(abc) = e.$$

Multiplying by c^{-1} on the right and by c on the left we have:

$$cabc(abc)^{p-2}abcc^{-1} = cc^{-1},$$

which is, by careful examination, $(cab)^p = e$. As $q = \operatorname{ord}(cab)$ we have that $p \geq q$. Now, taking $(cab)^q = e$ and transforming it into $(cab)(cab)^{q-2}(cab) = e$ we will have, by multiplying with c^{-1} on the left and c on the right that $ab(cab)^{q-2}cabc = e$, i.e. $(abc)^q = e$. From that we have $q \geq p$ and finally, by combining this with a previous result, $p = q$, that is, $\operatorname{ord}(abc) = \operatorname{ord}(cab)$. Now, the same thing goes for $\operatorname{ord}(bca)$ and this is generalized by previous theorem and following problem.

7. *Let* $x = a_1a_2\cdots a_n$*, and let* $y = a_ka_{k+1}\cdots a_na_1\cdots a_{k-1}$*, where* $1 < k < n$*. Then* $\operatorname{ord}(x) = \operatorname{ord}(y)$. Let $p = \operatorname{ord}(x)$ and $q = \operatorname{ord}(y)$. By previous theorem we have that $x^p = e$ implies $y^p = e$ and by that we have that $q \leq p$. Then, we have $y^q = e$ and that implies $x^q = e$. Therefore, $p \leq q$. So, that is $p = q$, i.e. $\operatorname{ord}(x) = \operatorname{ord}(y)$.

Problem. Let a be any element of finite order of a group G. Prove the following:

1. If $a^p = e$ where p is a prime number, and $a \neq e$, then a has order p;
2. The order of a^k is a divisor (factor) of the order of a;
3. If $\operatorname{ord}(a) = km$, then $\operatorname{ord}\left(a^k\right) = m$;
4. If $\operatorname{ord}(a) = n$ where n is odd, then $\operatorname{ord}(a^2) = n$;
5. If a has order n, and $a^r = a^s$, then n is a factor of $r - s$;
6. If a is the only element of order k in G, then a is in the center of G;
7. If the order of a is not a multiple of m, then the order of a^k is not a multiple of m;
8. If $\operatorname{ord}(a) = mk$ and $a^{rk} = e$, then r is a multiple of m.

Solution.

1. *If* $a^p = e$ *where* p *is a prime number, and* $a \neq e$*, then* a *has order* p. Let's denote $n = \operatorname{ord}(a)$. Then, as $a^p = e$, by previous theorem, we have that $n|p$. But, p has only two divisors, by definition, 1 and p. If it were $n = 1$, then it would be that $a = e$, contradicting that $a \neq e$. So, we are left with $n = p$, i.e. $\operatorname{ord}(a) = p$.
2. *The order of* a^k *is a divisor (factor) of the order of* a. Let $n = \operatorname{ord}(a)$ and $m = \operatorname{ord}\left(a^k\right)$. We have to prove that $m|n$. First we have $a^n = e$ and, as $e = e^k = (a^n)^k$, from that follows $(a^n)^k = e$. Furthermore, as $(a^n)^k = a^{nk} = \left(a^k\right)^n$, we have that $\left(a^k\right)^n = e$. As $m = \operatorname{ord}\left(a^k\right)$, by previous proposition, we have that $m|n$.
3. *If* $\operatorname{ord}(a) = km$*, then* $\operatorname{ord}\left(a^k\right) = m$. Let us denote $n = \operatorname{ord}\left(a^k\right)$. We have to prove that $m = n$. As n is the order of a^k, by previous proposition it's $n \leq m$. Next, we have $\left(a^k\right)^n = e$, i.e. $a^{kn} = e$. So, by definition of order of a, it's $km \leq kn$. Note that $k > 0$ (if it were that $k = 0$, we would have that order of a is zero, contradicting the definition that order is positive; if it were that $k < 0$, then it would have to be that $m < 0$ and then m couldn't possibly be order of a^k). That said dividing $km \leq kn$ with k does not change the inequality and we have $m \leq n$. Combining that with $n \leq m$, we have successfuly shown that $n = m$.

4. *If* $\operatorname{ord}(a) = n$ *where* n *is odd, then* $\operatorname{ord}(a^2) = n$. Let us denote $\operatorname{ord}(a^2) = m$. We have to prove that $m = n$. From a previous problem we have that $m|n$, so m has to be odd too. We have $a^{2m} = e$, and from that $n|2m$. As n is odd, it cannot possibly divide 2 (which is a prime number), so we only have that $n|m$. As $m|n$ and $n|m$ it must be that $m = n$.

5. *If* a *has order* n*, and* $a^r = a^s$*, then* n *is a factor of* $r - s$. As $a^r = a^s$, multiplying the equation by a^{-s} on the right gives us $a^{r-s} = e$. By previous proposition, as n is the order of a, we have that $n|(r - s)$.

6. *If* a *is the only element of order* k *in* G*, then* a *is in the center of* G. We have to prove that $ax = xa$ for all $x \in G$. From a previous problem we know that $\operatorname{ord}(a) = \operatorname{ord}(xax^{-1})$, for all $x \in G$. The additional condition in assumption is that a is the only element of order k in group G. But we see, due to the previous problem, that all xax^{-1} also have order k. Therefore it must be that $xax^{-1} = a$, for all $x \in G$. Multiplying equality on right by x gives us $xa = ax$, for all $x \in G$. Thus, a is in center of G.

7. *If the order of* a *is not a multiple of* m*, then the order of* a^k *is not a multiple of* m. From a previous problem, order of a^k (we will denote it by z) is a divisor of the order of a (denoted by w). So there must exist $p \in \mathbb{Z}$ such that $w = pz$. As w is not a multiple of m, there must exist $q, r \in \mathbb{Z}$, by the division with remainder theorem, such that $w = mq + r$ where $0 < r < |m|$. Plugging that information into $w = pz$, we have $mq + r = pz$. Suppose that z is a multiple of m. Then there exists $t \in \mathbb{Z}$ such that $z = mt$. If we put that into previous equation, we have that $mq + r = pmt$ and by that $m(pt - q) = r$. That would mean, as $(pt - q) \in \mathbb{Z}$, that $m|r$, and that $|m| \leq r$, which is a contradiction to the fact that $0 < r < |m|$. Therefore z, order of a^k, cannot be a multiple of m.

8. *If* $\operatorname{ord}(a) = mk$ *and* $a^{rk} = e$*, then* r *is a multiple of* m. From a previous problem it follows that if $\operatorname{ord}(a) = km$, then $\operatorname{ord}\left(a^k\right) = m$. Furthermore, from $a^{rk} = e$ we have $\left(a^k\right)^r = e$. From that it follows not only that $m \leq r$, but that $m|r$. That means that there exists $p \in \mathbb{Z}$ such that $r = pm$, in other words, r is a multiple of m.

Problem. Let a and b be elements of a group G. Let $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$; let $\operatorname{lcm}(m, n)$ denote the least common multiple of m and n. Prove:

1. If a and b commute, then $\operatorname{ord}(ab)$ is a divisor of $\operatorname{lcm}(m, n)$ (give a counterexample if they don't commute);

2. If m and n are relatively prime, then no power of a can be equal to any power of b (except for e);

3. If m and n are relatively prime, then the products $a^i b^j$ $(0 \leq i < m,\ 0 \leq j < n)$ are all distinct;

Solution.

1. *If a and b commute, then* $\operatorname{ord}(ab)$ *is a divisor of* $\operatorname{lcm}(m,n)$. From $a^m = e$ and $b^n = e$ it follows that $a^m b^n = e$. It's also true that $a^{mk} = e$ and $b^{nl} = e$ for any $k, l \in \mathbb{Z}$ which implies $a^{mk} b^{nl} = e$. We are looking for $k, l \in \mathbb{Z}$ such that $mk = nl$. Say $t = \operatorname{lcm}(m,n)$. Then from definition of least common multiple $m \mid t$ and $n \mid t$. So we can take $k = \frac{t}{m}$ and $l = \frac{t}{n}$. Then, $mk = nl$ will be true as $m\frac{t}{m} = n\frac{t}{n}$ yielding $t = t$. Therefore, we take $a^t b^t = e$. This is true as $t = mk$ and $t = nl$, where $k, l \in \mathbb{Z}$. As a and b commute we can use the rule $a^t b^t = (ab)^t$ (see problems in the beginning of the script) and then it's $(ab)^t = e$, i.e. $(ab)^{\operatorname{lcm}(m,n)} = e$. Using that and the definition of order it follows that $\operatorname{ord}(ab) \mid \operatorname{lcm}(m,n)$. Still in search of a counterexample, somewhere in D_n, quaternions, S_n...?

2. *If m and n are relatively prime, then no power of a can be equal to any power of b (except for e).* As m and n are relatively prime[36], then $\gcd(m,n) = \pm 1$. Suppose $a^k = b^l$ for some $k, l \in \mathbb{Z}$ such that $a^k \neq e$ and $b^l \neq e$. As they are equal, their orders are also, obviously, equal. Let us denote $q = \operatorname{ord}\left(a^k\right) = \operatorname{ord}\left(b^l\right)$. By a previous problem $\operatorname{ord}\left(a^k\right) \mid \operatorname{ord}(a)$ and $\operatorname{ord}\left(b^l\right) \mid \operatorname{ord}(b)$. That would mean that $q|m$ and $q|n$. But the only integer q for which it is true that q divides both m and n is either 1 or -1. Furthermore, order must be positive, so it's $\operatorname{ord}\left(a^k\right) = \operatorname{ord}\left(b^l\right) = 1$ and by a previous problem that means that $a^k = e$ and $b^l = e$, which is a contradiction to assumption that $a^k \neq e$ and $b^l \neq e$.

3. *If m and n are relatively prime, then the products $a^i b^j$ $(0 \leq i < m,\ 0 \leq j < n)$ are all distinct.* Suppose $a^i b^j = a^k b^l$, where $0 \leq i, k < m$ and $0 \leq j, l < n$. Further condition is that $i \neq k$ and $j \neq l$, as equality would then be trivial. If we multiply the equality with a^{-k} on the left and b^{-j} on the right, we get $a^{i-k} = b^{l-j}$. Now, by the same logic from previous problem it must be that $\operatorname{ord}\left(a^{i-k}\right) = \operatorname{ord}\left(b^{l-j}\right) = q$. So it must be that $q|m$ and $q|n$. But the only such possible number is 1 (remember order has to be positive). That would mean that $a^{i-k} = e$ and $b^{l-j} = e$. That is possible only when $i = k$ and $l = j$, contradicting our assumption that $i \neq k$ and $j \neq l$.

Problem. Let a be an element of order 12 in a group G.

1. What is the smallest positive integer k such that $a^{8k} = e$?

2. What is the order of a^8?

[36] In my works on introductory number theory, I define greatest common divisor to be a natural number, so it would only be that $\gcd(m,n) = 1$.

3. What are the orders of a^9, a^{10}, a^5?

Solution.

1. *What is the smallest positive integer k such that $a^{8k} = e$?* From a previous theorem, it follows that $12|8k$. Therefore, we are looking for k, l such that $8k = 12l$. We take $\text{lcm}(8, 12) = 24$ and $k = 3$, $l = 2$. Therefore $k = 3$.

2. *What is the order of a^8?* It must be that the order of a^8 divides 12. Therefore, it can be 1, 2, 3, 4, 6 and 12. Obviously it's 3 as $(a^8)^3 = a^{8\cdot 3} = a^{24} = a^{12\cdot 2} = (a^{12})^2 = e$.

3. *What are the orders of a^9, a^{10}, a^5?* Order of a^9 is 4 as $3|12$ and $(a^9)^4 = a^{36} = (a^{12})^3 = e$. Order of a^{10} is 6 as $6|12$ and $(a^10)^6 = a^{60} = (a^{12})^5 = e$. Order of a^5 is 12 as $12|12$ and $(a^5)^{12} = a^{60} = (a^{12})^5 = e$.

Lemma. Let G be a group, $a \in G$ such that $\text{ord}\,(a) = m$. Then, $k \in \mathbb{Z}$ is relatively prime to m, that is $\gcd(m, k) = 1$, if and only if $\text{ord}\left(a^k\right) = m$.

Proof. *Necessity.* Let $n = \text{ord}\left(a^k\right)$. We have to show that $m = n$. Now, we start with $\left(a^k\right)^n = e$. That is equivalent to $a^{kn} = e$ and it must be that $m|(kn)$. But, due to Euclid's lemma, as $\gcd(m, k) = 1$, it must be that $m|n$. Furthermore, form a previous problem, we have that $\text{ord}\left(a^k\right)|\text{ord}\,(a)$, id est $n|m$. From $m|n$ and $n|m$ we have $m = n$.

Sufficiency. Let $\text{ord}\left(a^k\right) = m$. Take $g = \gcd(m, k)$. Let's prove that $g = 1$. Let us also denote l as least common multiple of m and k. Then it's $l = \frac{mk}{g}$. As l is a multiple of m it's true that $a^l = e$. Substituting l for its expression gives us $a^{\frac{mk}{g}} = e$. It follows that $\left(a^k\right)^{\frac{m}{g}} = e$. But, as m is order of a^k, we have that $m|\frac{m}{g}$, i.e. there exists $q \in \mathbb{N}$ such that $\frac{m}{g} = qm$. Dividing by m (which is positive, by definition of order) yields $\frac{1}{g} = q$ and that is possible if and only if $g = 1$ (as g and q are both natural numbers).

□

Remark. For the next propositions we will use *fundamental theorem of arithmetic*, stating that every natural number can be decomposed as a product of prime factors in a unique way (up to order of factors). Proof can be found in my works on number theory.

Lemma. Let a and b commute. If m and n are relatively prime, then $\text{ord}\,(ab) = mn$.

Proof. Let us denote $q = \text{ord}\,(ab)$ and $l = \text{lcm}\,(m, n)$. As, m and n are relatively prime, they contain no common divisors (except 1), and by that, no prime divisors. So

we can write them down[37] as $m = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$, where $s, t \in \mathbb{N}$. Now, from a previous problem we have that $q|l$, so it must be that there exists some $k \in \mathbb{N}$ (as $q \in \mathbb{N}$ and $l \in \mathbb{N}$ it cannot be non-positive) such that $l = qk$. But, as m and n are relatively prime their least common multiple is mn. So we may say that:

$$q = \frac{p_1 p_2 \cdots p_t q_1 q_2 \cdots q_s}{k}.$$

Now, q is a natural number, so k must (obviously) divide mn. So it contains some or none p_i and some or none q_j. So we may say[38] that:

$$k = \prod_{i \in S} p_i \prod_{j \in T} q_j,$$

where $S \subseteq \{i \in \mathbb{N} : \ i \leq s\}$ and $T \subseteq \{j \in \mathbb{N} : \ j \leq t\}$. We may introduce new $k_1, k_2 \in \mathbb{N}$ such that k_1 is the product of p_i's and k_2 is the product of q_j's from the above equation, so we have that:

$$k = \underbrace{\prod_{i \in S} p_i}_{k_1} \underbrace{\prod_{j \in T} q_j}_{k_2} = k_1 k_2.$$

Obviously $k_1|m$ and $k_2|n$. So we may write:

$$q = \frac{m}{k_1} \frac{n}{k_2}.$$

It is obvious that both fractions are therefore integers. Also note that $\gcd(m, n) = 1$ and $\gcd(k_1, k_2) = 1$. As $(ab)^q = e$, we have $(ab)^{qk_1} = e$. Then,

$$a^{m\frac{n}{k_2}} b^{m\frac{n}{k_2}} = e.$$

But, as $\operatorname{ord}(a) = m$ and $\frac{n}{k_2} \in \mathbb{N}$, then $a^{m\frac{n}{k_2}} = e$ and we only have $b^{m\frac{n}{k_2}} = e$. But that would mean that $n|m\frac{n}{k_2}$. Due to Euclid's lemma, as m and n are relatively prime, it must be that $n|\frac{n}{k_2}$, i.e. there exists some $k' \in \mathbb{N}$ such that $\frac{n}{k_2} = nk'$. That means, after dividing by n (which is positive) that $\frac{1}{k_2} = k'$ and it must be that $k_2 = k' = 1$. Furthermore, we also have that $(ab)^{qk_2} = e$ and by that:

$$a^{\frac{m}{k_1}n} b^{\frac{m}{k_1}n} = e.$$

[37] Notice that here we are rather ambiguous as to which p_i equal some p_j, that is not of importance right now. On the other hand, we are unambiguous when saying $p_i \neq q_j$, for all $i \leq s$ and $j \leq t$.

[38] I sometimes denote indices differently to add some unnecessary unambiguity.

But here $b^{\frac{m}{k_1}n} = e$ so it must be that $a^{\frac{m}{k_1}n} = e$. From that we have $m|\frac{m}{k_1}n$. By Euclid's lemma, as m and n are relatively prime, we have $m|\frac{m}{k_1}$ and that is, by the same reasoning as for n, possible only when $k_1 = 1$. Therefore, from $k_1k_2q = mn$ we have $q = mn$, that is, $\operatorname{ord}(ab) = mn$, when m and n are relatively prime.

□

Remark. In next two theorems we will denote P as the set of all primes, i.e.

$$P = \{n \in \mathbb{N}\backslash\{1\} : (\forall m \in \mathbb{N}\backslash\{1\})\,(m \nmid n)\}.$$

Then, by fundamental theorem of arithmetic every natural number n can be written down as:

$$n = \prod_{p \in P} p^{\alpha(p)},$$

where $\alpha : P \to \mathbb{N}_0$ denotes the power for each prime number p. For example, 36 can be written as:

$$36 = \prod_{p \in P} p^{\alpha(p)},$$

where $\alpha(2) = 2$, $\alpha(3) = 2$ and $\alpha(p) = 0$ for all $p \in P\backslash\{2, 3\}$.

Theorem. Let G be a group and $a \in G$ such that $\operatorname{ord}(a) = m$. Then,

$$\operatorname{ord}\left(a^k\right) = \frac{\operatorname{lcm}(m, k)}{k} = \frac{m}{\gcd(m, k)}.$$

Proof. Let $q = \operatorname{ord}\left(a^k\right)$. Now, let $g = \gcd(m, k)$. Then, we can take $\left(a^k\right)^{\frac{m}{g}} = a^{k\frac{m}{g}}$. But, g divides both k and m so we can write that down as $\left(a^k\right)^{\frac{m}{g}} = a^{m\frac{k}{g}} = \left(a^m\right)^{\frac{k}{g}} = e$ (because $\frac{k}{g} \in \mathbb{N}$ due to the fact that $g|k$). Now, the order of a^k must divide $\frac{m}{g}$, so we know that $q|\frac{m}{g}$. So there must exist $l \in \mathbb{N}$ such that $\frac{m}{g} = ql$, i.e. $q = \frac{m}{gl}$. We have $\left(a^k\right)^q = e$ so it must be $\left(a^k\right)^{\frac{m}{gl}} = e$. That can be written down as $a^{\frac{mk}{gl}} = e$. Therefore it must be that $m|\frac{mk}{gl}$, i.e. there exists m' such that $\frac{mk}{gl} = mm'$. That is equivalent to $mk = mm'gl$. After dividing by m (which is positive) we have $k = m'gl$. But, from $q = \frac{m}{gl}$ we have $m = qgl$. Let us think about what we have. We have $k = m'gl$ and $m = qgl$. Remember that g is the greatest common divisor of m and k. But, there is one more common divisor and that is l. Therefore, if $l > 1$, greatest common divisor would not be g but gl, contrary to our assumption. Therefore, $l = 1$ and $q = \frac{m}{g}$.

In other words, $\operatorname{ord}\left(a^k\right) = \frac{m}{\gcd(m,k)}$. Of course we can multiply that by $\frac{k}{k}$ and get $\operatorname{ord}\left(a^k\right) = \frac{mk}{k\gcd(m,k)} = \frac{\operatorname{lcm}(m,k)}{k}$, which proves our theorem.

□

Example. We will give an idea for a proof of the next theorem. Suppose $\operatorname{ord}(a) = 12$ and $\operatorname{ord}(b) = 18$ in a group G where a and b commute. Does there exist some $c \in G$ such that $\operatorname{ord}(c) = \operatorname{lcm}(12, 18) = 36$? Well, from a previous theorem, if we take $a^i b^j$ we know that $\operatorname{ord}(a^i) = \frac{12}{\gcd 12,i}$ and $\operatorname{ord}(b^j) = \frac{18}{\gcd 18,j}$. If we could make these two orders relatively prime, we could use a previous lemma to easily multiply these two orders. Well, luckily, greatest common divisor can be easily *controlled* if we pick i to be divisors of 12. Let's see how we can write 12 and 18 down using the fundamental theorem of arithmetic. We have $12 = 2^2 \cdot 3$ and $18 = 2 \cdot 3^2$. If we remove 3 from 12 and remove 2 from 18 we would have two relatively prime numbers, 4 and 9, which multiplied yield 36, least common multiple of 12 and 18. But how to remove 3 from 12? Well, $3|12$ so $\gcd(3, 12) = 3$. Same thing goes for 18 and 2. Looking in the formula above, we can see that it's a most natural thing to choose $i = 3$ and $j = 2$. Then we have $\operatorname{ord}(a^3) = \frac{12}{\gcd 3,12} = \frac{12}{3} = 4$. Similarly we get $\operatorname{ord}(b^2) = \frac{18}{2} = 9$. Their orders are relatively prime. Now, if we're trying to find $\operatorname{ord}(a^3b^2)$, it's easily done by a previous lemma. As orders of factors are relatively prime, the order of the product is product of their orders, i.e. $\operatorname{ord}(a^3b^2) = 9 \cdot 4 = 36$.

Another point we'd like to make is how we should handle the divisors more clearly. Let $m = 2^4 \cdot 3 \cdot 5 \cdot 7$ (order of $a \in G$) and $n = 2^2 \cdot 3 \cdot 5^2$ (order of $b \in G$, which commutes with a). First, we compare the exponents in the prime powers and take all where there is less. Why? Well, least common divisor is $\frac{mn}{\gcd(m,n)}$. And what we're actually doing is that we're dividing greatest common divisor in two parts (by taking common divisors, of course) but so that we get two relatively prime factors. Hence, we will make that experiment now. In m we have 2^4 which is less than 2^2 (so we will take 2^2 from n as it's a common divisor). In m we have 3 and in n we have 3. It does not matter from which we take, we can as well take from n, as we're already taking 2^2. Then, we have 5 in m and 5^2 in n, so we'll take 5 from m. Finally, 7 appears only once in m and never in n, therefore we will leave it alone (it's not a common divisor). Thus we take $i = 5$ and $j = 2^2 3 = 12$. Then, $\operatorname{ord}(a^5) = \frac{m}{\gcd(m,5)} = 2^4 \cdot 3 \cdot 7$. Also, $\operatorname{ord}(b^{12}) = \frac{n}{\gcd(12,n)} = 5^2$. Obviously, $\gcd(\operatorname{ord}(a^5), \operatorname{ord}(b^{12})) = 1$, so $\operatorname{ord}(a^5b^{12}) = 2^4 \cdot 3 \cdot 5^2 \cdot 7$, which is the least common multiple of m and n. That is how we will prove the general statement.

Theorem. Let G be a group and $a, b \in G$ such that $ab = ba$ and $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$. Then there exists $c \in G$ such that $\operatorname{ord}(c) = \operatorname{lcm}(m, n)$.

Proof. Let, by using fundamental theorem of arithmetic,

$$\begin{aligned} m &= \prod_{p\in P} p^{\alpha(p)}, \\ n &= \prod_{p\in P} p^{\beta(p)}. \end{aligned}$$

Then, the greatest common divisor of m and n is:

$$\gcd(m,n) = \prod_{p\in P} p^{\min\{\alpha(p),\beta(p)\}}.$$

We will divide $\gcd(m,n)$ into two separate products. First product will contain all prime powers for which $\alpha(p) \leq \beta(p)$ and the second all the others, namely all prime powers for which $\beta(p) < \alpha(p)$. So we have:

$$\gcd(m,n) = \prod_{\substack{p\in P \\ \alpha(p)\leq\beta(p)}} p^{\min\{\alpha(p),\beta(p)\}} \prod_{\substack{p\in P \\ \alpha(p)>\beta(p)}} p^{\min\{\alpha(p),\beta(p)\}}.$$

But, for all $\alpha(p) \leq \beta(p)$ the minimum of the two is $\alpha(p)$. Similarly, for all $\beta(p) < \alpha(p)$ the minimum is $\beta(p)$. Therefore we can write the products more simply:

$$\gcd(m,n) = \prod_{\substack{p\in P \\ \alpha(p)\leq\beta(p)}} p^{\alpha(p)} \prod_{\substack{p\in P \\ \alpha(p)>\beta(p)}} p^{\beta(p)}.$$

The first product we will denote by i and the second by j, so that we have:

$$\begin{aligned} i &= \prod_{\substack{p\in P \\ \alpha(p)\leq\beta(p)}} p^{\alpha(p)} \\ j &= \prod_{\substack{p\in P \\ \alpha(p)>\beta(p)}} p^{\beta(p)}. \end{aligned}$$

Obviously, $\gcd(m,n) = ij$. That implies (rather trivial but useful) $i|\gcd(m,n)$ and $j|\gcd(m,n)$. Then, as $\gcd(m,n)|m$ and $\gcd(m,n)|n$, then $i|m$ and $j|n$. That also implies that $\gcd(m,i) = i$ and $\gcd(n,j) = j$. Furthermore, $\frac{m}{i} \in \mathbb{N}$ and $\frac{n}{j} \in \mathbb{N}$. Let us show that these two numbers are relatively prime. We have:

$$\frac{m}{i} = \frac{\prod_{p\in P} p^{\alpha(p)}}{\prod_{\substack{p\in P \\ \alpha(p)\leq\beta(p)}} p^{\alpha(p)}}.$$

If $\alpha(p) \leq \beta(p)$ for some p, then obviously $\frac{m}{i}$ will not contain that prime power, as we will have expresion of the form:

$$\frac{f(p)p^{\alpha(p)}}{g(p)p^{\alpha(p)}}.$$

Therefore $\frac{m}{i}$ will contain only $p^{\alpha(p)}$ such that $\beta(p) < \alpha(p)$. But, $\frac{n}{j}$ is:

$$\frac{n}{j} = \frac{\prod_{p \in P} p^{\beta(p)}}{\prod\limits_{\substack{p \in P \\ \beta(p) < \alpha(p)}} p^{\beta(p)}}.$$

So, by similar logic, only $p^{\beta(p)}$ such that $\alpha(p) \geq \beta(p)$ will remain. So if some p were to divide both $\frac{m}{i}$ and $\frac{n}{j}$ then it would have to satisfy both that $\alpha(p) \geq \beta(p)$ and $\beta(p) < \alpha(p)$, which is impossible. Therefore, $\frac{m}{i}$ and $\frac{n}{j}$ are relatively prime.

The final step in the proof is to find $\operatorname{ord}(a^i b^j)$. For that we need $\operatorname{ord}(a^i)$ and $\operatorname{ord}(b^j)$. As $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$, from a previous theorem we have that $\operatorname{ord}(a^i) = \frac{m}{\gcd(m,i)}$ and $\operatorname{ord}(b^j) = \frac{n}{\gcd(n,j)}$. But, we have shown previously in the proof, rather trivially, that $\gcd(m,i) = i$ and $\gcd(n,j) = j$. Thereofore, $\operatorname{ord}(a^i) = \frac{m}{i}$ and $\operatorname{ord}(b^j) = \frac{n}{j}$. The orders of a^i and b^j are relatively prime, so we by a previous problem we have that $\operatorname{ord}(a^i b^j) = \operatorname{ord}(a^i)\operatorname{ord}(b^j)$. That implies that $\operatorname{ord}(a^i b^j) = \frac{mn}{ij} = \frac{mn}{\gcd(m,n)} = \operatorname{lcm}(m,n)$, which concludes our proof.

□

Problem. Let a denote an element of a group G. (i) Let $\operatorname{ord}(a) = 12$. Prove that if a has a cube root, say $a = b^3$ for some $b \in G$, then b has order 36. (ii) Let a have order 6. If a has a fourth root in G, say $a = b^4$, what is the order of b? (iii) Let a have order 10. If a has a sixth root in G, say $a = b^6$, what is the order of b?

Solution. (i) We have that $b^{36} = b^{12 \cdot 3} = (b^3)^{12} = a^{12} = e$. Therefore, as $b^{36} = 3$, by a previous problem order of b must divide 36. So, we have to observe each factor on its own, and we have 1, 2, 3, 4, 6, 9, 12 and 18. If $\operatorname{ord}(b) = 1$ that would mean that $b = e$ and we would have $a = b^3 = e^3 = e$, contradicting that $\operatorname{ord}(a) = 12$. Now, if $\operatorname{ord}(b) = 2$ we have $b^2 = e$. That would mean that $a = b$ and it would mean that $\operatorname{ord}(b) = 12$ and it could not be that $b^2 = e$. Furthermore, if $b^3 = e$, that would again mean that $a = e$, which cannot be. If $\operatorname{ord}(b) = 4$ we would have $b^4 = e$. That would mean that $ab = e$, i.e. $a = b^{-1}$. But, $\operatorname{ord}(b^{-1}) = \operatorname{ord}(b)$ and so $\operatorname{ord}(a) = \operatorname{ord}(b)$ and it cannot be as $12 \neq 4$. If $\operatorname{ord}(b) = 6$, then $e = (b^3)^2 = a^2$, which cannot be as order of a would be 2. Then, $e = b^9 = (b^3)^3 = a^3$ also cannot be as it would imply that $\operatorname{ord}(a) = 3$. Furthermore, if $\operatorname{ord}(b) = 12$ we would have $(b^3)^4 = a^4 = e$ and

from $\text{ord}\,(b) = 18$ would follow $a^6 = e$; both of these cases contradict the fact that $\text{ord}\,(a) = 12$. So, the only possible solution is that $\text{ord}\,(b) = 36$.

(ii) We have $\text{ord}\,(a) = 6$ and $a = b^4$. We want to find $\text{ord}\,(b)$. First time we encounter e is $a^6 = a^5b^4 = (b^4)^5\, b^4 = b^{20}b^4$ and that is $e = b^{24}$. Now, let's again convince ourselves that $b^{24} = e$. We have $b^{24} = (b^4)^6 = a^6 = e$. But, we also need to prove that no divisor of 24 will be order of b. Trivially, we have 1, and that is $b^1 = b = e$ which cannot be as then it would be that $a = e^4 = e$. If $\text{ord}\,(b) = 2$, we would have $a = b^2b^2 = e$. Then, suppose $b^3 = e$. We have $a = bb^3$ and from that $a = b$, which would mean that $\text{ord}\,(a) = \text{ord}\,(b) = 3$ which is a contradiction. Now, if $\text{ord}\,(b) = 4$ we would have $a = b^4 = e$, and again it cannot be as then order of a would be 1. If $\text{ord}\,(b) = 6$ we would have $b^6 = ab^2 = e$, meaning that $a = b^{-2}$. That would mean that $a^3 = b^{-6}$, i.e. $a^3 = (b^{-1})^6$. But $\text{ord}\,(b) = \text{ord}\,(b^{-1}) = 6$, so we have $a^3 = e$, which, again, cannot be. If $\text{ord}\,(b) = 8$ we would have $e = b^8 = (b^4)^2 = a^2$, which is a contradiction. Now, if $\text{ord}\,(b) = 12$, we would have $e = b^{12} = (b^4)^3 = a^3$ and that is impossible as $\text{ord}\,(a) = 6$. Therefore, the least positive power of b which equals e is 24.

(iii) We have $\text{ord}\,(a) = 10$ and $a = b^6$. We will have $e = a^{10} = (b^6)^1\, 0 = b^{60}$. Following the previous examples we will have 1, 2, 3, 4, 5, 6, 10, 12, 15, 20 and 30 as candidates for order of b. Obviously $b^1 = e$ would imply $b^6 = e = a$, not possible. Then, $b^2 = e$ would imply $e = (b^2)^3 = b^6 = a$, not possible; $b^3 = e$ similarly implies $e = (b^3)^2 = b^6 = a$, not possible. Going further, $b^4 = e$ implies $a = b^4b^2 = b^2$ and $a = b^2$. That would mean that $a^3 = b^6 = a$ and from that $a^2 = e$, which is impossible. Then, $b^5 = e$ would give us $a = bb^5 = e$, which is impossible. Following that, $b^6 = e$ directly implies $a = e$, not possible. Then, $b^{10} = e$ yields $a^2 = b^{12} = b^10b^2 = b^2$. That would mean that $(a^2)^3 = (b^2)^3$, which is $a^6 = b^6 = a$ and from that $a^5 = e$. Which is impossible. Then, from $b^{12} = e$ we have $(b^6)^2 = e$, i.e. $a^2 = e$, impossible. Going further, $b^{15} = e$ would imply $(b^6)^2\, b^3 = e$, that is $a^2b^3 = e$. From that we have $a^4b^6 = e$, implying $a^5 = e$, not possible. Then, $e = b^{20} = (b^6)^3\, b^2$ would imply $e = a^3b^2$, which is possible as $e^3 = a^9b^6 = a^{10}$. Finaly, $e = b^{30} = (b^6)^5 = a^5$ is impossible. In conclusion, order of b is either 20 or 60.

Problem. Let a have order n, and suppose a has a k-th root in G, say $a = b^k$.

1. Explain why the order of b is a factor of nk.
2. Let $\text{ord}\,(b) = \frac{nk}{l}$. Prove that n and l are relatively prime.
3. Let k be an integer such that every prime factor of k is a factor of n. Prove that if a has a k-th root b, then $\text{ord}\,(b) = nk$.

Solution. Let a have order n, and suppose a has a k-th root in G, say $a = b^k$.

1. *Explain why the order of b is a factor of nk.* From $a = b^k$, by multiplying equation with a^{n-1} we get $aa^{n-1} = a^{n-1}b^k$ which is $a^n = \left(b^k\right)^{n-1} b^k$, i.e. $a^n = \left(b^k\right)^n$. From that, as $\operatorname{ord}(a) = n$, we have $e = b^{kn}$. Therefore, order of b must divide kn.

2. *Let* $\operatorname{ord}(b) = \frac{nk}{l}$. *Prove that n and l are relatively prime.* From a previous problem we have that order of b must divide nk, i.e. $\frac{nk}{l} | (nk)$. That means that there exists $m \in \mathbb{N}$ such that $nk = m\frac{nk}{l}$, that is $l = m$. Now, suppose that n and l have a factor in common, that is $n = qn'$ and $l = ql'$, where we can take $q = \gcd(n, l)$ and suppose $q > 1$. Notice that n' and l' are now relatively prime. That implies:

$$\operatorname{ord}(b) = \frac{nk}{l} = \frac{qn'k}{ql'} = \frac{n'k}{l'}.$$

Furthermore, as n' and l' are relatively prime, by Euclid's Lemma, it must be that $l' | k$ (we assume that order of b is a natural number, therefore, by canceling out n and l, that property must be preserved). Now, as $\frac{k}{l'} \in \mathbb{N}$, we have:

$$e = b^{\frac{n'k}{l'}} = \left(b^{n'}\right)^{\frac{k}{l'}}$$

and, using the fact that $e = e^{l'}$, we can obtain:

$$e^{l'} = \left(\left(b^{n'}\right)^{\frac{k}{l'}}\right)^{l'} = \left(b^{n'}\right)^k = b^{n'k},$$

that is $e = \left(b^k\right)^{n'}$. Furthermore, from $a = b^k$, it follows that, $a^{n'} = \left(b^k\right)^{n'} = e$, i.e. $a^{n'} = e$. As $\operatorname{ord}(a) = n$, it must be that $n \leq n'$. But, from our assumption that $n = qn'$ and $q > 1$, it must also be that $n > n'$, which is a contradiction, therefore n and l have no factor in common, that is, they are relatively prime.

3. *Let k be an integer such that every prime factor of k is a factor of n. Prove that if a has a k-th root b, then* $\operatorname{ord}(b) = nk$. Suppose that for every $p \in P$ such that $p | k$ it follows that $p | n$. Now, the order of b is $\frac{kn}{l}$ (see the proposition below that summarizes first two problems) and $\gcd(n, l) = 1$. If $p | k$ it must also be that $p | n$. Therefore, it must be that $p \nmid l$. As l then shares no common prime factors with k (or n), and it must divide k, it can only be that $l = 1$.

Proposition. Let G be a group and $a \in G$ such that $\operatorname{ord}(a) = n$. If $a = b^k$, for some $k \in \mathbb{N}$, then $\operatorname{ord}(b) = \frac{nk}{l}$, for some $l \in \mathbb{N}$, such that $\gcd(n, l) = 1$. Furthermore, if $p | k$ implies $p | n$, for all $p \in P$, then $\operatorname{ord}(b) = nk$.

Proof. From the first problem it follows that $\operatorname{ord}(b)$ is a factor of nk, i.e. $\operatorname{ord}(b) | nk$. So there exists $l \in \mathbb{N}$ such that $nk = l\operatorname{ord}(b)$, that is, $\operatorname{ord}(b) = \frac{nk}{l}$. As now we have $\operatorname{ord}(b) = \frac{nk}{l}$ it follows, from the second problem, that $\gcd(n, l) = 1$. From the third problem it follows that $\operatorname{ord}(b) = nk$, if, for all $p \in P$, $p|k$ implies $p|n$.

□

Partitions and equivalence relations

Definition. A **partition** of a set A is a family[39] $\{A_i : \ i \in I\}$ of nonempty subsets of A which are mutually disjoint[40] and whose union[41] is all of A. Subsets A_i from the forementioned family are then called **classes**, and indices are a way of naming them.

Remark. This definition can also be more explicitly defined with two properties (taking all assumptions and namings from the previous definition):

1. If $x \in A_i$ and $x \in A_j$, for some $i, j \in I$, then $A_i = A_j$ (and by that $i = j$).
2. If $x \in A$, then there exists $i \in I$ such that $x \in A_i$.

Definition. A **relation** $\mathcal{R}$ on a set A is a function $\mathcal{R} : A \times A \to \{\top, \bot\}$. If $\mathcal{R}(x, y) = \top$, for some $(x, y) \in A^2$, we write $x\mathcal{R}y$.

Definition. By an **equivalence relation** on a set A we mean a relation $\sim$ which is:

1. *Reflexive:* for every $x \in A$, $x \sim x$.
2. *Symmetric:* for every $x, y \in A$, if $x \sim y$, then $y \sim x$.
3. *Transitive:* for every $x, y, z \in A$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

Definition. Let $\sim$ be an equivalence relation on A and $x \in A$. The set of all the elements equivalent to x is called the **equivalence class** of x, and is denoted by $[x]$. In other words:

$$[x] = \{y \in A : \ y \sim x\}.$$

Lemma. $x \sim y$ if and only if $[x] = [y]$.

Proof. *Necessity.* Suppose $x \sim y$. As $x \sim x$ and $y \sim y$ we have $x \in [x]$ and $y \in [y]$. Then, by symmetry $y \sim x$ and by definition $y \in [x]$. So we have $[y] \subseteq [x]$. Also, as $x \sim y$, we have that $x \in [y]$ and $[x] \subseteq [y]$. From that we have $[x] = [y]$.

Sufficiency. If $[x] = [y]$, then $x \in [x]$ implies $x \in [y]$ and from that $x \sim y$.

□

[39] Family of sets contains a set A_i for each index i as i ranges over $I \subseteq \mathbb{N}$.
[40] That is, $A_i \cap A_j = \emptyset$, for all A_i and A_j, where $i, j \in I$.
[41] In other words, $\bigcup_{i \in I} A_i = A$.

Theorem. If $\sim$ is an equivalence relation on A, the family of all the equivalence classes, that is, $\{[x] : \ x \in A\}$, is a partition of A.

Proof. Obviously, as $[x] = \{y \in A : \ y \sim x\}$, we have that $[x] \subseteq A$. Then, if we take $x \in [y]$ and $x \in [z]$, then we have $x \sim y$ and $x \sim z$. By simmetry $y \sim x$ and $x \sim z$, and by transitivity $y \sim z$, so by a previos lemma $[y] = [z]$. That satisfies the necessity for disjunctivity of classes in definition of partition. Finally, for all $x \in A$ there exists a class such that $x \in [x]$. Therefore, $\{[x] : \ x \in A\}$ is a partition of A.

□

Problem. Prove that (and describe equivalence relation associated with that partition):

1. $\{A_0, \ldots, A_4\}$ is a partition of $\mathbb{Z}$, where $A_r = \{x \in \mathbb{Z} : \ (\exists q \in \mathbb{Z})(x = 5q + r)\}$, for $r \in \{0, \ldots, 4\}$;

2. $\{A_n : \ n \in \mathbb{Z}\}$ is a partition of $\mathbb{Q}$, where $A_n = \{x \in \mathbb{Q} : \ n \leq x < n + 1\}$, for $n \in \mathbb{Z}$;

3. $\{A_r : \ r \in \mathbb{Q}\}$ is a partition of $\mathbb{Z} \times \mathbb{Z}^*$, where[42] $A_r = \{(m, n) \in \mathbb{Z} \times \mathbb{Z}^* : \ \frac{m}{n} = r\}$, for $r \in \mathbb{Q}$;

4. $\{A_0, \ldots, A_0\}$ is a partition of $\mathbb{Z}$, where $A_r = \{x \in \mathbb{Z} : \ (\exists q \in \mathbb{Z})(x = 10q + r)\}$, for $r \in \{0, \ldots, 9\}$;

5. $\{A_r : \ 0 \leq r < 1, \ r \in \mathbb{Q}\}$ is a partition of $\mathbb{Q}$, where

$$A_r = \{x \in \mathbb{Q} : \ (\exists q \in \mathbb{Z})\,(x = q + r)\}\,,$$

   for each $r \in [0, 1\rangle \cap \mathbb{Q}$;

6. $\{A_r : \ r \in \mathbb{R}\}$ is a partition of $\mathbb{R} \times \mathbb{R}$, where $A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ x - y = r\}$, for $r \in \mathbb{R}$;

7. $A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y = 2x + r\}$, for each $r \in \mathbb{R}$, is a partition of $\mathbb{R} \times \mathbb{R}$;

8. $A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ x^2 + y^2 = r^2\}$, for each $r \in \mathbb{R}$, is a partition of $\mathbb{R} \times \mathbb{R}$;

9. $A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y = |x| + r\}$, for each $r \in \mathbb{R}$, is a partition of $\mathbb{R} \times \mathbb{R}$.

Solution.

[42] Let us remind the reader that $\mathbb{Z}^* := \mathbb{Z} \backslash \{0\}$.

1. $\{A_0, \ldots, A_4\}$ *is a partition of* $\mathbb{Z}$*, where* $A_r = \{x \in \mathbb{Z} : (\exists q \in \mathbb{Z})(x = 5q + r)\}$*, for* $r \in \{0, \ldots, 4\}$. Suppose $x \in \mathbb{Z}$. Then, by division with remainder theorem, there exist $q, r \in \mathbb{Z}$ such that $x = 5q + r$ where $0 \leq r < 5$. Therefore, x is in some A_r, for $r \in \{0, \ldots, 4\}$. Suppose $x \in A_{r_1}$ and $x \in A_{r_2}$. Then we have $x = 5q_1 + r_1$ and $x = 5q_2 + r_2$ for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ where $0 \leq r_1, r_2 < 5$. It follows[43] that $5q_1 + r_1 = 5q_2 + r_2$, i.e. $r_1 = 5(q_2 - q_1) + r_2$. But, as $r_2 \geq 0$, for $q_2 - q_1 \geq 1$ we have that $r_1 \geq 5 \cdot 1$, which is impossible, as it has to be $r_1 < 5$. So it must be that $q_2 = q_1$. Then we would have $r_1 = 5 \cdot 0 + r_2 = r_2$. Therefore, as $r_1 = r_2$ we have $A_{r_1} = A_{r_2}$. Thus, $\{A_0, \ldots, A_4\}$ is a partition of $\mathbb{Z}$. Associated equivalence relation is $x \sim y$ if and only if $5|(x - y)$, for all $x, y \in \mathbb{Z}$.

2. $\{A_n : n \in \mathbb{Z}\}$ *is a partition of* $\mathbb{Q}$*, where* $A_n = \{x \in \mathbb{Q} : n \leq x < n + 1\}$*, for* $n \in \mathbb{Z}$. Suppose $x \in \mathbb{Q}$. Then $x = \frac{m}{n}$, where $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. By division with remainder theorem, there exist $q, r \in \mathbb{Z}$ such that $m = nq + r$ where $0 \leq r < n$. So we have $\frac{m}{n} = \frac{nq+r}{n} = \frac{nq}{n} + \frac{r}{n} = q + \frac{r}{n}$. But, as $r < n$, then $\frac{r}{n} < 1$ and we have $\frac{m}{n} = q + \frac{r}{n} < q + 1$. Furthermore, as $r \geq 0$ we have $\frac{m}{n} = q + \frac{r}{n} \geq q + 0 = q$. From $q \in \mathbb{Z}$ and $q \leq x < q + 1$ we have that $x \in A_q$. Let us assume that $x \in A_{n_1}$ and $x \in A_{n_2}$. Then we have $n_1, n_2 \in \mathbb{Z}$ such that $n_1 \leq x < n_1 + 1$ and $n_2 \leq x < n_2 + 1$. Furthermore, assume that $n_1 \leq n_2$. Then we have $n_2 \leq x < n_1 + 1$. From that we have $n_2 < n_1 + 1$ and $n_1 \leq n_2 < n_1 + 1$. The only integer between n_1 and $n_1 + 1$ that is greater or equal to n_1 is of course n_1. Therefore, $n_1 = n_2$ and that implies $A_{n_1} = A_{n_2}$. Here, equivalence relation is $x \sim y$ if and only if there exists $n \in \mathbb{Z}$ such that $n \leq x < n + 1$ and $n \leq y < n + 1$, for all $x, y \in Q$.

3. $\{A_r : r \in \mathbb{Q}\}$ *is a partition of* $\mathbb{Z} \times \mathbb{Z}^*$*, where* $A_r = \{(m, n) \in \mathbb{Z} \times \mathbb{Z}^* : \frac{m}{n} = r\}$*, for* $r \in \mathbb{Q}$. Suppose $x \in \mathbb{Z} \times \mathbb{Z}^*$. Then $x = (a, b)$, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^*$. Then there exists $r = \frac{a}{b}$ and that implies $x \in A_r$. Let us assume that $(a, b) \in A_{r_1}$ and $(a, b) \in A_{r_2}$. Then we have $r_1 = \frac{a}{b}$ and $r_2 = \frac{a}{b}$. That implies $r_1 = r_2$, i.e. $A_{r_1} = A_{r_2}$. The associated equivalence relation is $(a, b) \sim (c, d)$ if and only if $\frac{a}{b} = \frac{c}{d}$, for all $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ and $(c, d) \in \mathbb{Z} \times \mathbb{Z}^*$.

4. $\{A_0, \ldots, A_0\}$ *is a partition of* $\mathbb{Z}$*, where* $A_r = \{x \in \mathbb{Z} : (\exists q \in \mathbb{Z})(x = 10q + r)\}$*, for* $r \in \{0, \ldots, 9\}$. By division with remainder theorem for each $x \in \mathbb{Z}$ there exist unique $q, r \in \mathbb{Z}$ such that $x = 10q + r$, where $0 \leq r < 10$. Therefore, as in the first example, $x \in \mathbb{Z}$ will imply $x \in A_r$ (where r is obtained by using division with remainder theorem; which in turn guarantees its existence) and $x \in A_{r_1}$ with $x \in A_{r_2}$ will imply $A_{r_1} = A_{r_2}$ (due to uniqueness of q and r in division with remainder theorem). Associated equivalence relation is $x \sim y$ if and only if $10|(x - y)$, for all $x, y \in \mathbb{Z}$.

[43] Here we are actually proving again uniqueness part of division with remainder theorem, but for a special case, for dividing with 5; see my works on number theory. It's rather redundant but good for excercise.

5. $\{A_r :\ 0 \leq r < 1,\ r \in \mathbb{Q}\}$ *is a partition of* $\mathbb{Q}$*, where*

$$A_r = \{x \in \mathbb{Q} :\ (\exists q \in \mathbb{Z})\,(x = q + r)\}\,,$$

for each $r \in [0,1\rangle \cap \mathbb{Q}$. By a corollary of division with remainder theorem, proved in my works on number theory, for any $x \in \mathbb{Q}$ there exist $q \in \mathbb{Z}$, $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$ such that $x = q + \frac{m}{n}$ where $0 \leq m < n$. Dividing those two inequalities by $n \neq 0$ gives us $0 \leq \frac{m}{n} < 1$. Therefore taking $r = \frac{m}{n}$ implies $x \in A_r$. Also, if we took $x \in A_{r_1}$ and $x \in A_{r_2}$, by the uniqueness part of the same corollary, we would have $A_{r_1} = A_{r_2}$ (as $x = k_1 + r_1$ and $x = k_2 + r_2$ implies $k_1 = k_2$ and $r_1 = r_2$, because $0 \leq r_1, r_2 < 1$; explained in more detail in the proof in my works on elementary number theory). Here, equivalence relation is $x \sim y$ if and only if there exist $q_1, q_2 \in \mathbb{Z}$ and $r \in \mathbb{Q}$ such that $x = q_1 + r$ and $y = q_2 + r$, where $0 \leq r < 1$ and $x, y \in Q$.

6. $\{A_r :\ r \in \mathbb{R}\}$ *is a partition of* $\mathbb{R}\times\mathbb{R}$*, where* $A_r = \{(x,y) \in \mathbb{R}\times\mathbb{R} :\ x - y = r\}$*, for* $r \in \mathbb{R}$. Take $(x,y) \in \mathbb{R}$. Then there exists $r \in \mathbb{R}$ such that $x - y = r$, therefore, $(x,y) \in A_r$. Also, suppose $(x,y) \in A_{r_1}$ and $(x,y) \in A_{r_2}$. Then, $r_1 = x - y$ and $r_2 = x - y$ implies $r_1 = r_2$, id est $A_{r_1} = A_{r_2}$. Equivalence relation associated with this partition is, for all $(x,y), (z,w) \in \mathbb{R} \times \mathbb{R}$, $(x,y) \sim (z,w)$ if and only if $x - y = z - w$.

7. $A_r = \{(x,y) \in \mathbb{R} \times \mathbb{R} :\ y = 2x + r\}$*, for each* $r \in \mathbb{R}$*, is a partition of* $\mathbb{R} \times \mathbb{R}$. If we take $(x,y) \in \mathbb{R} \times \mathbb{R}$, then there exists $r \in \mathbb{R}$ such that $y = 2x + r$ obtained with $r = y - 2x$ and then $(x,y) \in A_r$. For $(x,y) \in A_{r_1}$ and $(x,y) \in A_{r_2}$ we have $y = 2x + r_1$ and $y = 2x + r_2$. From that we have $2x + r_1 = 2x + r_2$ which in turn implies, after subtracting $2x$, that $r_1 = r_2$ and $A_{r_1} = A_{r_2}$. We have $(x,y) \sim (z,w)$ if and only if $y - 2x = w - 2z$. Geometrically, this is the partition of Euclidean space as parallel lines.

8. $A_r = \{(x,y) \in \mathbb{R} \times \mathbb{R} :\ x^2 + y^2 = r^2\}$*, for each* $r \in \mathbb{R}$*, is a partition of* $\mathbb{R} \times \mathbb{R}$. Take $(x,y) \in \mathbb{R} \times \mathbb{R}$. Then we have $r = \sqrt{x^2 + y^2}$ and $(x,y) \in A_r$, where r is obtained as shown. If we take $(x,y) \in A_{r_1}$ and $(x,y) \in A_{r_2}$, we have $x^2 + y^2 = r_1^2$ and $x^2 + y^2 = r_2^2$. That implies $r_1^2 = r_2^2$. But, $r_1, r_2 \geq 0$, so from that we have $r_1 = r_2$ and $A_{r_1} = A_{r_2}$. Equivalence relation is $(x,y) \sim (z,w)$ if and only if $x^2 + y^2 = z^2 + w^2$. Geometrically, this equivalence relation partitions Euclidean space into circles sharing the same center.

9. $A_r = \{(x,y) \in \mathbb{R} \times \mathbb{R} :\ y = |x| + r\}$*, for each* $r \in \mathbb{R}$*, is a partition of* $\mathbb{R} \times \mathbb{R}$. If we take $(x,y) \in \mathbb{R}\times\mathbb{R}$ we have $r = y - |x|$ and by that $(x,y) \in A_r$. Furthermore, if $(x,y) \in A_{r_1}$ and $(z,w) \in A_{r_2}$, we have $y - |x| = r_1$ and $y - |x| = r_2$ from which

trivially follows that $r_1 = r_2$. Equivalence relation is $(x, y) \sim (z, w)$ if and only if $y - |x| = w - |z|$. Geometrically, this is the partition of Euclidean space as graphs of absolute value function.

Problem. Prove each of the following is an equivalence relation on the indicated set. Then describe the partition associated with that equivalence relation.

1. In $\mathbb{Z}$, $m \sim n$ iff $|m| = |n|$;
2. In $\mathbb{Q}$, $r \sim s$ iff $r - s \in \mathbb{Z}$;
3. Let $\lceil x \rceil$ denote the greatest integer less than or equal to x. In $\mathbb{R}$, let $a \sim b$ iff $\lceil a \rceil = \lceil b \rceil$;
4. In $\mathbb{Z}$, let $m \sim n$ iff $m - n$ is a multiple of 10;
5. In $\mathbb{R}$, let $a \sim b$ iff $a - b \in \mathbb{Q}$;
6. In $\mathcal{F}(\mathbb{R})$, let $f \sim g$ iff $f(0) = g(0)$;
7. In $\mathcal{F}(\mathbb{R})$, let $f \sim g$ iff $f(x) = g(x)$ for all $x > c$, where c is some fixed real number;
8. If C is any set, $\mathcal{P}(C)$ denotes the set of all the subsets of C. Let $D \subseteq C$. In $\mathcal{P}(C)$, let $A \sim B$ iff $A \cap D = B \cap D$;
9. In $\mathbb{R} \times \mathbb{R}$, let $(a, b) \sim (c, d)$ iff $a^2 + b^2 = c^2 + d^2$;
10. In $\mathbb{R}^*$, let $a \sim b$ iff $\frac{a}{b} \in \mathbb{Q}$;
11. In $\mathbb{R} \times \mathbb{R}$, $(x, y) \sim (u, v)$ iff $ax^2 + by^2 = au^2 + bv^2$ (where $a, b > 0$);
12. In $\mathbb{R} \times \mathbb{R}$, $(x, y) \sim (u, v)$ iff $x + y = u + v$;
13. In $\mathbb{R} \times \mathbb{R}$, $(x, y) \sim (u, v)$ iff $x^2 - y = u^2 - v$.

Solution.

1. *In $\mathbb{Z}$, $m \sim n$ iff $|m| = |n|$. Reflexivity.* $m \sim n$ holds as $|m| = |m|$. *Symmetry.* $m \sim n$ implies $|m| = |n|$ and $|n| = |m|$ implies $n \sim n$. *Transitivity.* If $m \sim n$ and $n \sim p$ then we have $|m| = |n|$ and $|n| = |p|$, i.e. $|m| = |n| = |p|$ which implies $|m| = |p|$ and $m \sim p$. We have $A_m = [m] = \{n \in \mathbb{Z} : \ n \sim m\} = \{n \in \mathbb{Z} : \ |n| = |m|\}$. As $A_m = A_{-m}$ we can only consider family $\{A_m : \ m \in \mathbb{N}_0\}$ as partition.
2. *In $\mathbb{Q}$, $r \sim s$ iff $r - s \in \mathbb{Z}$. Reflexivity.* $r \sim r$ is true as $r - r = 0 \in \mathbb{Z}$. *Symmetry.* $r \sim s$ implies $r - s \in \mathbb{Z}$. And, if $r - s \in \mathbb{Z}$ then $s - r = -(r - s) \in \mathbb{Z}$, so $s \sim r$. *Transitivity.* If $r \sim s$ and $s \sim t$, then $r - s \in \mathbb{Z}$ and $s - t \in \mathbb{Z}$. But, $(r - s) + (s - t) \in \mathbb{Z}$, that is $r - t \in \mathbb{Z}$, i.e. $r \sim t$. We have $A_r = [r] = \{x \in \mathbb{Q} : x - r \in \mathbb{Z}\}$. Partition is the family $\{A_r : \ r \in \mathbb{Q}\}$.

3. *Let* $\lceil x \rceil$ *denote the greatest integer less than or equal to* x. *In* $\mathbb{R}$, *let* $a \sim b$ *iff* $\lceil a \rceil = \lceil b \rceil$. Due to equality ("=") being reflexive, transitive and symmetric, so is $\sim$. Partition is the family $\{A_r : \ r \in \mathbb{Z}\}$ where $A_r = \{x \in \mathbb{R} : \ \lceil x \rceil = r\}$.

4. *In* $\mathbb{Z}$, *let* $m \sim n$ *iff* $m - n$ *is a multiple of* 10. *Reflexivity.* $m \sim m$ as $10|0$, i.e. $10|m - m$. *Symmetry.* $m \sim n$ implies $10|m - n$, i.e. there exists $q \in \mathbb{Z}$ such that $m - n = 10q$. Taking $q' = -q$ we have $m - n = -10q'$, from that $n - m = 10q'$ which in turn implies $10|n - m$ and $n \sim m$. *Transitivity.* If $m \sim n$ and $n \sim p$ then there exist $q, r \in \mathbb{Z}$ such that $m - n = 10q$ and $n - p = 10r$. Taking the sum we have $m - n + n - p = 10q + 10r$, id est $m - p = 10(q + r)$, which means that $m \sim p$. If we take $A_m = [m] = \{n \in \mathbb{Z} : \ 10|m - n\}$ we get a partition $\{A_m : \ m \in \mathbb{Z}\}$.

5. *In* $\mathbb{R}$, *let* $a \sim b$ *iff* $a - b \in \mathbb{Q}$. *Reflexivity.* We have $a \sim a$ as $0 = a - a \in \mathbb{Q}$. *Symmetry.* $a \sim b$ implies $a - b \in Q$, but so is $b - a = -(a - b) \in \mathbb{Q}$ and $b \sim a$. *Transitivity.* $a \sim b$ and $b \sim c$ imply $a - b \in \mathbb{Q}$ and $b - c \in \mathbb{Q}$; their sum is also in $\mathbb{Q}$ and we have $a - c \in \mathbb{Q}$, i.e. $a \sim c$. Partition is the family $\{A_r : \ r \in \mathbb{R}\}$, where $A_r = [r] = \{p \in \mathbb{R} : \ r - p \in \mathbb{Q}\}$.

6. *In* $\mathcal{F}(\mathbb{R})$, *let* $f \sim g$ *iff* $f(0) = g(0)$. Reflexivity, symmetry and transitivity hold due to the same properties being shared with equality ("="). Partition is the family $\{A_r : \ r \in \mathbb{R}\}$, where $A_r = \{g \in \mathcal{F}(\mathbb{R}) : \ f(0) = r\}$.

7. *In* $\mathcal{F}(\mathbb{R})$, *let* $f \sim g$ *iff* $f(x) = g(x)$ *for all* $x > c$, *where* c *is some fixed real number.* Let $c \in \mathbb{R}$. *Reflexivity.* Trivial, as $f(x) = f(x)$, for all $x > c$. *Symmetry.* If $f \sim g$ then $f(x) = g(x)$, for all $x > c$ and due to symmetry of equality we have $g(x) = f(x)$ and $g \sim f$. *Transitivity.* $g \sim f$ and $f \sim h$ imply $g(x) = f(x)$ and $f(x) = h(x)$, for all $x > c$ and that means that $g(x) = h(x)$, for all $x > c$. Partition is the family $\{A_f : \ f \in \mathcal{F}(\mathbb{R})\}$, where $A_f = [f] = \{g \in \mathcal{F}(\mathbb{R}) : \ (\forall x > c)(f(x) = g(x))\}$, where $c \in \mathbb{R}$.

8. *If* C *is any set,* $\mathcal{P}(C)$ *denotes the set of all the subsets of* C. *Let* $D \subseteq C$. *In* $\mathcal{P}(C)$, *let* $A \sim B$ *iff* $A \cap D = B \cap D$. *Reflexivity.* $A \sim A$ as $A \cap D = A \cap D$. *Symmetry.* $A \sim B$ implies $A \cap D = B \cap D$, that is $B \cap D = A \cap D$ which means $B \sim A$. *Transitivity.* $A \sim B$ and $B \sim C$ imply $A \cap D = B \cap D$ and $B \cap D = C \cap D$. Combined, we get $A \cap D = C \cap D$, i.e. $A \sim C$. Partition is the family $\{A_C : \ C \in \mathcal{P}_C\}$ where $A_C = \{X \in \mathcal{P}(C) : \ A \cap D = X \cap D\}$ and $D \subseteq C$.

9. *In* $\mathbb{R} \times \mathbb{R}$, *let* $(a, b) \sim (c, d)$ *iff* $a^2 + b^2 = c^2 + d^2$. Reflexivity, symmetry and transitivity hold due to the same property being shared with equality ("="). Partition is the family $\{A_{(a,b)} : \ (a, b) \in \mathbb{R} \times \mathbb{R}\}$ where $A_{(a,b)} = [(a, b)] = \{(c, d) \in \mathbb{R} \times \mathbb{R} : \ a^2 + b^2 = c^2 + d^2\}$.

10. *In* $\mathbb{R}^*$*, let* $a \sim b$ *iff* $\frac{a}{b} \in \mathbb{Q}$*. Reflexivity.* $a \sim a$ holds as $1 = \frac{a}{a} \in \mathbb{Q}$. *Symmetry.* $a \sim b$ implies $\frac{a}{b} \in \mathbb{Q}$, but so is $\frac{b}{a} \in \mathbb{Q}$ (note that $a, b \neq 0$ as $a, b \in \mathbb{R}^*$ and $\mathbb{Q}^*$ is a group and therefore closed with respect to inverses) and $b \sim a$. *Transitivity.* $a \sim b$ and $b \sim c$ impliy that $\frac{a}{b} \in \mathbb{Q}$ and $\frac{b}{c} \in \mathbb{Q}$. Multiplying those two numbers gets us $\frac{a}{b}\frac{b}{c} = \frac{a}{c} \in \mathbb{Q}$ ($\mathbb{Q}^*$ is closed with respect to multiplication). Partition is the family $\{A_r : \ r \in \mathbb{R}^*\}$, where $A_r = [r] = \{p \in \mathbb{R}^* : \ \frac{r}{p} \in \mathbb{Q}\}$.

11. *In* $\mathbb{R} \times \mathbb{R}$*,* $(x, y) \sim (u, v)$ *iff* $ax^2 + by^2 = au^2 + bv^2$ *(where* $a, b > 0$*).* Reflexivity, symmetry and transitivity all hold due to the fact that equality defines the relation. Partition associated with it is $\{A_r : \ r \in \mathbb{R}_0^+\}$ where $A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : ax^2 + by^2 = r\}$. Geometrically, it partitions Euclidean space into elypses.

12. *In* $\mathbb{R} \times \mathbb{R}$*,* $(x, y) \sim (u, v)$ *iff* $x + y = u + v$*.* Again, reflexivity, symmetry and transitivity follow trivially. The partition is $\{A_r : \ r \in \mathbb{R}\}$ such that $A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y = r - x\}$. It partitions Euclidean space into parallel lines.

13. *In* $\mathbb{R} \times \mathbb{R}$*,* $(x, y) \sim (u, v)$ *iff* $x^2 - y = u^2 - v$*.* Reflexivity, symmetry and transitivity hold due to equality in definition. Partition is $\{A_r : \ r \in \mathbb{R}\}$ where $A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 = y + r\}$. This is the partition of Euclidean space into parabolas.

Problem. Let G be a group. In each of the following, a relation on G is defined. Prove it is an equivalence relation. Then describe the equivalence class of e.

1. If H is a subgroup of G, let $a \sim b$ iff $ab^{-1} \in H$;
2. If H is a subgroup of G, let $a \sim b$ iff $a^{-1}b \in H$;
3. Let $a \sim b$ iff there is an $x \in G$ such that $a = xbx^{-1}$;
4. Let $a \sim b$ iff there is an integer k such that $a^k = b^k$;
5. Let $a \sim b$ iff ab^{-1} commutes with every $x \in G$;
6. Let $a \sim b$ iff ab^{-1} is a power of c (where c is a fixed element of G).

Solution.

1. *If* H *is a subgroup of* G*, let* $a \sim b$ *iff* $ab^{-1} \in H$*. Reflexivity.* $a \sim a$ as $aa^{-1} = e \in H$. *Symmetry.* $a \sim b$ implies $ab^{-1} \in H$, but as H is closed with respect to multiplication then $a \in H$ and $b^{-1} \in H$. As H is closed with respect to inverses and multiplication we have $ba^{-1} \in H$ which implies $b \sim a$. *Transitivity.* If $a \sim b$ and $b \sim c$ then $ab^{-1} \in H$ and $bc^{-1} \in H$. Multiplying those two elements gives us $ab^{-1}bc^{-1} = ac^{-1} \in H$, due to H being closed with respect to multiplication. Finally, $[e] = \{x \in G : \ x \sim e\} = \{x \in G : \ xe^{-1} \in H\} = \{x \in G : \ x \in H\} = H$.

2. *If H is a subgroup of G, let $a \sim b$ iff $a^{-1}b \in H$.* Reflexivity, symmetry and transitivity follow similarly as in the previous example. Also, $[e] = H$. This is actually the same equivalence relation as in the previous example as $a^{-1}b \in H$ will imply that $ab^{-1} \in H$ and reverse.

3. *Let $a \sim b$ iff there is an $x \in G$ such that $a = xbx^{-1}$. Reflexivity.* $a \sim a$ holds because $a = aaa^{-1}$. *Symmetry.* From $a \sim b$ follows that $a = xbx^{-1}$. Multiplying by x on the right and x^{-1} on the left gives us $x^{-1}ax = b$ which implies $b \sim a$ (maybe it's a little bit unclear but taking $y = x^{-1} \in G$ would clarify our conclusion on a more symbolical level). *Transitivity.* If $a \sim b$ and $b \sim c$ then $a = xbx^{-1}$ and $b = xcx^{-1}$ which gives us $a = xxcx^{-1}x^{-1}$ and that is $a = x^2c\left(x^2\right)^{-1}$. As $x^2, x^{-2} \in G$, then $a \sim c$. We have $[e] = \{y \in G : \ (\exists x \in G)(e = xyx^{-1})\} = \{y \in G : \ (\exists x \in G)(x = xy)\} = \{y \in G : \ e = y\} = \{e\}$.

4. *Let $a \sim b$ iff there is an integer k such that $a^k = b^k$. Reflexivity.* $a \sim a$ because $a^k = a^k$. *Symmetry.* $a \sim b$ implies that there exists $k \in \mathbb{Z}$ such that $a^k = b^k$. Simply taking $b^k = a^k$ gives us $b \sim a$. *Transitivity.* $a \sim b$ and $b \sim c$ implies $a^k = b^k$ and $b^k = c^k$, i.e. $a^k = c^k$ and $a \sim c$. Equivalence class of e is $[e] = \{x \in G : \ (\exists k \in \mathbb{Z})(x^k = e^k)\} = \{x \in G : \ (\exists k \in \mathbb{Z})(x^k = e)\} = \{x \in G : \ \mathrm{ord}\,(x) < \infty\}$.

5. *Let $a \sim b$ iff ab^{-1} commutes with every $x \in G$.* If ab^{-1} commutes with every $x \in G$, then ab^{-1} is in the center C of group G. So we could have said $a \sim b$ iff ab^{-1} is in center C of group G. And, as C is a subgroup of G, from first example we have that $\sim$ is an equivalence relation. Also $[e] = \{y \in G : \ (\forall x \in G)(xye^{-1} = ye^{-1}x)\} = \{y \in G : \ (\forall x \in G)(xy = yx)\} = C$.

6. *Let $a \sim b$ iff ab^{-1} is a power of c (where c is a fixed element of G).* Let $c \in G$. *Reflexivity.* We have $a \sim a$ as $aa{-}1 = e = c^0$. *Symmetry.* We have $a \sim b$ and from that $ab^{-1} = c^k$, for some $k \in G$. Multiplying by c^{-k} on the right gives us $\left(ab^{-1}\right)c^{-k} = e$. Multiplying by $\left(ab^{-1}\right)^{-1} = ba^{-1}$ on the left gives $c^{-k} = ba^{-1}$ and that implies $b \sim a$. *Transitivity.* From $a \sim b$ and $b \sim d$ follows that $ab^{-1} = c^k$ and $bd^{-1} = c^l$. Multiplying first equation by c^l on the right gives us $\left(ab^{-1}\right)c^l = c^kc^l$. That is equivalent to $ab^{-1}bd^{-1} = c^{k+l}$, i.e. $ad^{-1} = c^{k+l}$, which means that $a \sim d$. For $c \in G$ we have $[e] = \{y \in G : \ (\exists k \in \mathbb{Z})(ye^{-1} = c^k)\} = \{y \in G : \ (\exists k \in \mathbb{Z})(y = c^k)\}$, i.e. all elements whose k-th root is c.

Proposition. Let $\{A_i : \ i \in I\}$ be a partition of A and $\{B_j : \ j \in J\}$ a partition of B. Then, $\{A_i \times B_j : \ (i,j) \in I \times J\}$ is a partition of $A \times B$. Furthermore, if $\sim_I$ and $\sim_J$ are equivalence relations corresponding to partitions of A and B, respectively, then equivalence relation $\sim$ corresponding to $A \times B$ is $(a_1, b_1) \sim (a_2, b_2)$ if and only if $a_1 \sim_I a_2$ and $b_1 \sim_J b_2$.

Proof. If we take $(a, b) \in A \times B$ then $a \in A$ and $b \in B$. But, as we have partitions of A and B, as defined, there exist $i \in I$ and $j \in J$ such that $a \in A_i$ and $b \in B_j$, that is $(a, b) \in A_i \times B_j$. If we take $(a, b) \in A_i \times B_j$ and $(a, b) \in A_k \times B_l$ then we have $a \in A_i$ and $b \in B_j$, and $a \in A_k$ and $b \in B_l$. But, $a \in A_i$ and $a \in A_k$ implies that $A_i = A_k$, and $b \in B_j$ with $b \in B_l$ implies $B_j = B_l$, so we have $A_i \times B_j = A_k \times B_l$.

Let $\sim_I$ and $\sim_J$ be equivalence relations as defined. First we will show that $\sim$ is an equivalence relation. *Reflexivity.* $(a, b) \sim (a, b)$ is true as $a \sim_I a$ and $b \sim_J b$. *Symmetry.* $(a_1, b_1) \sim (a_2, b_2)$ implies $a_1 \sim_I a_2$ and $b_1 \sim_J b_2$. As $\sim_I$ and $\sim_J$ are equivalence relations, and are therefore symmetric, we have $a_2 \sim_I a_1$ and $b_2 \sim_J b_1$, which in turn implies $(a_2, b_2) \sim (a_1, b_1)$. *Transitivity.* If $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$ then we have $a_1 \sim_I a_2$ and $b_1 \sim_J b_2$ with $a_2 \sim_I a_3$ and $b_2 \sim_J b_3$. As $\sim_I$ and $\sim_J$ are transitive, we have $a_1 \sim_I a_3$ and $b_1 \sim_J b_3$, that is, $(a_1, b_1) \sim (a_3, b_3)$. Now, if $[a_i]_I = A_i$ and $[b_i]_J = A_j$, then $A_i \times B_j = [(a_i, b_j)] = \{(x, y) \in A \times B : (x, y) \sim (a_i, b_j)\} = \{(x, y) \in A \times B : (x \sim_I a_i) \wedge (y \sim_J b_j)\} = \{(x, y) \in A \times B : (x \in [a_i]_I) \wedge (y \in [b_j]_J)\} = [a_i]_I \times [b_j]_J$.

□

Proposition. Let $f : A \to B$ be a function and $\sim$ a relation such that, for all $a_1, a_2 \in A$, $a_1 \sim a_2$ if and only if $f(a_1) = f(a_2)$. Then, $\sim$ is an equivalence relation on A.

Proof. *Reflexivity.* $a \sim a$ as $f(a) = f(a)$. *Simmetry.* $a_1 \sim a_2$ implies $f(a_1) = f(a_2)$, i.e. $f(a_2) = f(a_1)$ and that is $a_2 \sim a_1$. *Transitivity.* If $a_1 \sim a_2$ and $a_2 \sim a_3$ then $f(a_1) = f(a_2)$ and $f(a_2) = f(a_3)$, which combined yields $f(a_1) = f(a_3)$, id est $f(a_1) = f(a_3)$.

□

Proposition. Let $f : A \to B$ be a function, and let $\{B_i : i \in I\}$ be a partition of B. Then[44] $\{f^{-1}(B_i) : i \in I\}$ is a partition of A.

Proof. If $a \in A$ then there exists $b \in B$ such that $b = f(a)$, i.e. $f(a) \in B$. As B has a forementioned partition, then there exists $i \in I$ such that $f(a) \in B_i$. As $a \in A$ implies $f(a) \in B_i$ then $a \in \{x \in A : f(x) \in B_i\}$, i.e. $a \in f^{-1}(B_i)$. Then, if $a \in f^{-1}(B_i)$ and $a \in f^{-1}(B_j)$, then there exists $b \in B_i$ and $b \in B_j$ such that $b = f(a)$. As B_i and B_j are sets in the partition of B, $b \in B_i$ and $b \in B_j$ implies $B_i = B_j$ and that further implies $f^{-1}(B_i) = f^{-1}(B_j)$. Therefore, $\{f^{-1}(B_i) : i \in I\}$ is a partition of A.

□

[44]Keep in mind that, for $f : A \to B$, and any $C \subseteq B$, we define $f^{-1}(C) = \{x \in A : f(x) \in C\}$.

Proposition. Let $\sim_1$ and $\sim_2$ be distinct equivalence relations on A. Define $\sim_3$ by $a \sim_3 b$ if and only if $a \sim_1 b$ and $a \sim_2 b$. Then, $\sim_3$ is an equivalence relation of A. Furthermore, let $[x]_i$ denote the equivalence class of x for $\sim_i$ (where $i \in \{1, 2, 3\}$). Then, $[x]_3 = [x]_1 \cap [x]_2$.

Proof. *Reflexivity.* $a \sim_3 a$ holds as $a \sim_1 a$ and $a \sim_2 a$. *Symmetry.* $a \sim_3 b$ implies that $a \sim_1 b$ and $a \sim_2 b$. But, $\sim_1$ and $\sim_2$ are equivalence relations, so $a \sim_1 b$ and $a \sim_2 b$ imply $b \sim_1 a$ and $b \sim_2 a$ and from that follows that $b \sim_3 a$. *Transitivity.* If $a \sim_3 b$ and $b \sim_3 c$ we have $a \sim_1 b$ and $a \sim_2 b$ with $b \sim_1 c$ and $b \sim_2 c$. Again, as $\sim_1$ and $\sim_2$ are transitive, we have $a \sim_1 c$ and $a \sim_2 c$ which implies $a \sim_3 c$. If we take $a \in [x]_3$, then $a \sim_3 x$. That implies that $a \sim_1 x$ and $a \sim 2x$, i.e. $a \in [x]_1$ and $a \in [x]_2$. As $a \in [x]_3$ implies $a \in [x]_1$ and $a \in [x]_2$, then by definition of intersection, $[x]_3 = [x]_1 \cap [x]_2$.

□

Cyclic groups

Definition. Let G be a group and $a \in G$. Then, $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ is called a **cyclic group**.

Lemma. Let G be a group and $a \in G$. Then, $a^k \in G$, for all $k \in \mathbb{Z}$.

Proof. Let $k > 0$. If we take $k = 1$, we have $a^1 = a \in G$. Suppose $a^k \in G$. Then, $a^{k+1} = a^k a$. As $a^k \in G$ by assumption and $a \in G$, then their product is in G. Therefore, $a^{k+1} \in G$. If $k = 0$ we have $a^0 = e$ by definition and $e \in G$. If $k < 0$, we can take $l = -k$. So $l > 0$ and we have $a^k = a^{-l} = (a^{-1})^l$. As $a^{-1} \in G$ and $l > 0$, by the first part of the proof we have $a^{-l} \in G$, i.e. $a^k \in G$, for all $k \in \mathbb{Z}$.

□

Proposition. Let G be a group and $a \in G$. Then, $\langle a \rangle$ is a subgroup of G.

Proof. Let $a^k \in \langle a \rangle$. By a previous lemma, we have $a^k \in G$, so $\langle a \rangle \subseteq G$. If we take $a^k, a^l \in \langle a \rangle$, we have $a^k a^l = a^{k+l}$ and $a^{k+l} \in \langle a \rangle$. Also, $a^k a^{-k} = a^{k-k} = a^0 = e$ and $a^{-k} \in \langle a \rangle$. Therefore, as $\langle a \rangle$ is a subset of G and is closed with respect to products and inverses, it is a subgroup of G.

□

Proposition. Let G be a group and $a \in G$. Then, $|\langle a \rangle| = \operatorname{ord}(a)$.

Proof. Let $A = \left\{a^k : k \in [0, \ldots, \operatorname{ord}(a) - 1] \cap \mathbb{Z}\right\}$. By a previous proposition all powers of a are different, i.e. if $k \neq l$, then $a^k \neq a^l$. Therefore, $|A| = \operatorname{ord}(a)$. Now, we will show that $A = \langle a \rangle$. If we take $a^k \in A$, where $0 \leq k < \operatorname{ord}(a)$, as also $k \in \mathbb{Z}$, we have $a^k \in \langle a \rangle$. So, $A \subseteq \langle a \rangle$. Then, we take $a^k \in \langle a \rangle$. By division with remainder theorem we have that there exist $q, r \in \mathbb{Z}$ such that $k = q\operatorname{ord}(a) + r$, where $0 \leq r < |\operatorname{ord}(a)| = \operatorname{ord}(a)$. So, $a^k = a^{q\operatorname{ord}(a)+r}$, i.e. $a^k = \left(a^{\operatorname{ord}(a)}\right)^q a^r = e^q a^r = e a^r = a^r$. As $r \in [0, \ldots, \operatorname{ord}(a) - 1] \cap \mathbb{Z}$, we have $a^r \in A$. But, $a^r = a^k$, so $a^k \in A$ and $\langle a \rangle \subseteq A$. That implies $\langle a \rangle = A$ and $|\langle a \rangle| = |A|$, i.e. $|\langle a \rangle| = \operatorname{ord}(a)$.

□

Definition. Let $n \in \mathbb{N}$. For all $a, b \in \mathbb{Z}$, let $a \sim_n b$ if and only if $a \equiv b \pmod{n}$.

Proposition. $\sim_n$ is an equivalence relation.

Proof. Follows directly from the fact (proved in my other script) that congruence is an equivalence relation on $\mathbb{Z}$.

□

Definition. Let $n \in \mathbb{N}$. We define equivalence class for each $a \in \mathbb{Z}$ so that $[a]_n = \{b \in \mathbb{Z} : \ a \sim_n b\}$. Let $\mathbb{Z}_n = \{[a]_n : \ a \in \mathbb{Z}\}$ be a family of all equivalence classes for $\sim_n$.

Proposition. $|\mathbb{Z}_n| = n$.

Proof. Let $\mathcal{Z} = \{[a]_n : \ a \in [0, \ldots, n-1] \cap \mathbb{Z}\}$. Let $[a]_n, [b]_n \in \mathcal{Z}$, with $a \neq b$. Then, $0 \leq a, b < n$. Assume $[a]_n = [b]_n$. From that follows that $a \sim_n b$, i.e. $a \equiv b \pmod{n}$. As $0 \leq a, b < n$, from a proposition discussed in my number theory script, we have $a = b$, which is a contradiction. Therefore, for $a \neq b$ we have $[a]_n \neq [b]_n$. Therefore, $|\mathcal{Z}| = n$. Obviously $\mathcal{Z} \subseteq \mathbb{Z}_n$. But, if we take $[a]_n \in \mathbb{Z}_n$, we can use the division with remainder theorem to get $a = nq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < |n| = n$. Then, $[a]_n = [nq + r]_n = \{b \in \mathbb{Z} : \ b \equiv nq + r \pmod{n}\}$. But, again, from a proposition proved in my number theory works, we have that $b \equiv nq + r \pmod{n}$ is equivalent to $b \equiv r \pmod{n}$. Therefore, $[a]_n = \{b \in \mathbb{Z} : \ b \equiv r \pmod{n}\} = [r]_n$. As $0 \leq r < n$, we have $[r]_n \in \mathcal{Z}$ and from that $\mathbb{Z}_n \subseteq \mathcal{Z}$. That implies $\mathbb{Z}_n = \mathcal{Z}$ and $|\mathbb{Z}_n| = |\mathcal{Z}| = n$.

□

Proposition. Operation $[a]_n + [b]_n = [a + b]_n$, for all $a, b \in \mathbb{Z}$, is well-defined.

Proof. The operation is obviously defined for all $a, b \in \mathbb{Z}$, as for each element of $\mathbb{Z}$ there exists a corresponding equivalence class (as equivalence relations partition sets). Now, assume $[a]_n = [c]_n$ and $[b]_n = [d]_n$, for some $a, b, c, d \in \mathbb{Z}$. That implies that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. From a property of congruence relation we have that then $a + b \equiv c + d \pmod{n}$, i.e. $(a + b) \sim_n (c + d)$. That implies $[a + b]_n = [c + d]_n$. That proves uniqueness property.

□

Proposition. $\mathbb{Z}_n$ with operation defined in previous proposition is an Abelian group.

Proof. Let $a, b, c \in \mathbb{Z}$. *Associativity.* Holds as $[a]_n + ([b]_n + [c]_n) = [a]_n + [b + c]_n = [a + (b + c)]_n = [(a + b) + c]_n = [a + b]_n + [c]_n = ([a]_n + [b]_n) + [c]_n$. *Neutral element.* Obviously, $[0]_n + [a]_n = [0 + a]_n = [a]_n = [a + 0]_n = [a]_n + [0]_n$. *Inverse elements.* We have $[a]_n + [-a]_n = [a + (-a)]_n = [0]_n = [-a + a]_n = [-a]_n + [a]_n$. *Commutativity.* As follows from addition, $[a]_n + [b]_n = [a + b]_n = [b + a]_n = [b]_n + [a]_n$.

□

Proposition. $\mathbb{Z}_n$ is cyclic.

Proof. If we take $[a]_n \in \mathbb{Z}_n$, then $[a]_n = \underbrace{[1+1+\cdots+1]_n}_{a \text{ times}} = \underbrace{[1]_n + [1]_n + \cdots + [1]_n}_{a \text{ times}}$. Thus, every $[a]_n \in \mathbb{Z}_n$ can be shown as a power (here we use the notation for addition) of $[1]_n \in \mathbb{Z}_n$.

□

Remark. As there is no difference between an operation on equivalence class in $\mathbb{Z}_n$ and an operation between representatives of equivalence classes, we will just, for now, denote $a = [a]_n$, for all $[a]_n \in \mathbb{Z}_n$.

Theorem. Every infinite cyclic group, say $G = \langle a \rangle$, is isomorphic to $\mathbb{Z}$. Similarly, every finite cyclic group, say $G_n = \langle a \rangle$ with generator $a^n = e$, for some $n \in \mathbb{N}$, is isomorphic to $\mathbb{Z}_n$.

Proof. (i) We will define a function $f : \mathbb{Z} \to G$ with formula $f(x) = a^x$, where $a \in G$. First we will show that it is a bijection. *Injectivity.* Take $f(x) = f(y)$. We have $a^x = a^y$. Multiplying by a^{-y} we get $a^{x-y} = e$. As order of a is infinite, there is no positive (nor negative) integer such that $a^n = e$ except for $n = 0$. Thus it must be that $x - y = 0$, i.e. $x = y$ and f is, by that, injective. *Surjectivity.* We take $y \in G$ and want to find $x \in \mathbb{Z}$ such that $f(x) = y$. But, every $y \in G$ is of the form $y = a^i$, where $i \in \mathbb{Z}$, so it is sufficient to take $x = i$ and get $f(i) = a^i$. As both injectivity and surjectivity hold, the function is bijective. Last thing to show is that $f(x + y) = f(x)f(y)$, for all $x, y \in \mathbb{Z}$. We have $f(x+y) = a^{x+y} = a^x a^y = f(x)f(y)$. Therefore, f is an isomorphism, so $G \cong \mathbb{Z}$. (ii) We use the function $f : \mathbb{Z}_n \to G_n$ with $f(x) = a^x$. *Injectivity.* From $f(x) = f(y)$, where $0 \leq x < n$ and $0 \leq y < n$, we get $a^x = a^y$ and $a^{x-y} = e$. As $\operatorname{ord}(a) = n$, it must be that $n|(x - y)$ and $n \leq |x - y|$, i.e. $x - y = nk$, for some $k \in \mathbb{Z}$. Furthermore, that implies $|x - y| = n|k|$. Now, $\mathbb{Z}_n$ contains only integers from 0 to n (excluding), therefore, as $0 \leq x < n$ and $0 \leq y < n$, then surely $|x - y| < n$. Therefore, the only choice for $k \in \mathbb{Z}$ is 0 and it must be $x = y$. *Surjectivity.* Follows from (i) with restriction that $0 \leq x < n$. The property that $f(x + y) = f(x)f(y)$ also follows from (i). Thus, f is an isomorphism and $\mathbb{Z}_n \cong G_n$, for all $n \in \mathbb{N}$.

□

Theorem. Every subgroup of a cyclic group is a cyclic group.

Proof. Let $G = \langle a \rangle$ be a cyclic group. Let G' be a subgroup of G. To show that G' is cyclic we need to find a generator a^g, for some $g \in \mathbb{N}$, and show that every $x \in G'$ can be shown as $x = (a^g)^i$ for some $i \in \mathbb{N}$. As G' is a subgroup of G, every $x \in G'$

is of the form $x = a^i$, for some $i \in \mathbb{N}$. Let $g \in \mathbb{N}$ be such number that $g \leq i$ for all $a^i \in G'$. By division theorem we divide i by g and get $i = gq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < |g| = g$. Therefore, $a^i = a^{gq+r}$, i.e. $a^i = a^{gq}a^r$. By multiplying with a^{-gq} on the right we have $a^i \left(a^q\right)^{-m} = a^r$. As G' is closed under multiplication and with respect to inverses, $a^i \left(a^{-q}\right)^m$ is in G', i.e. $a^r \in G'$. But $0 \leq r < g$ and we assumed that $g > 0$ and $g \leq i$, for all $i \in G$. So it must be $r = 0$. Therefore, $a^i = (a^q)^g$. Thus, G' is generated by a^g.

□

Proposition. Every group $G = \langle a \rangle$ of infinite order is generated by a and a^{-1} and has no other generators.

Proof. From definition of a cyclic group G is generated by a. If we take some $b \in G$, it has to be of the form $b = a^n$, where $n \in \mathbb{Z}$. Taking $b = \left(a^{-1}\right)^{-n}$ shows that every element can be written as a power of inverse of a, therefore G is also generated by a^{-1}. Now suppose that G is generated by some element g. As $g \in G$, and G is cyclic, it has to be of form $g = a^k$, for some $k \in \mathbb{Z}$. Now, if we take some $h \in G$, for which it's $h = a^l$, as g is generator by our assumption, we need to have $h = g^n$, for some $n \in \mathbb{Z}$, id est, $a^l = \left(a^k\right)^n$. From that we get $a^l = a^{kn}$. Multiplying equation by a^{-kn} on the right we get $a^{l-kn} = e$. As a is of infinite order (if it were finite then $\langle a \rangle$ would also be finite, contradicting our statement), the only possibility is that $a^0 = e$. Therefore it must be that $l - kn = 0$, that is $l = kn$. That would mean that $k|l$. But, as our choice of h, and therefore of l, is arbitrary, we can take $l = k - 1$. But, $k \nmid (k-1)$ and l cannot be written as a product of k and n (if $k - 1 = kn$, then $k(1 - n) = 1$ and $k = \frac{1}{1-n}$, which is possible only when $n = 2$ or $n = 0$).

□

Proposition. $\mathbb{R}$ and $\mathbb{R}^*$ are not cyclic groups.

Proof. Suppose that $k \in \mathbb{R}$ generates $\mathbb{R}$. Then every $a \in \mathbb{R}$ can be written as $a = \underbrace{k + k + \cdots + k}_{n \text{ times}} = nk$, where $n \in \mathbb{Z}$. Suppose that k is odd. If we take $b = (n+1)k \in \mathbb{R}$, then $\frac{a+b}{2} \in \mathbb{R}$, but $\frac{a+b}{2} = \frac{k(2n+1)}{2}$. As $2 \nmid (2n+1)$, obviously $\frac{a+b}{2} \in \mathbb{R}$ is not generated by k (it would have to be of the form mk, where $m \in \mathbb{Z}$).

Now, suppose that $k \in \mathbb{R}^*$ generates $\mathbb{R}^*$. Then for some $a \in \mathbb{R}^*$ it has to be $a = k^n$ for some $n \in \mathbb{Z}$. We can also take $b \in \mathbb{R}^*$ such that $b = k^{n+1}$. We can take $\sqrt{ab} \in \mathbb{R}^*$ which is $\sqrt{ab} = k^{\frac{2n+1}{2}}$, which is not an integer power of k.

□

Proposition. Let G be a group and $|G| = n$. G is cyclic if and only if G has an element of order n.

Proof. *Necessity.* Suppose that G is cyclic and $|G| = n$. As G is cyclic it has a generator $a \in G$ which is, by definition, of order n.

Sufficiency. Suppose that $|G| = n$ and G has an element of order n. Suppose that $\operatorname{ord}(b) = n$ for some $b \in G$. We need to prove that G is cyclic. By a previous proposition, all powers of b up to n are distinct. Also, $b^k \in G$ (due to G being closed under multiplication), for every $k \in \{0, \ldots, n-1\}$. Therefore, G must contain all n powers of b and no other elements (as it would be a contradiction with the fact that it's order is n). So, by definition, group G is cyclic.

□

Proposition. Every cyclic group is Abelian.

Proof. Let G be a cyclic group generated by a. Then, every $b, c \in G$ can be written down as $b = a^n$, for some $n \in \{0, \ldots, |G|-1\}$ and $c = a^m$, for some $m \in \{0, \ldots, |G|-1\}$. Thus we have $bc = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = cb$, so G is Abelian.

□

Proposition. If $G = \langle a \rangle$ and $b \in G$, the order of b is a factor of the order of a, i.e. $\operatorname{ord}(b) \,|\operatorname{ord}(a)$.

Proof. We have $\operatorname{ord}(a) = n$ and suppose $\operatorname{ord}(b) = m$. As $b \in G$, then there exists $k \in \{0, \ldots, n-1\}$ such that $b = a^k$. As $a^n = e$, we have $e = (a^n)^k = a^{nk} = \left(a^k\right)^n = b^n$. So, $b^n = e$ and $b^m = e$. By a definition of order we have $m \leq n$. If we divide n by m, we have that $n = mq + r$, for some $q, r \in \mathbb{N}_0$ (as order is always positive) and $0 \leq r < m$. Then, $e = b^n = b^{mq+r} = b^{mq} b^r$, i.e. $e = b^r$. As $b^r = e$ and $0 \leq r < m$ and as it must be that either $r \geq m$ or $r = 0$, the only possible choice is that $r = 0$, so $n = mq$ and from that $m|n$, id est[45] $\operatorname{ord}(b) \,|\operatorname{ord}(a)$.

□

Proposition. Let G be a cyclic group of order n. For every integer k which divides n, there are elements of order k.

Proof. Let $G = \langle a \rangle$, $|G| = n$ and $k \in \mathbb{Z}$ such that $k|n$. We need to prove that there exists $b \in G$ such that $\operatorname{ord}(b) = k$. We have $n = qk$ for some $q \in \mathbb{Z}$. That means

[45] I could have just written down that it follows from previous propisitions, but I wanted to repeat the nice proofs one more time.

that $a^{qk} = e$ and $(a^q)^k = e$, which means that for some $b = a^q$, $m = \operatorname{ord}(b) \,|k$. As $\operatorname{ord}(a) = n$, we have that, by a previous proposition that $\operatorname{ord}(a) = \frac{mq}{l}$, where m and l are relatively prime. So, $n = m\frac{q}{l}$ and from that $m = \frac{nl}{q}$ and $m = \frac{qkl}{q} = kl$, meaning that $k|m$. As we have $m|k$ and $k|m$ then $m = k$, that is, $\operatorname{ord}(b) = k$.

□

Proposition. Let G be an Abelian group of order mn, where m and n are relatively prime. If G has an element of order m and an element of order n, G is cyclic.

Proposition. Let $a, b \in G$ such that $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$ and $\gcd(m, n) = 1$. By a previous proposition, $\operatorname{ord}(ab) = mn$. Also, by a previos proposition, G is cyclic as its order is mn and it contains element of order mn.

□

Proposition. Let $G = \langle a \rangle$ be a cyclic group of order n. If n and m are relatively prime, then the function $f(x) = x^m$ is an automorphism.

Proof. We need to prove that $f : G \to G$ is bijective and that $f(ab) = f(a)f(b)$, for all $a, b \in G$. First we will prove that it is a function. If we take $x \in G$ there needs to be $y \in G$ such that $y = x^m$. So, if we take $a^k \in G$ so that $\left(a^k\right)^m = y$, we need to show that $y \in G$. We have $y = a^{km}$. If we divide km by n, then there exist $q, r \in \mathbb{Z}$ such that $0 \leq r < |n| = n$ and $km = nq + r$. So $y = a^{nq+r}$, i.e. $y = a^{nq}a^r$. But, $a^{nq} = e$ as $\operatorname{ord}(a) = e$ and $y = a^r$. As $0 \leq r < n$, then $a^r \in G$, that is $y \in G$.

Then, if we take $x_1 = x_2$ it must follow that $f(x_1) = f(x_2)$. This one can be proved by induction. From $x_1 = x_2$, by multiplying equation on the right with x_1 we get $x_1^2 = x_2x_1$. But, $x_1 = x_2$, so $x_1^2 = x_2^2$. Then we suppose that the statement is true for some k, that is, $x_1^k = x_2^k$. If we multiply the equation on the right by x_1, we get $x_1^{k+1} = x_2^k x_1$ which is $x_1^{k+1} = x_2^{k+1}$. Therefore, the statement is valid for any $n \in \mathbb{N}$ and by that for m; from $x_1 = x_2$ follows $x_1^m = x_2^m$. Therefore, f is a function.

Injectivity. We need to show that $f(x) = f(y)$ implies $x = y$ for all $x, y \in G$. Let $x = a^k$ and $y = a^l$ (G is cyclic), where $k, l \in \{0, \ldots, n-1\}$. We have $x^m = y^m$, that is, $a^{km} = a^{lm}$. Multiplying by a^{-lm} on the right yields $a^{km-lm} = e$, i.e. $(a^m)^{k-l} = e$. That means that $\operatorname{ord}(a^m) \,|(k-l)$. But, as $\gcd(m, n) = 1$, we have that $\operatorname{ord}(a^m) = n$. That implies that $n|(k-l)$. But, as $0 \leq k, l < n$, then also $|k-l| < n$ and due to our conclusion that $n|(k-l)$ it has to be that $k - l = 0$, i.e. $k = l$ and from that $y = a^l = a^k = x$.

Surjectivity. By a previous theorem, f is an injection if and only if it is a surjection and $|\mathrm{dom}(f)| = |\mathrm{cod}(f)|$. As $|G| = n$, and $f : G \to G$ is an injection, then it must be a surjection and a bijection.

As a last thing, we will prove that $f(xy) = f(x)f(y)$, for all $x, y \in G$. Take $x = a^k$ and $y = a^l$. Then:

$$\begin{aligned} f(xy) &= f(a^k a^l) = f(a^{k+l}) = \left(a^{k+l}\right)^m = a^{m(k+l)} \\ &= a^{mk+ml} = a^{mk}a^{ml} = \left(a^k\right)^m \left(a^l\right)^m = f(a^k)f(a^l) \\ &= f(x)f(y). \end{aligned}$$

Therefore, f is an isomorphism from G to G, and by definition, an automorphism on G.

□

Proposition. Let $G = \langle a \rangle$ be a cyclic group of order n. Then, $r \in \mathbb{N}$ and $\gcd(n, r) = 1$ if and only if a^r is a generator of G.

Proof. *Necessity.* Let $r \in \mathbb{N}$ and $\gcd(n, r) = 1$. As $\operatorname{ord}(a) = n$ by definition, then, as r and n are relatively prime, $\operatorname{ord}(a^r) = n$, by a previous proposition. Also, by a previous proposition, all powers of a^r are distinct. Therefore, $(a^r)^k \in G$, for all $k = 0, \ldots, n-1$, i.e. each power of a must correspond to some power of a^r and reverse. So a^r is a generator of G.

Sufficiency. Suppose a^r is a generator of G. As $|G| = n$ it follows that $\operatorname{ord}(a^r) = n$. From a previous proposition, that means that $\gcd(n, r) = 1$.

□

Definition. Let $\phi : \mathbb{N} \to \mathbb{N}$ be a function which, for every natural number n, assigns the number of natural numbers, less than n, that are relatively prime to n. Such a function is called *Euler's totient function*

Remark. Euler's totient function can be written using the Iverson brackets as:

$$\phi(n) = \sum_{k=1}^{n} [\gcd(n, k) = 1].$$

Proposition. Each cyclic group G of order n has $\phi(n)$ generators.

Proof. From a previous proposition $x \in G$ is a generator of G iff $\gcd(\operatorname{ord}(x), n) = 1$. Also, as we are observing only $x \in G$, they are all distinct and if $x = a^k$ then $k < n$. The number of generators of G is then, by definition of totient function, equal to $\phi(n)$.

□

Proposition. For any factor m of n, let $C_m = \{x \in \langle a \rangle : \ x^m = e\}$. Then, C_m is a subgroup of $\langle a \rangle$ and has exactly m elements.

Proof. Let $G = \langle a \rangle$. By a definition of C_m we have $C_m \subseteq G$. Is C_m non-empty? Due to a previous problem, for every k such that $k|n$ there are elements of order k. Therefore, there are elements of the form $x^m = e$, as $m|n$. If we take $x, y \in C_m$ we have to show that $xy \in C_m$. So, from $x^m = e$ and $y^m = e$, we have that $x^m y^m = e$ and, as $x, y \in G$, and G is Abelian, as proven by a previous proposition, we have $(xy)^m = e$ and by that $xy \in C_m$. Therefore, C_m is closed under multiplication. Furthermore, if we take $x \in C_m$ we need to show that $x^{-1} \in C_m$. As $(x^{-1})^m = x^{-m} = (x^m)^{-1} = e^{-1} = e$, we have that $x^{-1} \in C_m$. That implies that C_m is closed with respect to inverses and C_m is a subgroup of G.

As argued for $C_m \neq \emptyset$, there are elements of order m and they are in C_m. Say $x \in C_m$ is such that $\text{ord}\,(x) = m$. Every subgroup of a cyclic group is cyclic. Therefore C_m has to be generated by a single element. We know that C_m has at least m different elements (from $\text{ord}\,(x) = m$). But, suppose that there exists $y \in C_m$ such that $\text{ord}\,(y) = q > m$ and $y^m = e$. From that we have that $q|m$, which is a contradiction that $q > m$. Therefore as $\text{ord}\,(x) = m$ and there is no element of higher order, and all m powers of C_m are distinct, it must be that $|C_m| = m$.

□

Proposition. An element x in $G = \langle a \rangle$, $|G| = n$, has order m (where $m|n$) if and only if x is a generator of C_m.

Proof. *Necessity.* Suppose $x \in G$ and $\text{ord}\,(x) = m$. Then $x^m = e$ and by definition of C_m it must be that $x \in C_m$. Similarly to the proof in the proposition above, as C_m has exactly m elements and is cyclic, it must be that x generates C_m (as $\text{ord}\,(()\,x) = m$ it generates m different powers of itself and in C_m we have exactly m different powers by previous propositions and it contains x; so every element of C_m is a power of x). *Sufficiency.* If x is a generator of C_m then $\text{ord}\,(x) = m$ (as C_m has exactly m elements).

□

Proposition. There are $\phi(m)$ elements of order m in $G = \langle a \rangle$, $|G| = n$ (where $m|n$).

Proof. By a previous proposition we have that an element is a generator of a group if and only if the order of the group and order of the element are relatively prime. So, if an element $x \in G$ has an order m in G, then it must be in C_m, and it also generates C_m. As x is of the form a^k, where $k \in \{0, \ldots, n-1\}$, we have that a^k generates C_m. Then, by a previous proposition, k and m are relatively prime. As there are $\phi(m)$

natural numbers $(k_1, k_2, \ldots, k_{\phi(m)})$ that are relatively prime to m, then it must be that there are $\phi(m)$ elements of order m in G.

□

Remark. Previous series of propositions actually tell us that if we have $G = \langle a \rangle$ with $|G| = n$, then there are $\phi(k)$ elements of order k for every k that divides n.

Proposition. Let G be a cyclic group generated by a with $|G| = n$. Furthermore, let $n = mk$. a^r has order m if and only if $r = kl$ where l and m are relatively prime.

Proof. *Necessity.* Suppose a^r has order m and $n = mk$. We need to show that $r = kl$ and $\gcd(m, l) = 1$. Suppose that $q|m$ and $q|l$ where $q \in \mathbb{N}$ and $q > 1$. Then $m = qm'$ and $l = ql'$; also, $n = qm'k$ and $r = ql'k$. As a^r generates C_m it must be that r and m are relatively prime. As $r = ql'k$ and $m = qm'$, we have $\gcd(r, m) = q$, which is a contradiction. Therefore m and l are relatively prime.

Sufficiency. Let $n = mk$ and $r = kl$, where $\gcd(l, m) = 1$. We need to show that $\operatorname{ord}(a^r) = m$. As $a^r = a^{kl}$, we have that $\operatorname{ord}\left(a^{kl}\right) = \frac{n}{\gcd(kl,n)}$, by a previous proposition. As $\gcd(kl, n) = \gcd(kl, mk)$ and $\gcd(m, l) = 1$ it must be[46] that $\gcd(kl, n) = k$. We have $\operatorname{ord}\left(a^{kl}\right) = \frac{n}{k} = \frac{mk}{k} = m$, i.e. $\operatorname{ord}(a^r) = m$.

□

Remark. Notice that if c is any generator of $G = \langle a \rangle$, $|G| = n$, then $\operatorname{ord}(c) = n$. If $c = a^k$, it must be that $\gcd(k, n) = 1$. Then if $\gcd(r, n) = 1$, we have $c^r = a^{kr}$ and it must be[47] that $\gcd(kr, n) = 1$. Therefore, c^r is generator of G and the set $\{c^r : \gcd(r, n) = 1\}$ contains all generators of G.

Problem. Let G be a group and let $a, b \in G$. Prove the following:

1. If a is a power of b, say $a = b^k$, then $\langle a \rangle \subseteq \langle b \rangle$;
2. Suppose a is a power of b, say $a = b^k$. Then b is equal to a power of a iff $\langle a \rangle = \langle b \rangle$;
3. Suppose $a \in \langle b \rangle$. Then $\langle a \rangle = \langle b \rangle$ iff a and b have the same order;
4. Let $\operatorname{ord}(a) = n$ and $b = a^k$. Then $\langle a \rangle = \langle b \rangle$ iff n and k are relatively prime;
5. Let $\operatorname{ord}(a) = n$, and suppose a has a k-th root, say $a = b^k$. Then $\langle a \rangle = \langle b \rangle$ iff k and n are relatively prime;
6. Any cyclic group of order mn has a unique subgroup of order n.

[46] Details in my proofs from number theory.
[47] Again, proof in my works on number theory.

Solution.

1. *If a is a power of b, say $a = b^k$, then $\langle a \rangle \subseteq \langle b \rangle$.* If we take some $a^l \in \langle a \rangle$ then $a^l = b^{lk}$, i.e. every power of a can be shown as a power of b, for all $l \in \{0, \ldots, \operatorname{ord}(a)\}$. By definition of a subset of a set, the assumption is true.

2. *Suppose a is a power of b, say $a = b^k$. Then b is equal to a power of a iff $\langle a \rangle = \langle b \rangle$.* *Necessity.* Suppose $a = b^k$ and b is equal to a power of a, i.e. $b = a^l$. Then, by a previous problem we have $\langle a \rangle \subseteq \langle b \rangle$ and $\langle b \rangle \subseteq \langle a \rangle$, for both assumptions, respectively. Those two relations combined yield our necessary implication.

   Sufficiency. Suppose $\langle a \rangle = \langle b \rangle$. If we take $a \in \langle a \rangle$, then also $a \in \langle b \rangle$, so it must be that $a = b^k$. Conversely, if we take b, then it's also in a group generated by a and it must be that $b = a^l$, for some $k, l \in \mathbb{Z}$.

3. *Suppose $a \in \langle b \rangle$. Then $\langle a \rangle = \langle b \rangle$ iff a and b have the same order.* Suppose $a = b^k$, for some $k \in \mathbb{Z}$. *Necessity.* Let us assume that $\langle a \rangle = \langle b \rangle$. We need to prove that $\operatorname{ord}(a) = \operatorname{ord}(b)$. Suppose $\operatorname{ord}(a) = n$ and $\operatorname{ord}(b) = m$. Then, as $a = b^k$, the order of b is $\operatorname{ord}(b) = n\frac{k}{l}$, i.e. $m = n\frac{k}{l}$. Also as $b \in \langle a \rangle$, then $b = a^p$ and $\operatorname{ord}(a) = m\frac{p}{q}$, i.e. $n = m\frac{p}{q}$, where $\frac{k}{l} \in \mathbb{N}$ and $\frac{p}{q} \in \mathbb{N}$ (which follows from Euclid's lemma as $\gcd(n, l) = 1$ and $\gcd(m, q) = 1$). Therefore, as $m|n$ and $n|m$ we have that $\operatorname{ord}(a) = n = m = \operatorname{ord}(b)$.

   Sufficiency. Let $n = \operatorname{ord}(a) = \operatorname{ord}(b)$ and $a = b^k$, for some $k \in \{0, \ldots, n-1\}$. We have that $\operatorname{ord}\left(b^k\right) = n$ (as $a = b^k$ implies $\operatorname{ord}(a) = \operatorname{ord}\left(b^k\right)$) and $\operatorname{ord}(b) = n$. That means that k and n are relatively prime. Thus, b^k generates $\left\langle b^k \right\rangle$ with order n. As $\left\langle b^k \right\rangle$ and $\langle b \rangle$ contain n distinct powers of b, all elements must be equal.

4. *Let $\operatorname{ord}(a) = n$ and $b = a^k$. Then $\langle a \rangle = \langle b \rangle$ iff n and k are relatively prime.* *Necessity.* We have $\operatorname{ord}(a) = n$, $b = a^k$ and $\langle a \rangle = \langle b \rangle$. By a previous proposition a and b have the same order, that is, $\operatorname{ord}(a) = \operatorname{ord}(b) = n$. As $b = a^k$ and $\operatorname{ord}(b) = \operatorname{ord}\left(a^k\right) = n$, by a previous theorem n and k are relatively prime.

   Sufficiency. Let k and n be relatively prime. Then, $\operatorname{ord}(b) = \operatorname{ord}\left(a^k\right) = n$ and by a previous problem we have $\langle a \rangle = \langle b \rangle$.

5. *Let $\operatorname{ord}(a) = n$, and suppose a has a k-th root, say $a = b^k$. Then $\langle a \rangle = \langle b \rangle$ iff k and n are relatively prime.* *Necessity.* If $\langle a \rangle = \langle b \rangle$ then $\operatorname{ord}(a) = \operatorname{ord}(b) = n$. We also have that $\operatorname{ord}(b) = \frac{nk}{l}$, where n and l are relatively prime. But, that means that $n = \frac{nk}{l}$ and from that we have $ln = nk$, i.e. $l = k$. As $\gcd(l, n) = 1$ then, as $l = k$, we have $\gcd(k, n) = 1$.

   Sufficiency. Let k and n be relatively prime. Then, from $\operatorname{ord}(a) = n$ and $a = b^k$ we have that $\operatorname{ord}(a) = \operatorname{ord}\left(b^k\right) = n$. As k and n are relatively prime, it must be, by a previous theorem, that $\operatorname{ord}(b) = n$. From a previous problem, as $\operatorname{ord}(a) = \operatorname{ord}(b) = n$, we have that $\langle a \rangle = \langle b \rangle$.

6. *Any cyclic group of order mn has a unique subgroup of order n. Existence.* Let $G = \langle a \rangle$ be a cyclic group such that $|G| = mn$, for some $m, n \in \mathbb{N}$. If we take $b \in G$, such that $b = a^m$, then $\operatorname{ord}(b) = \frac{mn}{\gcd(mn,m)}$. We have $\gcd(mn, m) = m$ and from that $\operatorname{ord}(b) = \frac{mn}{m} = n$. Therefore we will define $G' = \langle b \rangle$ and, as $\operatorname{ord}(b) = n$, by definition, $|G'| = n$. Let us show that G' is a subgroup of G. By a previous problem, as $b = a^m$, we have that $\langle b \rangle \subseteq \langle a \rangle$, i.e. $G' \subseteq G$. As G' itself is a cyclic group, and is a subset of G, then G' is a subgroup of G with $|G'| = n$.

   Uniqueness. Now, suppose that there exists some cyclic subgroup $H \subseteq G$ such that $|H| = n$. Let $H = \langle c \rangle$. Then as $c \in H \subseteq G$ we have $c = a^k$ for some $k \in \{0, \ldots, mn-1\}$. As $\operatorname{ord}(c) = n$ and $\operatorname{ord}\left(a^k\right) = \frac{mn}{\gcd(mn,k)}$ we have $n \gcd(mn, k) = mn$ and $\gcd mn, k = m$. That means that $m|k$, i.e. $k = mq$. As $c = a^k = a^{mq} = (a^m)^q$ and $b = a^m$, we have $c = b^q$. Which means that $c \in G'$. As $c \in G'$ and $n = \operatorname{ord}(b) = \operatorname{ord}(c)$, by a previous problem we have that $G' = H$.

Problem. Let G and H be groups, with $a \in G$ and $b \in H$. Prove:

1. If (a, b) is a generator of $G \times H$, then a is a generator of G and b is a generator of H. If $G \times H$ is a cyclic group, then G and H are both cyclic and converse is false;

2. Let $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$. The order of (a, b) in $G \times H$ is the least common multiple of m and n;

3. If m and n are relatively prime, then (a, b) has order mn;

4. Suppose $(c, d) \in G \times H$, where c has order m and d has order n. If m and n are not relatively prime, then the order of (c, d) is less than mn.

Solution.

1. *If (a, b) is a generator of $G \times H$, then a is a generator of G and b is a generator of H.* Take $x \in G$ and $y \in H$. We want to show that x can be shown as a power of a and y as a power of b. As (a, b) is a generator of $G \times H$, we have that for $(x, y) \in G \times H$ holds:

$$(x, y) = (a, b)^k = \underbrace{(a, b)(a, b) \cdots (a, b)}_{k \text{ times}}.$$

   By definition of a direct product we have that $(a, b)(a, b) = (aa, bb) = (a^2, b^2)$. When applied k times, as in the above equality, we have $(x, y) = (a^k, b^k)$, so $x = a^k$ and $y = b^k$. Now, as any $x \in G$ and any $y \in H$ can be shown as a power of a and of b, respectively, we have that a generates G and b generates H. From this also follows that if $G \times H$ is cyclic then G and H are both cyclic.

Suppose that G and H are cyclic and $G = \mathbb{Z}_2$ and $H = \mathbb{Z}_4$. By a previous problem (on page 70, excuse me for not labeling problems and theorems, no time for that now, as it's time to practice violin), we have that $G \times H$ is not cyclic, altough generated by two elements.

2. *Let* $\operatorname{ord}(a) = m$ *and* $\operatorname{ord}(b) = n$. *The order of* (a, b) *in* $G \times H$ *is the least common multiple of* m *and* n. As $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$, we have $a^m = e$ and $b^n = e$. Now, $(a, b)^l = (a^l, b^l) = e$, where $l = \operatorname{lcm}(m, n)$. This is obvious as both $m|l$ and $n|l$. Suppose there is some $k \leq l$ such that $(a, b)^k = e$. That would mean that $a^k = e$ and $b^k = e$, which would mean that $m|k$ and $n|k$, therefore k is a common multiple of m and n. As $k \leq l$ and k is a common multiple of m and n, we have a contradiction to assumption that l is the least common multiple of m and n.

3. *If* m *and* n *are relatively prime, then* (a, b) *has order* mn. From a previous problem $\operatorname{ord}((a, b)) = \operatorname{lcm}(m, n)$ and as $\gcd m, n = 1$ we have that $\operatorname{lcm}(m, n) = mn$, so $\operatorname{ord}((a, b)) = mn$.

4. *Suppose* $(c, d) \in G \times H$, *where* c *has order* m *and* d *has order* n. *If* m *and* n *are not relatively prime, then the order of* (c, d) *is less than* mn. As $\operatorname{ord}(c) = m$ and $\operatorname{ord}(c) = n$, then $\operatorname{ord}((c, d)) = \operatorname{lcm}(m, n) < mn$.

Proposition. $\langle a \rangle \times \langle b \rangle$ is cyclic if and only if $\operatorname{ord}(a)$ and $\operatorname{ord}(b)$ are relatively prime.

Proof. Let $G = \langle a \rangle$ and $H = \langle b \rangle$. *Necessity.* Suppose $G \times H$ is cyclic. Then, as (a, b) is obviously a generator of $G \times H$, we have that $\operatorname{ord}((a, b)) = \operatorname{lcm}(m, n)$, where $m = \operatorname{ord}(a)$, and $n = \operatorname{ord}(b)$. Suppose m and n are not relatively prime. Then $\operatorname{ord}((a, b))$ is less than mn, but $G \times H$ must contain all ordered pairs of the form (a^k, b^l), for $k \in \{0, \ldots, m-1\}$ and $l \in \{0, \ldots, n-1\}$ and there are mn of them. Therefore, some cannot be shown as a power of (a, b) as order of (a, b) is less than mn. To conclude, m and n must be relatively prime.

Sufficiency. Suppose m and n are relatively prime. Then, in group $G \times H$ generator (a, b) has order mn and all its elements are distinct. As there are mn possible combinations of (a^k, b^l) (if m and n are relatively prime, by a previos problem, no power of a can equal a power of b), for $k \in \{0, \ldots, m-1\}$ and $l \in \{0, \ldots, n-1\}$ all of them must be contained in $G \times H$, meaning each can be shown as a power of (a, b).

□

Proposition. Let G be an Abelian group of order mn, where m and n are relatively prime. If G has an element a of order m and an element b of order n, then $G \cong \langle a \rangle \times \langle b \rangle$.

Proof. By a previous proposition, as $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$ and $\gcd(m, n) = 1$,

(a, b) generates $\langle a\rangle \times \langle b\rangle$, which has mn elements. If m and n are relatively prime, by a previous problem, no power of a can equal a power of b. Thus, as there are mn combinations of $a^i b^j$ and $\operatorname{ord}(ab) = mn$, by a previous proposition, we have that ab generates G. As m and n are relatively prime $\langle a\rangle \times \langle b\rangle$ is cyclic with mn distinct elements. As (ab) is the only generator of G, i.e. $G = \langle ab\rangle$, and has mn elements, by a previous theorem, both groups are isomorphic to $\mathbb{Z}_{mn}$ and by the property of transitivity of isomorphism, they are isomorphic to each other.

□

Proposition. Let $\langle a\rangle$ be a cyclic group of order mn, where m and n are relatively prime. Then, $\langle a\rangle \cong \langle a^m\rangle \times \langle a^n\rangle$.

Proof. As $\operatorname{ord}(a) = mn$, we have that $\operatorname{ord}(a^m) = \frac{mn}{\gcd(m,mn)} = \frac{mn}{m} = n$. Similarly, $\operatorname{ord}(a^n) = m$. Now, as m and n are relatively prime, no power of a^m can equal a power of a^n (due to facts that cyclic groups are Abelian and that $\gcd(\operatorname{ord}(a^m), \operatorname{ord}(a^n)) = 1$). Therefore, there are mn distinct elements in $\langle a^m\rangle \times \langle a^n\rangle$. Also, as m and n are relatively prime, $\langle a^m\rangle \times \langle a^n\rangle$ is cyclic. Both groups are cyclic with mn elements, so they are isomorphic to $\mathbb{Z}_{mn}$, by a previous theorem, and by that to each other.

□

Theorem. Element a^m has a k-th root in $G = \langle a\rangle$, where $|G| = n$, if and only if $\gcd(k, n)|m$.

Proof. Let us denote $g = \gcd(k, n)$. *Necessity.* Suppose a^m has a k-th root in G, i.e. there exists $b \in G$ such that $a^m = b^k$. But, $b \in G$ so it must be of the form $b = a^x$, for some $x \in \{0, \ldots, n-1\}$ and we have $a^m = a^{xk}$. Multiplying by a^{-m} on the right gives us $e = a^{xk-m}$. Dividing $xk - m$ by n gives us $xk - m = nq + r$, for some $q, r \in \mathbb{Z}$, where $0 \leq r < |n| = n$. Then we have $e = a^{nq}a^r$, and as $a^{nq} = e$, we have $a^r = e$. But, $r < n$, and n is order of a, so it must be $r = 0$. Therefore we have $xk - m = nq$. That is equivalent to $xk - nq = m$. As m can be shown as a linear combination of k and n (we can take $q' = -q$ to have $xk + q'n = m$, and we assumed existence of x and shown existence of q' by division with remainder theorem), then it must be, by corollary of Bezout's lemma (discussed in my works on number theory) that $g|m$.

Sufficiency. Suppose $g|m$. By a corollary of Bezout's lemma we have that $m = xk + yn$ (because $g|m$), for some $x, y \in \mathbb{Z}$. So we have $a^m = a^{xk}a^{yn}$. As $\operatorname{ord}(a) = n$, then $a^{yn} = e$. Therefore, $a^m = a^{xk} = (a^x)^k$. Here a^x is obviously k-th root of a^m and it's existence is proven by forementioned corollary.

□

Corollary. Element a has a k-th root in $G = \langle a \rangle$, where $|G| = n$, if and only if $\gcd(k, n) = 1$.

Proof. By definition $a = a^1$, so by a previous theorem (taking $m = 1$ from a^1) a^1 will have a k-th root in G if and only if $\gcd(k, n)|m$, i.e. $\gcd(k, n)|1$. But, as $\gcd(k, n) \in \mathbb{Z}\backslash\{0\}$, it can only be that $\gcd(k, n) = 1$.

□

Corollary. Let p be a prime number and $G = \langle a \rangle$, where $|G| = n$.

1. If n is not a multiple of p, then every element in G has a p-th root.
2. If n is a multiple of p, and a^m has a p-th root, then m is a multiple of p.

Proof. Suppose $p \in P$ and $G = \langle a \rangle$.

1. Let us assume that $p \nmid n$. That implies, by fundamental theorem of arithmetic, that n must not contain any positive power of p and that further implies that $\gcd(p, n) = 1$. If we take a^k, for any $k \in \{0, \ldots, n-1\}$, we have that $1|k$. But, $\gcd(p, n) = 1$, so we have $\gcd(p, n)|k$. By a previous theorem it follows that a^k has a p-th root.
2. Let $n = pq$ for some $q \in \mathbb{N}$ (as $n, p \in \mathbb{N}$ by definition). If a^m has a p-th root, then from a previos theorem it follows that $\gcd(p, n)|m$. But, $\gcd(p, n) = \gcd(p, pq) = p$ (proof discussed in my work on number theory). So we have that $p|m$, i.e. m is a multiple of p.

□

Proposition. The set of all elements in $G = \langle a \rangle$, where $|G| = n$, having a k-th root is a subgroup of G and it is cyclic.

Proof. Let $R = \{x \in G : (\exists y \in G)(\exists k \in Z)(x = y^k)\}$. By definition $R \subseteq G$. Is R non-empty? Of course, it will contain at least neutral element $e \in G$ because $e = e^k$, for any $k \in \mathbb{Z}$. If we take $x, y \in R$ then x and y have k-th roots in G and $x = u^k$ and $y = v^k$, where $u, v \in G$. Multiplying them gives us $xy = u^k v^k$. As G is cyclic and therefore Abelian, we have $xy = (uv)^k$. Due to the fact that $u, v \in G$, and G is a group and therefore closed under multiplication, we have that $uv \in G$. So, xy has a k-th root in G and it must be that $xy \in R$. So, R is closed under multiplication. If we take $x \in R$, then $x = u^k$ for some $u \in G$. As $u \in G$, it has an inverse and we have $u^{-1}u = e$. Also, $(u^{-1}u)^k = e$ and, because it is cyclic and therefore Abelian, we have $(u^{-1})^k u^k = e$. But, $u^k = x$, so we have $(u^{-1})^k x = e$. Multiplying by $x^{-1} \in G$, on the

right gives us $(u^{-1})^k = x^{-1}$. We already discussed that $u^{-1} \in G$, so x^{-1} has a k-th root in G and it must be in R. Therefore, R is closed with respect to inverses and it is a subgroup of G. As every subgroup of a cyclic group is cyclic, it follows that R is also cyclic.

□

Remark. Notice that as R, from previous proposition, is cyclic and contains elements from G, it is of the form $R = \langle a^m \rangle$. But, if $a^m \in R$ then it has a k-th root in G, so it must be, by a previous theorem that $\gcd(k, n) | m$, i.e. there exists $q \in \mathbb{Z}$ such that $m = q \gcd(k, n)$. So, $R = \left\langle a^{q \gcd(k,n)} \right\rangle$, for some $q \in \mathbb{Z}$. But, if $a^{q \gcd(k,n)}$ is a generator of R, then it must be that $\gcd(|R|, q \gcd(k, n)) = 1$. From this point of view $|R| = \operatorname{ord}\left(a^{q \gcd(k,n)}\right) = \frac{n}{q \gcd(k,n)}$. Also, as $g | m$, then there exist $x, y \in \mathbb{Z}$ such that $m = xk + yn$ and $a^m = a^{xk} a^{yn} = a^{xk}$. So we also have that $R = \left\langle a^{xk} \right\rangle$, for some $x \in \mathbb{Z}$. We have $\operatorname{ord}\left(a^{xk}\right) = \frac{n}{\gcd(xk,n)}$ and it must also be that $\gcd\left(\frac{n}{\gcd(xk,n)}, xk\right) = 1$.

Counting cosets

Definition. Let G be a group and H a subgroup of G. Let $a \in G$. A **left coset** of H in G is defined as:

$$aH = \{y \in G : \ (\forall h \in H)(y = ah)\}.$$

Similarly, a **right coset** of H in G is:

$$Ha = \{y \in G : \ (\forall h \in H)(y = ha)\}.$$

Remark. From now on we will refer to the *right coset* of H in G simply as the *coset* of H in G. Thus we avoid any ambiguity.

Lemma. Let G be a group and H a subgroup of G. Let $a, b \in G$. If $a \in Hb$ then $Ha = Hb$.

Proof. As $a \in Hb$, then there exists $h_1 \in H$ such that $a = h_1 b$. If we take $x \in Ha$ then there exists $h_2 \in H$ such that $x = h_2 a$. That implies that $x = h_2 h_1 b$, i.e. $x = (h_2 h_1)b$. As H is a subgroup of G and $h_1, h_2 \in H$, then their product is in H. So, as there exists $h \in H$, where $h = h_2 h_1$, such that $x = hb$, it must be that $x \in Hb$. As $x \in Ha$ implies $x \in Hb$ we have $H_a \subseteq H_b$. Conversely, if we take $x \in H_b$ then there exists $h_3 \in H$ such that $x = h_3 b$. As $h_3 \in H$ and H is a subgroup of G, then H is closed with respect to inverses, and there exists $h_3^{-1} \in H$ such that $h_3^{-1} x = b$. Plugging that in $a = h_1 b$ we get $a = h_1 h_3^{-1} x$. Multiplying by h_1^{-1} and h_3 on the left gives us $h_1^{-1} h_3 a = x$, i.e. if we take $h' \in H$ such that $h_1^{-1} h_3 = h'$ (as H is a subgroup, i.e. H is closed with respect to inverses and multiplication), we have $x = h'a$, i.e. $x \in Ha$. As $x \in Hb$ implied $x \in Ha$ we have $Hb \subseteq Ha$. That, combined with $Ha \subseteq Hb$, implies $Ha = Hb$.

□

Theorem. Let G be a group and H a subgroup of G. Family $\{Ha : \ a \in G\}$ is a partition of G.

Proof. If we take $x \in G$ then obviously $x \in Hx$, as $e \in H$ and $x = ex$. Then, if we take $x \in Ha$ and $x \in Hb$, there exist $h_1, h_2 \in H$ such that $x = h_1 a$ and $x = h_2 b$. That implies that $h_1 a = h_2 b$. Multiplying with $h_1^{-1} \in H$ on the left gives us $a = (h_1^{-1} h_2)b$, i.e. $a \in Hb$. From a previous lemma it follows that $Ha = Hb$. Thus, the forementioned family is a partition of G.

□

Theorem. Let G be a group and H a subgroup of G. For each $a \in G$ there is a bijection $f : H \to Ha$.

Proof. Let $a \in G$ and $f(x) = xa$ with $f : H \to Ha$. *Injectivity.* If $f(x) = f(y)$ we have $xa = ya$. Multiplying by $a^{-1} \in G$ on the right gives us $x = y$, for all $x, y \in H$. *Surjectivity.* Take $y \in Ha$. Then $y = ha$, for some $h \in H$. We need to find $x \in H$ such that $f(x) = y$, i.e. $xa = ha$. Multiplying by $a^{-1} \in G$ on the right gives $x = h$. Indeed, as $h \in H$, also $h \in G$. Therefore, as f is injective and surjective, it is also bijective.

□

Theorem (Lagrange). If G is a finite group and H a subgroup of G, then $|H|$ divides $|G|$.

Proof. Suppose $|G| = n$ and $|H| = m$. We need to prove that $m|n$. Consider the partition $\{H_i : \ i \in I\}$, where H_i are cosets of H in G. As G is finite, so is this partition, say that there are k of H_i, where $k \in \mathbb{N}$ (we have at least $H = \{e\}$, a trivial subgroup, so $k \geq 1$). Then, using the fact that union of all H_i is G we have:

$$\bigcup_{i=1}^{k} H_i = G.$$

Then it also must be that:

$$\left| \bigcup_{i=1}^{k} H_i \right| = |G|.$$

Keep in mind that all H_i are mutually disjoint. Also by a previos theorem, there exists a bijection from H to each H_i, meaning $|H| = |H_i| = m$, i.e. $|H_i| = m$, for each $i \in \{1, \ldots, k\}$. So as there are k of disjoint H_i and $|H_i| = m$ we have $k \cdot m = n$ (remember that $|G| = n$ by assumption), i.e. it must be that $m|n$.

□

Corollary. If G is a group with a prime number p of elements, i.e. $|G| = p$, then G is a cyclic group. Furthermore, any element $a \neq e$ in G is a generator of G.

Proof. If we take $a \in G$ such that $\text{ord}\,(a) = m$, for some $m \in \mathbb{N}\backslash\{1\}$ we can observe $G' = \langle a \rangle$. By definition, $|G'| = m$. Also, G' is a cyclic group and is contained in G (as G is closed with respect to inverses and multiplication), so it is a subgroup of

G. Therefore, by Lagrange's theorem, it must be that $m|p$, but that can only be if $m = 1$ or $m = p$. We assumed that $\text{ord}\,(a) \neq 1$, so it must be that $m = p$. Therefore G' contains all elements of G. As G' is cyclic and contains all elements of G, then it follows that every element in G can be shown as a power of a; it is also cyclic and generated by a. Our choice of a was arbitrary so it proves the second part of the corollary.

□

Corollary. Let G be a finite group with $|G| = n$. Let $a \in G$. Then, $\text{ord}\,(a)\,|n$.

Proof. Consider the group $G' = \langle a \rangle$. Then, by definition, $|G'| = \text{ord}\,(a)$. Also, G' is a subgroup of G as G' is cyclic by definition and G contains all its elements. Then, by Lagrange's theorem $|G'|$ divides $|G|$. But, $|G'| = \text{ord}\,(a)$ and $|G| = n$ so $\text{ord}\,(a)\,|n$.

□

Definition. Let G be a group and H a subgroup of G. The **index of H in G** is the number of cosets of H in G, denoted by $[G : H]$.

Proposition. Let G be a group and H a subgroup of G. Then:

$$[G : H] = \frac{|G|}{|H|}.$$

Proof. Let G be a group with $|G| = n$ and H a subgroup of G such that $|H| = m$. Suppose there are k cosets of H. Then all H_i, for $i \in \{1, \ldots, k\}$, have the same number of elements. Furthermore, they have the same number of elements as H. So we would have k cosets of H with the same number of elements, and that is m. As they are all disjoint and their union is all of G, it must be that $m \cdot k = n$. So, the number of cosets of H is $k = \frac{n}{m}$.

□

Remark. If operation on G is denoted by $+$, it is customary to write $H + x$ for a coset, rather than Hx. That is true for some other operation $*$, where we would have $H * x$, et cetera.

Problem. In each of the following, H is a subgroup of G. List the cosets of H and their elements. Indicate the order and index of each of the subgroups.

1. $G = \mathbb{Z}_4$, $H = \{0, 2\}$;
2. $G = S_3$, $H = \{\epsilon, \beta, \delta\}$;

3. $G = S_3$, $H = \{\epsilon, \alpha\}$;

4. $G = \mathbb{Z}_{15}$, $H = \langle 5 \rangle$;

Remark. We will use this table for S_3:

$\circ$	ϵ	α	β	γ	δ	κ
ϵ	ϵ	α	β	γ	δ	κ
α	α	ϵ	γ	β	κ	δ
β	β	κ	δ	α	ϵ	γ
γ	γ	δ	κ	ϵ	α	β
δ	δ	γ	ϵ	κ	β	α
κ	κ	β	α	δ	γ	ϵ

We will also use:

Solution.

1. $G = \mathbb{Z}_4$, $H = \{0, 2\}$. We have $|G| = 4$ and $|H| = 2$. Therefore, $[G : H] = \frac{4}{2} = 2$. Furthermore, $H + 0 = H + 2 = \{0, 2\} = H$, $H + 1 = H + 3 = \{1, 3\}$.

2. $G = S_3$, $H = \{\epsilon, \beta, \delta\}$. From $|S_3| = 3! = 6$ and $|H| = 3$ follows that $[G : H] = \frac{6}{3} = 2$. Now, $H\epsilon = H\beta = H\delta = \{\epsilon, \beta, \delta\} = H$, $H\alpha = H\gamma = H\kappa = \{\alpha, \gamma, \kappa\}$.

3. $G = S_3$, $H = \{\epsilon, \alpha\}$. Similarly to the previous example, we have $[G : H] = \frac{6}{2} = 3$. So, $H\epsilon = H\alpha = \{\epsilon, \alpha\}$, $H\beta = H\gamma = \{\beta, \gamma\}$, $H\delta = H\kappa = \{\delta, \kappa\}$.

4. $G = \mathbb{Z}_{15}$, $H = \langle 5 \rangle$. We have $|\mathbb{Z}_{15}| = 15|$ and $H = \{0, 5, 10\}$, so $|H| = 3$ and $[G : H] = \frac{15}{3} = 5$. We have $H + 0 = H + 5 = H + 10 = \{0, 5, 10\}$, $H + 1 = H + 6 = H + 11 = \{1, 6, 11\}$, $H + 2 = H + 7 = H + 12 = \{2, 7, 12\}$, $H + 3 = H + 8 = H + 13 = \{3, 8, 13\}$ and $H + 4 = H + 9 = H + 14 = \{4, 9, 14\}$.

Proposition. Let $m \in \mathbb{Z}^+$. Then, $[\mathbb{Z} : \langle m \rangle] = m$.

Proof. Let us observe the cosets of $\langle m \rangle = \{\ldots, -2m, -m, 0, m, 2m, 3m, \ldots\} = \{km \in \mathbb{Z} : \ k \in \mathbb{Z}\}$. Then, $\langle m \rangle + l = \{km + l \in \mathbb{Z} : \ k \in \mathbb{Z}\}$, for all $l \in \mathbb{Z}$. By division with remainder theorem there exist $q, r \in \mathbb{Z}$ such that $l = qm + r$, where $0 \leq r < m$. So we have $\langle m \rangle + (qm + r) = \{(k + q)m + r \in \mathbb{Z} : \ k \in \mathbb{Z}\} = \{km + r \in \mathbb{Z} : \ k \in \mathbb{Z}\}$, for all $0 \leq r < m$. Therefore, there exist m different cosets of $\langle m \rangle$.

□

Problem. Describe the cosets of the following subgroups:

1. The subgroup $\langle 3 \rangle$ of $\mathbb{Z}$;

2. The subgroup $\mathbb{Z}$ of $\mathbb{R}$;

3. The subgroup $H = \{2^n : \ n \in \mathbb{Z}\}$ of $\mathbb{R}^*$;

4. The subgroup $\left\langle \frac{1}{2} \right\rangle$ of $\mathbb{R}^*$ and of $\mathbb{R}$;

5. The subgroup $H = \{(x, y) : \ x = y\}$ of $\mathbb{R} \times \mathbb{R}$.

Solution.

1. *The subgroup* $\langle 3 \rangle$ *of* $\mathbb{Z}$. We have $\langle 3 \rangle + r = \{\ldots, -6+r, -3+r, 0+r, 3+r, 6+r, \ldots\}$, for all $0 \leq r < 3$. So, there are 3 different cosets.

2. *The subgroup* $\mathbb{Z}$ *of* $\mathbb{R}$. $\mathbb{Z} + r = \{\ldots, -2 + r, -1 + r, r, 1 + r, 2 + r, \ldots\}$, for all $r \in \mathbb{R}$, i.e. $\mathbb{Z} + r = \{k + r \in \mathbb{R} : \ k \in \mathbb{Z}\}$.

3. *The subgroup* $H = \{2^n : \ n \in \mathbb{Z}\}$ *of* $\mathbb{R}^*$. $Hr = \{2^n r \in \mathbb{R}^* : \ n \in \mathbb{Z}\}$. Of course $H(2^k r) = Hr$, for all $k \in \mathbb{Z}$.

4. *The subgroup* $\left\langle \frac{1}{2} \right\rangle$ *of* $\mathbb{R}^*$ *and of* $\mathbb{R}$. $\left\langle \frac{1}{2} \right\rangle r = \{\frac{r}{2^k} \in \mathbb{R} : \ k \in \mathbb{Z}\}$ and $\left\langle \frac{1}{2} \right\rangle + r = \{\frac{1+2kr}{2k} \in \mathbb{R} : \ k \in \mathbb{Z}\}$, respectively.

5. *The subgroup* $H = \{(x, y) : \ x = y\}$ *of* $\mathbb{R} \times \mathbb{R}$. $H(a, b) = \{(xa, yb) \in \mathbb{R} \times \mathbb{R} : \ x = y\}$.

Problem. Find a subgroup of $\mathbb{R}^*$ whose index is equal to 2.

Solution. If we take $H = \{r \in \mathbb{R}^* : \ r > 0\}$ it is obvious that it is a subgroup of $\mathbb{R}^*$ as $x \cdot y > 0$ for $x, y > 0$ and for $x > 0$ we have $\frac{1}{x} \in H$ because $\frac{1}{x} > 0$ for $x > 0$. We can see that $Hx = H$ for $x > 0$ and $Hx = \{r \in \mathbb{R}^* : \ r < 0\}$ for $x < 0$. We are of course assuming $x \in \mathbb{R}^*$ for all mentions of x. Therefore, there are two different cosets of H in $\mathbb{R}^*$.

Proposition. If G is a group and has order n, then $x^n = e$ for every $x \in G$.

Proof. Suppose G is a group and $|G| = n$. Take $x \in G$. By a previous corollary $\operatorname{ord}(x) | n$, i.e. there exists $q \in \mathbb{Z}$ such that $n = q\operatorname{ord}(x)$. We have $x^n = x^{q\operatorname{ord}(x)} = \left(x^{\operatorname{ord}(x)}\right)^q$. As $x^{\operatorname{ord}(x)} = e$, by definition, we have $x^n = e^q = e$.

□

Proposition. Let G be a group and $|G| = pq$, where $p, q \in P$. Then, either G is cyclic, or every element $x \neq e$ in G has order p or q.

Proof. We have, by a previous corollary that $\operatorname{ord}(x) | pq$ for all $x \in G$. But, by

Euclid's lemma, as $\gcd(\text{ord}(x), p) = \gcd(\text{ord}(x), q) = 1$, the only possible options are that $\text{ord}(x) = p$, $\text{ord}(x) = q$ or $\text{ord}(x) = pq$ (we will ignore when $\text{ord}(x) = 1$ for that is true only for a neutral element). If $\text{ord}(x) = pq$ for some $x \in G$, then, by a previous theorem[48], we have that G is cyclic. If there does not exist $x \in G$ such that $\text{ord}(x) = pq$, then $\text{ord}(x) = p$ or $\text{ord}(x) = q$, for all $x \in G$ (except, of course, $e \in G$ whose order is 1).

□

Proposition. If G is a group and $|G| = 4$ then either G is cyclic, or every element of G is its own inverse. Every group of order 4 is Abelian.

Proof. By a previos corollary we have that $\text{ord}(x) | 4$ for every $x \in G$. So we can have $\text{ord}(x) = 4$ and $\text{ord}(x) = 2$ (we will ignore $\text{ord}(x) = 1$). Suppose there exists $x \in G$ such that $\text{ord}(x) = 4$. Then, by a theorem mentioned in the proof of the previous proposition, G is cyclic. Suppose that there does not exist $x \in G$ such that $\text{ord}(x) = 4$. Then, for all $x \in G$ (except $e \in G$) we have $\text{ord}(x) = 2$, that is $x^2 = xx = e$, which means that every element is its own inverse. We will prove that such group is Abelian. Take $x, y \in G$. We have $xy = z$, where $z \in G$. As $z^2 = e$, we have $(xy)^2 = e$, i.e. $xyxy = e$. Multiplying by y on the right gives us $xyx = y$. Multiplying by x on the left gives us $yx = xy$. Thus, G is Abelian.

□

Proposition. Let G be a group. If G has an element of order p and an element of order q, where p and q are distinct primes, then the order of G is a multiple of pq.

Proof. Let $|G| = n$. Suppose there exist $x, y \in G$ such that $\text{ord}(x) = p$ and $\text{ord}(x) = q$. Then, by a previous theorem, it must be that $p|n$ and $q|n$. As $p|n$, there exists $k \in \mathbb{Z}$ such that $n = pk$. Now, as $q|n$, and by that $q|pk$, with $q \neq 1$ and $q \neq p$ by assumption, by Euclid's lemma, as $\gcd(p, q) = 1$ for any two distinct primes $p, q \in P$, we have that $q|k$, i.e. there exists $l \in \mathbb{Z}$ such that $k = ql$. Plugging that back into n, we have $n = pql$, that is $pq|n$.

□

Proposition. Let G be a group with $|G| = n$. If G has an element of order k and an element of order m, then $\text{lcm}((k, m)) | n$.

Proof. By a previous corollary we have that $k|n$, i.e. there exists $q \in \mathbb{Z}$ such that $n = kq$. Let $g = \gcd(k, m)$. Then $k = gx$ and $m = gy$ for some $x, y \in \mathbb{Z}$ such that

[48] On page 159.

$\gcd(x,y) = 1$. Then, $\operatorname{lcm}(m,k) = \frac{gxgy}{g} = gxy$. We have $n = gxq$. But, as $m|n$, that is, $gy|gxq$, there exists $q' \in \mathbb{Z}$ such that $gxq = gyq'$. From that we have $xq = yq'$. That means that $x|yq'$. But, as $\gcd(x,y) = 1$, by Euclid's lemma it has to be $x|q'$, i.e. there exists $q'' \in \mathbb{Z}$ such that $q' = q''x$. Plugging that back gives us $gxq = gyq''x$, i.e. $n = gyq''x$. As $\operatorname{lcm}((m,k)) = gxy$, we have $n = q''\operatorname{lcm}((m,k))$ and from that it follows that $\operatorname{lcm}((m,k))\,|n$.

□

Proposition. Let p be a prime number. In any finite group, the number of elements of order p is a multiple of $p-1$.

Proof. Let G be a finite group and $|G| = n$. Suppose there exist k elements whose order is p. Choose $a \in G$ such that $\operatorname{ord}(a) = p$. Let's observe subgroup $\langle a \rangle$. As $\operatorname{ord}(a) = p$ then $|\langle a \rangle| = p$. By a previous theorem a^r, for $r \in \{1, \ldots, p-1\}$, is a generator of $\langle a \rangle$ if and only if p and r are relatively prime. But, as p is a prime number, then $\gcd(r,p) = 1$, for all $r \in \{1, \ldots, p-1\}$ (we exclude $e = a^0 = a^p$ as we know its order is 1). Therefore there are $p-1$ generators of $\langle a \rangle$. Also we have, by a previous theorem, $\operatorname{ord}(a^r) = p$ if and only if r and p are relatively prime, but that is true for all $r \in \{1, \ldots, p-1\}$. So, in $\langle a \rangle$ there are $p-1$ elements of order p. Suppose there are l such cyclic subgroups of G (not generated by any power of a; then they are disjoint, by a previous problem[49]). Thus, there are $l \times (p-1)$ elements of order p, i.e. $k = l \times (p-1)$.

□

Proposition. Let G be a finite group and let H and K be subgroups of G such that $H \subseteq K$. Then $[G:H] = [G:K] \cdot [K:H]$.

Proof. Obviously, H is a subgroup of K (H is a group itself, closed with respect to multiplication and inverses and all its elements are in K). By Lagrange's theorem $|H|$ divides $|K|$ and index of H in K is $[K:H] = \frac{|K|}{|H|}$. From that we have $|H| = \frac{|K|}{[K:H]}$. Now, as K is a subgroup of G, by Lagrange's theorem, we have $[G:K] = \frac{|G|}{|K|}$. From that follows $|K| = \frac{|G|}{[G:K]}$. Also, as H is also a subgroup of G, we have $[G:H] = \frac{|G|}{|H|}$. Plugging previous two equalities we have:

$$[G:H] = \frac{|G|}{\frac{|K|}{[K:H]}} = \frac{|G| \cdot [K:H]}{|K|} = \frac{|G| \cdot [K:H]}{\frac{|G|}{[G:K]}} = [K:H] \cdot [G:K].$$

□

[49] Third problem on page 164

Proposition. Let G be a finite group and H and K subgroups of G. Then:

1. $|H \cap K|$ is a common divisor of $|H|$ and $|K|$;
2. If $\gcd(|H|, |K|) = 1$ then $|H \cap K| = \{e\}$;
3. If $H \neq K$ and $|H| = |K| = p$ then $|H \cap K| = \{e\}$;
4. If $[G : H] = p$ and $[G : K] = q$, for $q, p \in P$ such that $q \neq p$, then $pq|[G : (H \cap K)]$.

Proof. Let $|H| = m$, $|K| = k$ and $|G| = n$. Remember[50] that $H \cap K$ is a subgroup of G if H and K are subgroups of G. Now, as in the previous proposition, as $H \cap K$ is a subgroup of G and so are H and K, and we have $H \cap K \subseteq H$ and $H \cap K \subseteq K$, then, $H \cap K$ is a subgroup of H and a subgroup of K.

Ad 1. Let $l = |H \cap K|$. Then, as $|H \cap K|$ is a subgroup of K, we have $l|k$, and $l|m$ as it is a subgroup of H. Therefore $|H \cap K|$ is a common divisor of $|H|$ and $|K|$.

Ad 2. Suppose $\gcd(|H|, |K|) = 1$. From a previous problem we have that $|H \cap K|$ is a common divisor of $|H|$ and $|K|$. But, the only divisor is 1, so it must be that $|H \cap K| = 1$. So, $H \cap K = \{x\}$. As $H \cap K$ is a subgroup of G, it must be closed with respect to multiplication, so the only option is $xx = x$. As it is closed with respect to inverses also, and the only option is $x^{-1} = x$, we have $x^{-1}x = x$. As $x^{-1}x = e$, where e is a neutral element in G it must be that $x = e$. Thus, $H \cap K = \{e\}$.

Ad 3. As $H \neq K$, they don't have all elements in common, but maybe some $k < |H| = |K| = p$. As $|H \cap K| = k$ and $|H \cap K|$ is a common divisor of $|H|$ and $|K|$, it must be that $k|p$. But, that is only possible if $k = 1$ or $k = p$. But, we assumed that $H \neq K$, and from that we concluded $k < p$ and the only option is that $k = 1$. As in 2, it implies that $H \cap K = \{e\}$.

Ad 4. We have that $[G : (H \cap K)] = [G : H] \cdot [H : (H \cap K)]$ and $[G : (H \cap K)] = [G : K] \cdot [K : (H \cap K)]$. That implies that $[G : H] \cdot [H : (H \cap K)] = [G : K] \cdot [K : (H \cap K)]$, i.e. $px = qy$, where we took $[H : (H \cap K)] = x$ and $[K : (H \cap K)] = y$. In assumption we have $p \neq q$. Then $\gcd(p, q) = 1$ (as they are prime) implies, by Euclid's lemma that $p|y$. So from $x = q\frac{y}{p}$ we can take $c \in \mathbb{N}$ to be $c = \frac{y}{p}$ and have $x = qc$. Similarly $y = p\frac{x}{q} = pc'$. Now we have $[G : (H \cap K)] = pqc$. Therefore, $pq|[G : (H \cap K)]$.

□

Proposition. If G is an abelian group of order n, and m is an integer such that m and n are relatively prime, then the function $f(x) = x^m$ is an automorphism of G.

Proof. First we will show that $f : G \to G$ is a bijection. *Injectivity.* If we take $f(x_1) = f(x_2)$ then we have $x_1^m = x_2^m$. If we multiply that by $(x_2^m)^{-1}$ (which is

[50] Proof on page 63, first problem.

equal to $\left(x_2^{-1}\right)^m$), we get $x_1^m \left(x_2^{-1}\right)^m = e$. From that, as G is Abelian, it follows that $\left(x_1 x_2^{-1}\right)^m = e$. By a corollary of Lagrange's theorem $\operatorname{ord}\left(x_1 x_2^{-1}\right) | n$, but also $\operatorname{ord}\left(x_1 x_2^{-1}\right) | m$. Therefore, $\operatorname{ord}\left(x_1 x_2^{-1}\right)$ is a common divisor of m and n. But, m and n are relatively prime, so it can only be that $\operatorname{ord}\left(x_1 x_2^{-1}\right) = 1$. That implies that $\left(x_1 x_2^{-1}\right)^1 = e$, i.e. $x_1 x_2^{-1} = e$. By multiplying with x_2 on the right we have $x_1 = x_2$. Therefore, f is injective.

Surjectivity. If we take $y \in G$, then we need to find $x \in G$ such that $y = x^m$. In other words, we are looking for m-th root of y. Let's observe $\langle y \rangle$. It is a subgroup of G, so it's order must divide n. Suppose $|\langle y \rangle| = n'$. Then we have, as $\langle y \rangle$ is a subgroup of G, by Lagrange's theorem that $n' | n$. But, as $\gcd(m, n) = 1$, then also $\gcd(m, n') = 1$ (proof in my works on number theory). By a previous proposition[51] we have that, as n' and m are relatively prime, that y has an m-th root in $\langle y \rangle$. Therefore there exists $x \in \langle y \rangle \subseteq G$ such that $y = x^m$

Finally, we want to show that $f(xy) = f(x)f(y)$, for all $x, y \in G$. We have $f(xy) = (xy)^m$. But, as G is Abelian, it follows that $(xy)^m = x^m y^m$, i.e. $f(xy) = x^m y^m = f(x)f(y)$. Therefore, f is an isomorphism from G to G, and by definition an automorphism on G.

□

Remark. Let S_1 and S_2 be two non-empty sets. We will say that $S_1 \subseteq S_2$ if for every $x \in S_1$ there exists $y \in S_2$ such that $x = y$. We will say that $S_1 = S_2$ if $S_1 \subseteq S_2$ and $S_2 \subseteq S_1$, i.e. if for every $x \in S_1$ there exists $y \in S_2$ such that $x = y$ and if for every $x \in S_2$ there exists $y \in S_1$ such that $x = y$. It takes a little observation to see that this is equivalent to saying that $S_1 = S_2$ if $x \in S_1$ implies $x \in S_2$ and if $x \in S_2$ implies $x \in S_1$.

Proposition. Let G be a group and H a subgroup of G. Let $a, b \in G$. Then:

1. $a \in Ha$;
2. $Ha = Hb$ iff $ab^{-1} \in H$;
3. $He = H$;
4. $Ha = H$ iff $a \in H$;
5. If $aH = Ha$ and $bH = Hb$, then $(ab)H = H(ab)$;
6. If $aH = Ha$, then $a^{-1}H = Ha^{-1}$;
7. If $(ab)H = (ac)H$, then $bH = cH$;

[51] Corollary on page 169

8. The number of right cosets of H is equal to the number of left cosets of H.

Proof. *Ad* 1. To prove that a is in Ha, we need to find $h \in H$ such that $a = ha$. But, it must be that $e \in H$, so we can take $h = e$ and have $a = ea$. That is, there exists $e \in H$ such that $a = ea$, and by definition, $a \in Ha$. *Ad* 2. *Necessity.* Suppose $Ha = Hb$. Then, as $a \in Ha$, it must be that $a \in Hb$, i.e. there must exist $h \in H$ such that $a = hb$. Multiplying by $b^{-1} \in G$ on the right gives us $ab^{-1} = h$. As $h \in H$, also must be $ab^{-1} \in H$.

Ad 2. *Sufficiency.* Suppose $ab^{-1} \in H$. Then, all elements of Hb are of the form hb as h ranges all over H. So, h also must equal, in one of the cases, $ab^{-1} \in H$. Therefore, for one of these cases, for $x \in Hb$, we have $x = ab^{-1}b = a$. And, as $x \in Hb$ and $x = a$ we have $a \in Hb$, and by a previous proposition, $Ha = Hb$. *Necessity.* Suppose $Ha = Hb$. Then, we can take $ha \in Ha$ such that $ha = h_1 b$ for some $h_1 b \in H$. Multiplying by b^{-1} on the right gives us $h_1 = hab^{-1}$. Also, if we multiply by h^{-1} on the left we have $h^{-1}h_1 = ab^{-1}$. As H is a subgroup, and as $h, h_1 \in H$, we have $h^{-1}h_1 \in H$, i.e. $ab^{-1} \in H$.

Ad 3. If we take $h \in H$, then $h = he$. And, as $h \in H$ and $e \in G$, we have $h \in He$. Therefore, $H \subseteq He$. Conversely, if we take $h \in He$, then there exists $h' \in H$ such that $h = h'e$, but that means that $h' = h$ and $h \in H$. So, $He \subseteq H$ and $H = He$.

Ad 4. By taking $b = e$ in (1) and applying (3), the statement is proved by simple substitution in both directions.

Ad 5. Take $(ab)h \in (ab)H$. For each $h \in H$ there exists $h_1 \in H$ such that $bh = h_1 b$ (as $bH \subseteq Hb$). So we have $abh = ah_1 b$. Also, for every $h \in H$ there exists $h_2 \in H$ such that $ah = h_2 a$ (as $aH \subseteq Ha$). As our choice of h was arbitrary we could take $h = h_1$ so we have $ah_1 = h_2 a$, specifically. From $abh = ah_1 b$ we have $abh = h_2 ab$, i.e. for each $h \in H$ there exists $h_2 \in H$ such that $(ab)h = h_2(ab)$; in other words, for each $(ab)h \in (ab)H$ there exists $h_2(ab) \in H(ab)$ such that $(ab)h = h_2(ab)$. From that we have $(ab)H \subseteq H(ab)$. Similarly, take $h(ab) \in H(ab)$. For each $h \in H$ there exists $ha \in Ha$ and $h_1 \in H$ such that $ha = ah_1$. So we have $hab = ah_1 b$. But, for every $h \in H$ there exists $hb \in Hb$ and $h_3 \in H$ such that $hb = bh_2$. As our choice of h was arbitrary, again, we can take $h = h_1$ specifically and have $h_1 b = bh_2$. From that we get $hab = abh_2$, i.e. for each $h(ab) \in H(ab)$ there exists $(ab)h_2 \in H$ such that $h(ab) = (ab)h_2$. In other words, $H(ab) \subseteq (ab)H$. From that and previous relation we have $(ab)H = H(ab)$.

Ad 6. For each $h \in H$ there exist $h_1, h_2 \in H$ such that $ah = h_1 a$ and $ha = ah_2$. Multiplying first equation by a^{-1} on the left and on the right yields $ha^{-1} = a^{-1}h_1$, and multiplying second equation by a^{-1} on the left and on right gives us $a^{-1}h = h_2 a^{-1}$. Therefore, as for each $h \in H$ there exist $h_1, h_2 \in H$ such that $ha^{-1} = a^{-1}h_1$ and $a^{-1}h = h_2 a^{-1}$, we have $a^{-1}H = Ha^{-1}$.

Ad 7. Let $a, b, c \in G$ such that $(ab)H = (ac)H$. If we take $(ab)h \in (ab)H$, then there exists $h_1 \in H$ such that $abh = ach_1$. Multiplying by a^{-1} on the left gives us

$bh = ch_1$. Similarly, if we take $(ac)h \in H$, there exists $h_2 \in H$ such that $ach = abh_2$ and multiplying on the left by a^{-1} gives us $ch = bh_2$. Therefore, for each $bh \in bH$ there exists $ch_1 \in cH$ such that $bh = ch_1$ (giving $bH \subseteq cH$) and for each $ch \in cH$ there exists $bh_2 \in bH$ such that $ch = bh_2$ (giving $cH \subseteq bH$). That implies that $bH = cH$.

Ad 8. Let $\mathcal{H}_L = \{xH : \ x \in G\}$ and $\mathcal{H}_R = \{Hx : \ x \in G\}$. We define a mapping $f : \mathcal{H}_L \to \mathcal{R}$ with $f(xH) = Hx$. Obviously, f is defined for each xH. But, is it uniquely defined? Suppose $x_1H = x_2H$. Then, for each $h \in H$ there exists $h_1 \in H$ such that $x_1h = x_2h_1$. Multiplying by x_1^{-1} on the left and h_1^{-1} on the right gives us $hh_1^{-1} = x_1^{-1}x_2$. That is equivalent to $(h_1^{-1}h)^{-1} = (x_1x_2^{-1})^{-1}$. Multiplying by $x_1x_2^{-1}$ on the right and by h_1h on the left gives us $x_1x_2^{-1} = h_1^{-1}h$. As $h_1^{-1}h \in H$ (as H is a subgroup of G), we have that $x_1x_2^{-1} \in H$, and by a previous problem $Hx_1 = Hx_2$, which is $f(x_1H) = f(x_2H)$. Therefore, f is a function. Now we will prove that it is a bijection. *Injectivity.* Suppose $f(x_1H) = f(x_2H)$, i.e. $Hx_1 = Hx_2$. By a previous problem we have $x_1x_2^{-1} \in H$. That means that there exists $h \in H$ such that $h = x_1x_2^{-1}$. Multiplying by h^{-1} on the left and $(x_1x_2^{-1})^{-1}$ on the right gives us $\left(x_1x_2^{-1}\right)^{-1} = h^{-1}$, i.e. $x_1^{-1}x_2 = h^{-1}$. That means that $x_1^{-1}x_2 \in H$. That means that for some $x_1h_1 \in x_1H$ we have $x_1h_1 = x_1x_1^{-1}x_2$, that is $x_1h = x_2$, which implies that $x_2 \in x_1H$ and $x_1H = x_2H$. *Surjectivity.* Trivial. If we take $Hx \in \mathcal{H}_R$, there exists $xH \in \mathcal{H}_L$ such that $f(xH) = Hx$. Therefore, f is bijective and $|\mathcal{H}_L| = |\mathcal{H}_R|$.

□

Remark. From considerations from above we also have some interesting properties. E.g. if H is a subgroup of G and $a, b \in G$, then $Ha = Hb$ if and only if $aH = bH$.

Proposition. Let G be a group and J, K and H subgroups of G such that $J = K \cap H$. Then for any $a \in G$, $Ja = Ha \cap Ka$.

Proof. Let $a \in G$. If we take $ja \in Ja$, we also have $j \in J = K \cap H$. That means that $j \in K$ and $j \in H$. If we observer Ha and Ka, then as a ranges over all elements of H and K it will also be that $ja \in Ha$ and $ja \in Ka$, i.e. $ja \in Ha \cap Ka$. Thus we have $Ja \subseteq Ha \cap Ka$. Now, if we take $xa \in Ha \cap Ka$, then $xa \in Ha$, i.e. $x \in H$, and $xa \in Ka$, that is $x \in K$. That means that $x \in H \cap K = J$ and $x \in J$. As $x \in J$ it will also be that $xa \in Ja$ which implies $Ha \cap Ka \subseteq Ja$. That implies that $Ja = Ha \cap Ka$.

□

Remark. From the previous proposition follows that if H and K are of finite index in G, then their intersection $H \cap K$ is also of finite index in G.

Definition. If $a \in G$, a **conjugate** of a is any element of the form xax^{-1}, where $x \in G$.

Proposition. Let G be a group. Relation $\sim\colon G^2 \to \{\top, \bot\}$ defined for all $a, b \in G$ as $a \sim b$ if and only if $a = xbx^{-1}$, for some $x \in G$ is an equivalence relation on G.

Proof. *Reflexivity.* $a \sim a$ holds as $a = eae^{-1}$. *Simmetry.* $a \sim b$ implies that there exists $x \in G$ such that $a = xbx^{-1}$. Multiplying by x on the right and x^{-1} on the left yields $x^{-1}ax = b$, so $b \sim a$ (note that if we took $y = x^{-1}$ we would have $yay^{-1} = b$, the possible confusion arises only in perceived ambiguity of an element and its inverse). *Transitivity.* $a \sim b$ and $b \sim c$ implies $a = xbx^{-1}$ and $b = ycy^{-1}$, for some $x, y \in G$. Substituting ycy^{-1} for b in xbx^{-1} gives us $a = xycy^{-1}x^{-1}$. But, as $(xy)^{-1} = y^{-1}x^{-1}$, we have $a = (xy)c(xy)^{-1}$. Of course, G is a group, so $xy \in G$, and their inverse also.

□

Definition. Let $a \in G$ and $\sim$ a relation on G such that $a \sim b$ if and only if $a = xbx^{-1}$ for some $x \in G$. **Conjugacy class** of a is $[a]_c = \{xax^{-1} : \ x \in G\}$.

Definition. For any element $a \in G$, the **centralizer** of a, denoted by C_a, is the set of all the elements in G which commute with a. That is,

$$C_a = \{x \in G : \ xa = ax\} = \{x \in G : \ xax^{-1} = a\}.$$

Proposition. For any $a \in G$, C_a is a subgroup[52] of G.

Proof. By definition, $C_a \subseteq G$. Take $a \in G$. Then, if we take $x, y \in C_a$, we have $a = xax^{-1}$ and $a = yay^{-1}$. Substituting the former into the latter expression we have $a = xyay^{-1}x^{-1}$ and that is, by the same reasoning as in the previous proposition, equivalent to $a = (xy)a(xy)^{-1}$, i.e. $xy \in C_a$. Then, if we take $x \in C_a$ we have $a = xax^{-1}$. Multiplying that by x on the right and $x^{-1} \in G$ on the left we have $x^{-1}ax = a$, so $x^{-1} \in C_a$ and C_a is a subgroup of G.

□

Lemma. Let G be a group, $a \in G$ and C_a centralizer of a. Then the following statements are equivalent:

1. $x^{-1}ax = y^{-1}ay$;
2. $xy^{-1}a = axy^{-1}$;

[52] In chapter on subgroups we have proved that the center of G is a subgroup of G. But note the difference of *center* and *centralizer*. Center of a group is the set of all elements which commute with all other elements in G while the centralizer needs a fixed element $a \in G$ to be defined and then it is a set of all elements which commute with a.

3. $xy^{-1} \in C_a$;

4. $C_a x = C_a y$.

Proof. From $x^{-1}ax = y^{-1}ay$ we get an equivalent expression (when multiplying by x on the left and y^{-1} on the right) $xy^{-1}a = axy^{-1}$ and that implies, as a commutes with xy^{-1}, that $xy^{-1} \in C_a$. Conversely, $xy^{-1} \in C_a$ implies that a commutes with xy^{-1} and we have $xy^{-1}a = axy^{-1}$. Now, assume $xy^{-1} \in C_a$. Then, it must be that $xy^{-1}y \in C_a y$, i.e. $x \in C_a y$. From a previous theorem it follows that $C_a x = C_a y$. Conversely, if $C_a x = C_a y$, then it must be that, $x \in C_a x$ (as $e \in C_a$ and $x = ex$). But, also $x \in C_a y$ (as $C_a x = C_a y$). As $x \in C_a y$ it is of the form $x = cy$, where $c \in C_a$, i.e. c commutes with a. That means that $ca = ac$. As we have $x = cy$, by multiplying with y^{-1} on the right we have $xy^{-1} = c$. Then, as $ca = ac$, it follows that $xy^{-1}a = axy^{-1}$. From this point it implies all the equivalences it is tied to.

□

Lemma. Let G be a group and $a \in G$. There is a one-to-one correspondence between the set of all the conjugates of $a \in G$ and the set of all the cosets of C_a in G.

Proof. Let $[a]_c$ be the set of all the conjugates of $a \in G$ (i.e. induced by forementioned equivalence relation) and $\mathcal{C}_a$ family of sets containing all the cosets of C_a, that is $\mathcal{C}_a = \{C_a x : \ x \in G\}$. Let $f : [a]_c \to \mathcal{C}_a$ be a mapping defined with $f(xax^{-1}) = C_a x$. It is obvious that this is a function as it is defined for all x, and it has the property of uniqueness, as $xax^{-1} = yay^{-1}$ would imply, by a previous proposition, that $C_a x^{-1} = C_a y^{-1}$, i.e. $f(xax^{-1}) = f(yay^{-1})$. Now, we will prove that it is a bijection. *Injectivity.* Suppose $f(xax^{-1}) = f(yay^{-1})$. That means that $C_a x^{-1} = C_a y^{-1}$ and by a previous proposition that $xax^{-1} = yay^{-1}$. *Surjectivity.* Let $C_a x \in \mathcal{C}_a$. Obviously, as $x \in G$, and $[a]_c$ is a class, it must contain xax^{-1}. Therefore, there exists $xax^{-1} \in [a]_c$ such that $f(xax^{-1}) = C_a x$. Thus, f is a bijection.

□

Lemma. Let G be a group. Then, $|[a]_c| = [G : C_a]$.

Proof. From a previous lemma we have a bijection from $[a]_c$ to $\mathcal{C}_a$. Therefore, $|[a]_c| = |\mathcal{C}_a|$. But $|\mathcal{C}_a|$ is the number of all the different cosets of C_a in G, i.e. index of C_a in G. So, by definition, $|\mathcal{C}_a| = [G : C_a]$.

□

Theorem. Let G be a group. The size of every conjugacy class is a factor of $|G|$.

Proof.. Let $a \in G$. By definition of index of C_a (centralizer of a) in G:

$$[G : C_a] = \frac{|G|}{|C_a|}.$$

Multiplying by $|C_a|$ gives us $|G| = |C_a| \cdot [G : C_a]$. But, by a previous lemma we have $|[a]_c| = [G : C_a]$, so $|G| = |C_a| \cdot |[a]_c|$, i.e. $|[a]_c|$ divides $|G|$. Our choice of a was arbitrary so the statement of the theorem is proved.

□

Definition. Let A be a set, and G a subgroup of S_A (group of all the permutations of A). We say that G is a **group acting on the set** A.

Definition. Let G be a finite group acting on a set A. If $a \in A$, then the **orbit** of a, with respect to G, is the set[53]:

$$O(a) = \{g(a) \in A : \ g \in G\}.$$

Definition. Let G be a group acting on a set A. The **stabilizer** of $a \in A$, with respect to G, is the set $G_a = \{g \in G : \ g(a) = a\}$.

Proposition. Let G be a group acting on a set A. $\sim$ be a relation on A defined as $a \sim b$ iff $g(a) = b$, for some $g \in G$. Then, $\sim$ is an equivalence relation on A, and orbits are its equivalence classes.

Proof. *Reflexivity.* Note that $e \in G$ and $e(a) = a$, for all $a \in G$. Therefore, we have $a \sim a$. *Symmetry.* From $a \sim b$ we have $g(a) = b$, for some $g \in G$. But, as $g : A \to A$ is a bijection, it has an inverse $g^{-1} \in G$. So we have $[g^{-1} \circ g](a) = g^{-1}(b)$. From definition of inverse we have $[g^{-1} \circ g](a) = a$, for all $a \in G$. So, we have $g^{-1}(b) = a$ and $b \sim a$. *Transitivity.* From $a \sim b$ and $b \sim c$ we have $g(a) = b$ and $f(b) = c$ for some $f, g \in G$. From that we have $f(g(a)) = c$, i.e. $[f \circ g](a) = c$. As G is a group, and $f, g \in G$, so is $[f \circ g] \in G$ and we have $a \sim c$. Let us observe equivalence classes. We have $[a] = \{b \in A : \ a \sim b\} = \{b \in A : \ (\exists g \in G)(g(a) = b)\} = \{g(a) \in A : \ g \in G\} = O(a)$.

□

[53]Recall that permutation is a bijection with equal domain and codomain, so if $g \in G \subseteq S_a$, then $g : A \to A$ and $g(x) \in A$ for all $x \in A$.

Proposition. Let G be a group acting on a set A and G_a stabilizer of $a \in A$. Then, G_a is a subgroup of G.

Proof. Obviously $G_a \subseteq G$. If we take $f, g \in G_a$ then $f(a) = a$ and $g(a) = a$. Taking their composition gives us $f(g(a)) = a$, i.e. $[f \circ g](a) = a$. So it must be that $[f \circ g] \in G_a$. If we take $g \in G$, then $g(a) = a$. As g is a bijection it has an inverse $g^{-1} \in G$ and it must be that $[g^{-1} \circ g](a) = g^{-1}(a)$, that is $g^{-1}(a) = a$. So it must be that $g^{-1} \in G_a$. Thus, G_a is a subgroup of G.

□

Proposition. Let G be a group acting on a set A, $a \in A$ and $f, g \in G$. Then, $f, g \in xG_a$, for some $x \in G$, if and only if $f(a) = g(a)$.

Proof. *Necessity.* Let $f, g \in xG_a$. That means that $f = [x \circ f']$ and $g = [x \circ g']$, for some $f', g' \in G_a$. As $x \in G$ it has an inverse $x^{-1} \in G$, so we have $[x^{-1} \circ f] = f'$ and $[x^{-1} \circ g] = g'$. And, as $f'(a) = a$ and $g'(a) = a$ we have $a = f'(a) = [x^{-1} \circ f](a)$ and $a = g'(a) = [x^{-1} \circ g](a)$. That implies that $x(a) = f(a)$ and $x(a) = g(a)$. Finally, from that follows $f(a) = g(a)$. *Sufficiency.* Obviously, $f \in fG_a$. Suppose $f(a) = g(a)$ for some $f, g \in G$. Applying $f^{-1} \in G$ gives us $a = [f^{-1} \circ g](a)$ and by definition $[f^{-1} \circ g] \in G_a$. So, it must be that $[f \circ [f^{-1} \circ g]] \in fG_a$. As function composition is associative, we have $g \in fG_a$, i.e. there exists $x \in G$ (here $x = f$) such that $f, g \in xG_a$.

□

Proposition. Let G be a group acting on a set A and $a \in A$. Then, $|O(a)| = [G : G_a]$.

Proof. Let $\mathcal{G}_a = \{xG_a : \ x \in G\}$ be a family of left cosets of G. We know that the number of left and right cosets of any group is equal, so this particular choice of left cosets is of no importance. Let $f : O(a) \to \mathcal{G}_a$ be a mapping with $f(x(a)) = xG_a$. Mapping is obviously defined for all $x(a) \in O(a)$, where $x \in G$. Assume $x(a) = y(a)$. Then, there exists $b \in A$ such that $x(a) = b$ and $y(a) = b$. Obviously $x \in xG_a$. Now, as we have $a = x^{-1}(b)$, and $y(a) = b$, we have $a = x^{-1}(y(a))$, i.e. $[x^{-1} \circ y](a) = a$, meaning $x^{-1}y \in G_a$. By a previous proposition, $xG_a = yG_a$. *Injectivity.* Suppose $xG_a = yG_a$. Then, by a previous proposition, $x^{-1}y \in G_a$, i.e. $[x^{-1} \circ y](a) = a$. From that we have $y(a) = x(a)$. *Surjectivity.* Suppose $yG_a \in \mathcal{G}$. As $y \in G$, we have $y(a) = b$, for some $b \in A$. Thus, $y(a) \in O(a)$ and we can have $f(y(a)) = yG_a$. Thus, f is bijective and $|O(a)| = |\mathcal{G}_a|$ where $\mathcal{G}_a = [G : G_a]$.

□

Corollary. Size of every orbit with respect to G is a factor of the order of G.

Proof. Let $a \in A$, $O(a)$ orbit of a with respect to G and G_a stabilizer of a. As G_a is a subgroup of G, its index in G is $[G : G_a] = \frac{|G|}{|G_a|}$. From that we have $[G : G_a] \cdot |G_a| = |G|$. As $|O(a)| = [G : G_a]$ by a previous proposition, we have $|O(a)| \cdot |G_a| = |G|$, which implies that the size of $O(a)$ is a factor of the order of G.

□

Corollary. If $f \in S_A$, then the length of each cycle of f is a factor of the order of $f \in S_A$.

Proof. Let $f \in S_A$ be a permutation decomposed in disjoint cycles $f_1, \ldots, f_n$ such that $f = f_1 f_2 \cdots f_n$ and let each have length $l(i)$, for $i \in \{1, \ldots, n\}$. Also, let m be the order of $f \in S_A$. Let us observe $\langle f \rangle$ and some cycle f_i which does not leave $a \in A$ fixed. Then, $O(a) = \{a, f_i(a), f_i^2(a), \ldots, f_i^{l(i)-1}(a)\}$. There are no other elements in $O(a)$ as f is decomposed in disjoint cycles, all other f_j, $i \neq j$, leave a fixed and copied into a. Therefore, the size of the orbit of a, which is not left fixed by f_i, is equal to the length of the cycle f_i. By a previous proposition it follows that size of the orbit of a is a factor of the order of $\langle f \rangle$, i.e. length of cycle f_i is a factor of the order of $f \in S_A$ (as the order of $\langle f \rangle$ is equal to order of f, by definition).

□

Remark. Lagrange's theorem can be proved using the orbit-stabilizer theorem, using only group actions and the fact that $Hg = H$ if and only if $g \in H$.

Lemma. Let G be a group, $H \leq G$ and $a, g \in G$. Then, $H(ga) = Ha$ if and only if $Hg = H$.

Proof. *Necessity.* If we take $x \in Hg$, then there exists $h_1 \in H$ such that $x = h_1 g$. But, as $h_1 \in H$ and $H(ga) = Ha$, there exists $h_2 \in H$ such that $h_1 ga = h_2 a$. That implies, after multiplying by a^{-1} on the right, that $h_1 g = h_2$ and $x = h_1 g = h_2$. Thus, $Hg \subseteq H$. If we take $x \in H$, then there exists $h_1 \in H$ such that $x = h_1$. But, then there exists $h_2 \in H$ such that $h_1 a = h_2 ga$. That implies, again, $h_1 = h_2 g$. So, $x = h_1 = h_2 g$ and $x \in Hg$. From that we get $H \subseteq Hg$. Combining that with former result, we have $H = Hg$.

Sufficiency. If $Hg = H$, then for all $h \in H$ there exists $h' \in H$ such that $hg = h'$. But, multiplying that by a on the right gives us that for all $h \in H$ there exists $h' \in H$ such that $hga = h'a$. So, $Hg \subseteq H$. Also, for all $h \in H$, there exists $h' \in H$ such that $h'g = h$, i.e. $h'ga = ha$. So, as for all $h \in H$ there exists $h' \in H$ such that $h'ga = ha$, then $H(ga) \subseteq Ha$. Thus, $H(ga) = Ha$.

□

Theorem (Lagrange). If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Proof. Let G/H be the set of all cosets of H in G. Let G act on G/H so that $g.Ha = H(ga)$. Then, $g \in \mathrm{Stab}_G(Ha)$ if and only if $g.Ha = Ha$. So, it must be $H(ga) = Ha$. Previous lemma tells us that that is equivalent to $Hg = H$. That is, furthermore equivalent to $g \in H$. Therefore, $g \in \mathrm{Stab}_G(Ha)$ if and only if $g \in H$. That is equivalent to $\mathrm{Stab}_G(Ha) = H$. Now, observe that $\mathrm{Orb}_G(Ha) = \{Hb \in G : (\exists g \in G)(g.Ha = Hb)\}$. That implies $\mathrm{Orb}_G(Ha) \subseteq G/H$. But, if we take $Hb \in G/H$, then we want to find $g \in G$ such that $g.Ha = Hb$, i.e. $H(ga) = Hb$. Therefore, we want $ga = b$. After multiplying by a^{-1} on the right, we get $g = ba^{-1}$. So, $(ba^{-1}).Ha = H((ba^{-1})a) = H(b(a^{-1}a)) = H(be) = Hb$. Therefore, $Hb \in \mathrm{Orb}_G(Ha)$ and $G/H \subseteq \mathrm{Orb}_G(Ha)$. That, and the previous result, gives us $\mathrm{Orb}_G(Ha) = G/H$. Using the orbit stabilizer theorem, we get $|G| = |\mathrm{Orb}_G(Ha)| \cdot |\mathrm{Stab}_G(Ha)|$, which is equivalent to $|G| = |G/H| \cdot |H|$. From that we have that $|H|$ divides $|G|$. Similarly, as $|G/H| = [G : H]$ we obtain $|G| = [G : H] \cdot |H|$, i.e. $[G : H] = \frac{|G|}{|H|}$.

□

Homomorphisms

Definition. Let G and H be groups. Function $f : G \to H$ is called a **homomorphism**[54] from G to H if $f(ab) = f(a)f(b)$, for all $a, b \in G$. Then, H is called a **homomorphic image** of G.

Theorem. Let G and H be groups, and f a homomorphism from G to H. Then:

1. $f(e) = e$, where e is a neutral element in H (on the right-hand side) and a neutral element in G (on the left-hand side);
2. $f\left(a^{-1}\right) = [f(a)]^{-1}$, for all $a \in G$.

Proof. *Ad* 1. We have that $f(ab) = f(a)f(b)$, for all $a, b \in G$. If we take $f(ee) = f(e)f(e)$, we have $f(e) = f(e)f(e)$. As $f(e) \in H$, and H is a group, there exists $[f(e)]^{-1} \in H$ such that $[f(e)]^{-1}f(e) = e'$, where e' is a neutral element in H. So, we multiply equation by $[f(e)]^{-1}$ on the left and we have $e' = f(e)$. But, due to this property, it will be unambiguous if we use e to represent neutral element in G and in H. Therefore, $f(e) = e$.

Ad 2. As $aa^{-1} = e$, for all $a \in G$, we have $f(aa^{-1}) = f(a)f(a^{-1})$, i.e. $f(e) = f(a)f(a^{-1})$. From previous property we have $f(e) = e$, so we have $e = f(a)f(a^{-1})$. As $f(a) \in H$, and H is a group, we can multiply the former equation by $[f(a)]^{-1} \in H$ on the left to get $[f(a)]^{-1} = [f(a)]^{-1}f(a)f(a^{-1})$, i.e. $[f(a)]^{-1} = f(a^{-1})$.

□

Definition. Let $f : G \to H$ be a homomorphism from group G to group H. Then, the **kernel** of f is the set:

$$\ker(f) = \{a \in G : \ f(a) = e\}.$$

The **range** of f is the set:

$$\operatorname{ran}(f) = \{f(a) \in H : \ a \in G\}.$$

Definition. Let G be a group and H a subgroup of G. If $xyx^{-1} \in H$, for all $y \in H$ and $x \in G$, then H is called a **normal subgroup** of G.

Remark. Notice that a normal subroup of G is any nonempty subset of G, with

[54] Notice that the only difference from isomorphism is that we do not require f to be a bijection. Every isomorphism is therefore homomorphism.

operation inherited from G, which is closed with respect to multiplication, inverses and conjugates.

Theorem. Let $f : G \to H$ be a homomorphism. Then:

1. $\ker(f)$ is a normal subgroup of G;
2. $\text{ran}(f)$ is a subgroup of H.

Proof. *Ad* 1. Obviously $\ker(f) \subseteq G$, by definition. If we take $a, b \in \ker(f)$ we have $f(a) = e$ and $f(b) = e$. Multiplying first equation by $f(b)$ gives us $f(a)f(b) = ef(b)$. But, as $f(b) = e$, we have $f(a)f(b) = ee$, i.e. $f(a)f(b) = e$. As f is a homomorphism, we have $f(a)f(b) = f(ab)$, which, from $f(a)f(b) = e$, implies $f(ab) = e$. Therefore, it must be that $ab \in \ker(f)$ and $\ker(f)$ is closed with respect to products. Now, take $a \in \ker(f)$. We have $f(a) = e$. If we multiply equation by $[f(a)]^{-1}$, we have $f(a)[f(a)]^{-1} = [f(a)]^{-1}$, which further yields $[f(a)]^{-1} = e$. But, by a previous theorem, $[f(a)]^{-1} = f(a^{-1})$, so we have $f(a^{-1}) = e$ and it must be that $a^{-1} \in \ker(f)$. So, $\ker(f)$ is closed with respect to inverses. Finally, if we take $x \in G$ and $y \in \ker(f)$ we need to show that $xyx^{-1} \in \ker(f)$. As f is a homomorphism, we have $f(xyx^{-1}) = f(x)f(yx^{-1}) = f(x)f(y)f(x^{-1})$. But, as $f(y) = e$ and $f(x^{-1}) = [f(x)]^{-1}$ by a previous theorem, we have $f(xyx^{-1}) = f(x)e[f(x)]^{-1} = f(x)[f(x)]^{-1} = e$. As $f(xyx^{-1}) = e$, it must be that $xyx^{-1} \in \ker(f)$. To conclude, $\ker(f)$ is a normal subgroup of G.

Ad 2. We have, by definition, $\text{ran}(f) \subseteq H$. If we take $f(a), f(b) \in \text{ran}(f)$, as f is a homomorphism we have $f(a)f(b) = f(ab)$, so $f(ab) \in \text{ran}(f)$ and by that $f(a)f(b) \in \text{ran}(f)$. For $f(a) \in \text{ran}(f)$ we have $[f(a)]^{-1} \in H$ such that $f(a)[f(a)]^{-1} = [f(a)]^{-1}f(a) = e$. But, by a previous theorem $[f(a)]^{-1} = f(a^{-1})$, so $f(a^{-1}) \in \text{ran}(f)$, and by that $[f(a)]^{-1} \in \text{ran}(f)$. Thus, $\text{ran}(f)$ is a subgroup of H.

□

Problem. Verify that $f : \mathbb{Z}_8 \to \mathbb{Z}_4$, given by

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{pmatrix}$$

is a homomorphism. Find $\ker(f)$ and all the cosets of $\ker(f)$.

Solution. First we will write the table of $\mathbb{Z}_8$:

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Now, as we transform the table using the definition of f we have:

$+$	0	1	2	3	0	1	2	3
0	0	1	2	3	0	1	2	3
1	1	2	3	0	1	2	3	0
2	2	3	0	1	2	3	0	1
3	3	0	1	2	3	0	1	2
0	0	1	2	3	0	1	2	3
1	1	2	3	0	1	2	3	0
2	2	3	0	1	2	3	0	1
3	3	0	1	2	3	0	1	2

From the table above we can see that last four rows are identical to first four rows; the same thing with columns. Therefore, we can eliminate duplicate information to get:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The table above is exactly the table of $\mathbb{Z}_4$. Therefore, f is a homomorphism from $\mathbb{Z}_8$ to $\mathbb{Z}_4$. Let us find its kernel. Kernel is of course the set containing all elements which are sent to a neutral element, in this case, zero. Thus, $\ker(f) = \{a \in \mathbb{Z}_8 : \ f(a) = 0\} = \{0, 4\}$. It is easy to notice that it is a subgroup of $\mathbb{Z}_8$ with the following table:

$+_8$	0	4
0	0	4
4	4	0

The cosets of $\ker(f)$ are (we will use notation for addition):

$$\begin{aligned}
\ker(f) + 0 &= \{0, 4\} = \ker(f) + 4 = \ker(f), \\
\ker(f) + 1 &= \{1, 5\} = \ker(f) + 5, \\
\ker(f) + 2 &= \{2, 6\} = \ker(f) + 6, \\
\ker(f) + 3 &= \{3, 7\} = \ker(f) + 7.
\end{aligned}$$

Problem. Prove that $f : \mathbb{Z} \to \{E, O\}$, given by $f(x) = E$ if x is even, and $f(x) = O$ if x is odd, is a homomorphism. Find $\ker(f)$ and all the cosets of $\ker(f)$. The table of $\{E, O\}$ is:

$+$	E	O
E	E	O
O	O	E

Solution. We need only to check if $f(a+b) = f(a) + f(b)$. Suppose a and b are odd. Then, their sum is even. If a is odd and b is even, their sum is odd. Same thing if a is even and b is odd. If a and b are even, their sum is even. We can see that this really corresponds to the table above and we have $f(a+b) = f(a) + f(b)$. Therefore, f is a homomorphism from $\mathbb{Z}$ to $\{E, O\}$. Neutral element in $\{E, O\}$ is evidently E. Therefore, $\ker(f) = \{n \in \mathbb{Z} : \ f(n) = E\} = \{2n : \ n \in \mathbb{Z}\}$. There are two cosets of $\ker(f)$:

$$\begin{aligned} \ker(f) + 0 &= \ker(f) + 2 = \ldots = \ker(f) + 2k = \ker(f), \\ \ker(f) + 1 &= \ker(f) + 3 = \ldots = \ker(f) + 2(k+1). \end{aligned}$$

Problem. Let G be the multiplicative group of all 2×2 matrices A satisfying $\det A \neq 0$. Prove that $f : G \to \mathbb{R}^{ast}$ with $f(A) = \det A$ is a homomorphism and describe its kernel.

Solution. Determinant is defined for all 2×2 matrices and returns a unique value. We only need to check if $f(AB) = f(A)f(B)$. We have $f(AB) = \det AB$. But, due to Binet-Cauchy theorem, $\det AB = \det A \det B$. Thus, $f(AB) = \det AB = \det A \det B = f(A)f(B)$ and f is a homomorphism from G to $\mathbb{R}^*$. Neutral element in $\mathbb{R}^*$ is 1. Therefore, $\ker(f) = \{A \in G : \ \det A = 1\}$, i.e. all orthogonal matrices.

Problem. Prove that each of the following[55] is a homomorphism and describe its kernel:

1. $\phi : \mathcal{F}(\mathbb{R}) \to \mathbb{R}$ with $\phi(f) = f(0)$;
2. $\phi : \mathcal{D}(\mathbb{R}) \to \mathcal{F}(\mathbb{R})$ with $\phi(f) = f'$;
3. $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ with $f(x, y) = x + y$;

[55]Keep in mind that $\mathcal{F}(\mathbb{R}) := (\mathcal{F}(\mathbb{R}), +)$, group of all real functions with real variables under addition. Similarly, $\mathcal{C}(\mathbb{R}) := (\mathcal{C}(\mathbb{R}), +)$, containing continuous functions and $\mathcal{D}(\mathbb{R}) := (\mathcal{D}(\mathbb{R}), +)$ containing differentiable functions.

4. $f : \mathbb{R}^* \to \mathbb{R}^+$ with $f(x) = |x|$;

5. $f : \mathbb{C}^* \to \mathbb{R}^+$ with $f(a + bi) = \sqrt{a^2 + b^2}$.

Solution.

1. $\phi : \mathcal{F}(\mathbb{R}) \to \mathbb{R}$ *with* $\phi(f) = f(0)$. All functions in $\mathcal{F}(\mathbb{R})$ are of the form $f : \mathbb{R} \to \mathbb{R}$, therefore they are defined in $f(0)$ and then so is $\phi(f)$. Now we have $\phi(f + g) = [f + g](0) = f(0) + g(0) = \phi(f) + \phi(g)$ and ϕ is a homomorphism from $\mathcal{F}(\mathbb{R})$ to $\mathbb{R}$. Remember that 0 is the neutral element in $\mathbb{R}$. It's kernel is $\ker(\phi) = \{f \in \mathcal{F}(\mathbb{R}) : \ f(0) = 0\}$, that is, the set containing all functions passing through the origin $O(0, 0)$.

2. $\phi : \mathcal{D}(\mathbb{R}) \to \mathcal{F}(\mathbb{R})$ *with* $\phi(f) = f'$. Set $\mathcal{D}(\mathbb{R})$ contains all differentiable functions, therefore ϕ is defined for all $f \in \mathcal{F}(\mathbb{R})$. Derivation is unique. Now, we have $\phi(f + g) = [f + g]' = f' + g' = \phi(f) + \phi(g)$. It's kernel is $\ker(\phi) = \{f \in \mathcal{D}(\mathbb{R}) : f' = 0\} = \{f \in \mathcal{D}(\mathbb{R}) : \ f = c, \ c \in \mathbb{R}\}$, that is the set of all constant functions.

3. $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ *with* $f(x, y) = x + y$. Obviously f is a function as it is defined for all $(x, y) \in \mathbb{R}^2$ and returns a unique value. We need only $f((a, b) + (c, d)) = f(a + c, b + d) = a + c + b + d = a + b + c + d = f(a, b) + f(c, d)$, i.e. f is a homomorphism. Its kernel is $\ker(f) = \{(x, y) \in \mathbb{R}^2 : \ x = -y\}$.

4. $f : \mathbb{R}^* \to \mathbb{R}^+$ *with* $f(x) = |x|$. Again, f is a function. We have $f(ab) = |ab| = |a| \cdot |b| = f(a)f(b)$. Thus, f is a homomorphism. Now, $\ker(f) = \{x \in \mathbb{R}^* : \ |x| = 1\} = \{-1, 1\}$.

5. $f : \mathbb{C}^* \to \mathbb{R}^+$ *with* $f(a + bi) = \sqrt{a^2 + b^2}$. As f is a function we have:

$$\begin{aligned} f((a + bi)(c + di)) &= f((ac - bd) + i(bc + ad)) = \sqrt{(ac - bd)^2 + (bc + ad)^2} \\ &= \sqrt{a^2c^2 - 2acbd + b^2d^2 + b^2c^2 + 2bcad + a^2d^2} \\ &= \sqrt{a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2} \\ &= \sqrt{a^2(c^2 + d^2) + b^2(c^2 + d^2)} = \sqrt{(c^2 + d^2)(a^2 + b^2)} \\ &= \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} = f(a + bi)f(c + di). \end{aligned}$$

   Therefore, f is a homomorphism. It's kernel is $\ker(f) = \{z \in \mathbb{C}^* : \ |z| = 1\}$, which is a unit circle.

Proposition. Let G, H and K be groups. If $f : G \to H$ and $g : H \to K$ are homomorphisms, then $g \circ f : G \to K$ is a homomorphism.

Proof. We have already proved that $g \circ f$, defined as above, is a function. Further we have $f(ab) = f(a)f(b)$, for all $a, b \in G$. As $f(a), f(b) \in H$, and $g : H \to K$, we have $g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b))$. That is, for all $a, b \in G$, we have $[g \circ f](ab) = [g \circ f](a)[g \circ f](b)$, for all $a, b \in G$. Thus, $g \circ f : G \to K$ is a homomorphism.

□

Theorem. Let G and H be groups. Homomorphism $f : G \to H$ is injective if and only if $\ker(f) = \{e\}$.

Proof. *Necessity.* Let $f : G \to H$ be an injective homomorphism. Then, for all $x_1, x_2 \in G$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$. Let us observe the set $\ker(f) = \{x \in G : \ f(x) = e\}$. From a previous proposition we have $f(e) = e$, so we can write $\ker(f) = \{x \in G : \ f(x) = f(e)\}$. But, by using forementioned property of injectivity, from $f(x) = f(e)$ it follows $x = e$. Thus, we have $\ker(f) = \{x \in G : \ x = e\} = \{e\}$.

Sufficiency. Suppose $f : G \to H$ is a homomorphism and $\ker(f) = \{e\}$. Suppose $f(x_1) = f(x_2)$ for some $x_1, x_2 \in G$. Then, as $f(x_1), f(x_2) \in H$, and H is a group, $f(x_2)$ has an inverse $[f(x_2)]^{-1} \in H$. Therefore, we can multiply the equality with $[f(x_2)]^{-1}$ on the right to get $f(x_1)[f(x_2)]^{-1} = f(x_2)[f(x_2)]^{-1}$, i.e. $f(x_1)[f(x_2)]^{-1} = e$. From a previous proposition we have $[f(x_2)]^{-1} = f\left(x_2^{-1}\right)$. Therefore from $f(x_1)[f(x_2)]^{-1} = e$ we have $f(x_1)f\left(x_2^{-1}\right) = e$. As f is a homomorphism, we have $f(ab) = f(a)f(b)$ for all $a, b \in G$. So, from $f(x_1)f\left(x_2^{-1}\right) = e$ it follows that $f\left(x_1x_2^{-1}\right) = e$. But, $\ker(f)$ contains all $x \in G$ such that $f(x) = e$, so it must be $x_1x_2^{-1} \in \ker(f)$. But, there is only one element in $\ker(f) = \{e\}$ and because of that $x_1x_2^{-1} = e$. As $x_2^{-1} \in G$ and G is a group we can multiply equality by x_2 on the right and get $x_1 = x_2$. Therefore, f is injective.

□

Proposition. Let G and H be groups and $f : G \to H$ a homomorphism.

1. If K is a subgroup of G, then $f(K) = \{f(x) : \ x \in K\}$ is a subgroup of H.
2. If J is a subgroup of H, then $f^{-1}(J) = \{x \in G : \ f(x) \in J\}$ is a subgroup of G and $\ker(f) \subseteq f^{-1}(J)$.

Proof. *Ad* 1. By definition, $f(K) \subseteq H$. Then, if we take $u, v \in f(K)$, there must exist $x, y \in K$ (by definition of $f(K)$) such that $f(x) = u$ and $f(y) = v$. As K is a subgroup of G we have $xy \in K$, and as $u, v \in f(K) \subseteq H$, and H is a group, we have $uv \in H$, i.e. $f(x)f(y) \in H$. As f is a homomorphism, we have $f(xy) \in H$. So, as $xy \in K$ and $f(xy) \in H$, we have $f(xy) = uv \in f(K)$. Now, take $u \in f(K)$ and there

must exist $x \in K$ such that $f(x) = u$. From K being a subgroup of G, also $x^{-1} \in K$. As $u \in f(K) \subseteq H$ and H is a group, then $u^{-1} \in H$. We have $u^{-1} = [f(x)]^{-1} = f(x^{-1})$. So, from $x \in K$ and $f(x^{-1}) = u^{-1} \in H$, we have $u^{-1} \in f(K)$. So, $f(K)$ is a subgroup of H.

Ad 2. We have $f^{-1}(J) \subseteq G$ by definition. If we take $x, y \in f^{-1}(J) \subseteq G$, then $f(x), f(y) \in J$. As G is a group and $x, y \in G$, we have $xy \in G$. Also, as J is a subgroup of H, we have $f(x)f(y) \in J$, and as f is a homomorphism, $f(xy) \in J$. As $f(xy) \in J$ and $xy \in G$, then $xy \in f^{-1}(J)$. Take $x \in f^{-1}(J) \subseteq G$. Then, we have $f(x) \in J$. As G is a group and $x \in G$, we have $x^{-1} \in G$. As $f(x) \in J$ and J is a subgroup of H, we have $[f(x)]^{-1} \in J$, that is $f(x^{-1}) \in J$. So, from $f(x^{-1}) \in J$ and $x^{-1} \in G$, we have $x^{-1} \in f^{-1}(J)$. If we take $x \in \ker(f)$, then it must be $f(x) = e$. But, $e \in J$ (as it is a subgroup of H) and so it must be $f(x) \in J$. As $x \in \ker(f) \subseteq G$, i.e. $x \in G$ and $f(x) \in J$, we have $x \in f^{-1}(J)$. From that we have $\ker(f) \subseteq f^{-1}(J)$.

□

Proposition. Let G and H be groups. If $f : G \to H$ is a homomorphism and J is a subgroup of G, then we have $\ker(f_J) = J \cap \ker(f)$ (where f_J is a restriction of f to J).

Proof. Obviously f_J is a function as it is defined for all $x \in G$, and so for all $x \in J$. Also, uniqueness holds for all $x \in G$ and so for all $x \in J$. Restriction f_J is the same function as f up to domain. So, for all $x \in J$, $f_J(x) = f(x)$. Therefore, if $x, y \in J$, and J is a subgroup of G, we have $xy \in J$. So, $f_J(xy) = f(xy) = f(x)f(y) = f_J(x)f_J(y)$, i.e. $f_J : J \to H$ is a homomorphism. Let us take $x \in \ker(f_J)$. By definition we have $x \in J$, but also, as $f_J(x) = e$, we have $f_J(x) = f(x) = e$, so $x \in \ker(f)$. Therefore, as $x \in \ker(f_J)$ implies $x \in \ker(f)$ and $x \in J$, we have $\ker(f_J) \subseteq J \cap \ker(f)$. If we take $x \in J \cap \ker(f)$, then $x \in J$ and $x \in \ker(f)$. As $x \in \ker(f)$ we have $f(x) = e$ and, as $x \in J$, we have $f_J(x) = f(x) = e$, so it must be that $x \in \ker(f_J)$. As $x \in J \cap \ker(f)$ implies $x \in \ker(f_J)$, we have $J \cap \ker(f) \subseteq \ker(f_J)$ and by that (and a previous relation) we have $\ker(f_J) = J \cap \ker(f)$.

□

Proposition. Let G be a group.

1. The function $f : G \to G$ defined by $f(x) = e$ is a homomorphism.
2. $\{e\}$ and G are homomorphic images of G.

Proof. *Ad* 1. If we take $x, y \in G$, then we have $f(x) = e$ and $f(y) = e$. That multiplied

gives us $f(x)f(y) = e$. But, as G is a group, from $x, y \in G$, we have $xy \in G$. From that we have $f(xy) = e$, and combining that with $f(x)f(y) = e$ gives us $f(xy) = f(x)f(y)$, i.e. f is a homomorphism.

Ad 2. From previous example we have that $f : G \to G$, with $f(x) = e$, is a homomorphism. Then, $\text{ran}\,(f) = \{f(x) \in G : \ x \in G\}$. But, as $f(x) = e$, we only have $\text{ran}\,(f) = \{e\}$ (which is a trivial group; also by a previous proposition it is a subgroup of $\text{cod}\,(f) = G$). If we take $f : G \to G$ with $f(x) = x$, then it is easy to check that f is a homomorphism. From $x, y \in G$ we have $f(x) = x$ and $f(y) = y$. Those two expressions multiplied give us $f(x)f(y) = xy$. But, as $x, y \in G$, and G is a group, also $xy \in G$ and we have $f(xy) = xy$, by definition. So, $f(x)f(y) = xy = f(xy)$ and f is a homomorphism. Now, $\text{ran}\,(f) = \{f(x) \in G : \ x \in G\}$, but for all $x \in G$ we have $f(x) = x$, therefore $\text{ran}\,(f) = G$ and G is a homomorphic image of G; so is $\{e\}$.

□

Proposition. The function $f : G \to G$ defined by $f(x) = x^2$ is a homomorphism if and only if G is Abelian.

Proof. *Necessity.* Suppose f is a homomorphism. If we take $x, y \in G$, then, as G is a group, also $xy \in G$. By applying f we have $f(xy) = (xy)^2$. But, $f(xy) = f(x)f(y) = x^2y^2$. So, we have $(xy)^2 = x^2y^2$. From that we have $xyxy = xxyy$. If we multiply that equality with y^{-1} on the right and x^{-1} on the left, we have $yx = xy$. So, for all $x, y \in G$, it's $xy = xy$, which in turn implies that G is Abelian.

Sufficiency. Suppose G is Abelian. Then, for all $x, y \in G$, we have $xy = yx$, but also, by a previous proposition (we can obtain next equality by multiplying previous equality with x on the left and y on the right), that $(xy)^2 = x^2y^2$. So, we have $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$ and f is a homomorphism.

□

Proposition. The functions $f_1(x, y) = x$ and $f_2(x, y) = y$, from $G \times H$ to G and H, respectively, are homomorphisms.

Proof. First, $f_1 : G \times H \to G$, with $f_1(x, y) = x$. We have $f_1((x, y)(z, w)) = f_1(xz, yw) = xz = f_1(x, y)f_1(z, w)$. Therefore, f_1 is a homomorphism. Similarly, for $f_2 : G \times H \to H$, we have $f_2((x, y)(z, w)) = f_2(xz, yw) = yw = f_2(x, y)f_2(z, w)$.

□

Proposition. Every subgroup of an Abelian group is normal.

Proof. Let G be an Abelian group and H a subgroup of G. Let $y \in H$ and $x \in G$.

As $H \subseteq G$, we also have $y \in G$. As G is Abelian, we have $xy = yx$, for all $y \in H$ and $x \in G$. Multiplying that by $x^{-1} \in G$ on the left, we have $y = x^{-1}yx$. As $y \in H$ and $y = x^{-1}yx$, then $x^{-1}yx \in H$, for all $y \in H$ and $x \in G$. Thus, H is a normal subgroup.

□

Proposition. The center of any group G is a normal subgroup of G.

Proof. Center of a group G is the subgroup (as proved by a previous proposition) $C = \{x \in G : \ (\forall y \in G)\,(xy = yx)\}$. If we take $x \in C$, then $xy = yx$, for all $y \in G$. Multiplying $xy = yx$ on the right by $y^{-1} \in G$, we have $x = yxy^{-1}$. As $x \in C$, then also $yxy^{-1} \in C$, for all $x \in C$ (our choice of $x \in C$ was arbitrary) and for all $y \in G$. Therefore, center of an arbitrary group is a normal subgroup.

□

Proposition. Let G be a group and H a subgroup of G. H is normal if and only if for all $a, b \in G$, $ab \in H$ iff $ba \in H$.

Proof. *Necessity.* Assume H is normal. Then, for all $a, b \in G$ such that $ab \in H$ we have, as H is normal, $a^{-1}(ab)a \in H$, i.e. $ba \in H$. Also, for all $a, b \in G$ such that $ba \in H$, as H is normal, we have $b^{-1}(ba)b \in H$, which is equivalent to $ab \in H$.

Sufficiency. Suppose that H is a subgroup of G and that for all $a, b \in G$ it holds that if $ab \in H$ then $ba \in H$ and reverse. Take some $a \in G$ and $b \in H$. As $b = baa^{-1}$, we have $(ba)a^{-1} \in H$. It then follows that also $a^{-1}(ba) \in H$. That is, for all $a \in G$ and $b \in H$ we have $a^{-1}ba \in H$, which means that H is normal.

□

Proposition. Let H be a subgroup of G. H is normal if and only if $aH = Ha$, for all $a \in G$.

Proof. *Necessity.* Suppose H is normal. Take some $ah \in aH$, where $a \in G$ and $h \in H$. As H is normal and $a \in G$ and $h \in H$, we also have $aha^{-1} \in H$. That means that $aha^{-1}a \in Ha$, i.e. $ah \in Ha$. Therefore, $aH \subseteq Ha$. Now, take $ha \in Ha$. We have, as H is normal, that $a^{-1}ha \in H$ and from that $aa^{-1}ha \in aH$, i.e. $ha \in aH$. That means that, not only $aH \subseteq Ha$, but also $Ha \subseteq aH$ and from that $aH = Ha$.

Sufficiency. Suppose $aH = Ha$, for all $a \in G$. Then, if we take $ah \in aH$, we also have $ah \in Ha$, i.e. there exists $h' \in H$ such that $ah = h'a$. Multiplying that by a^{-1} on the right gives us $h' = a^{-1}ha$. As $h' \in H$, then $a^{-1}ha \in H$ also. Therefore, for all $h \in H$ and $a \in G$ we have $a^{-1}ha \in H$, i.e. H is normal.

□

Proposition. Any intersection of normal subgroups of G is a normal subgroup of G.

Proof. Suppose H_1 and H_2 are normal subgroups of G. Let us denote $H = H_1 \cap H_2$. Take any $a \in G$ and $h \in H$. Then, $h \in H_1$ and $h \in H_2$, and as H_1 and H_2 are normal, we also have $aha^{-1} \in H_1$ and $aha^{-1} \in H_2$. In other words, $aha^{-1} \in H_1 \cap H_2 = H$.

□

Proposition. Let G be a group and H a subgroup of G. If H has index 2 in G, then H is normal.

Proof. We have $[G : H] = 2$, which means that there are only two left and two right cosets of H. Therefore, as one of the cosets has to be $He = H$ (and $eH = H$), we have, in the first case H and aH, and in the second case H and Hb, for some $a, b \in G$. As $H = H$, it must be that $aH = Hb$. We have $a \in aH$, and by that, as $\{H, aH\}$ is a partition, it must be $a \notin H$. So, observing partition $\{H, Hb\}$ and condition that $a \notin H$, it must be that $a \in Hb$, i.e. there exists $h \in H$ such that $a = hb$. That means that $h^{-1}a = b$ and that $b \in Ha$. As $b \in Ha$, it must be that $Ha = Hb$. Combined with $aH = Hb$, we have $aH = Ha$. By a previous proposition, we have that H is normal.

□

Proposition. Let G be a group and $a \in G$ such that $\operatorname{ord}(a) = 2$. Then, $\langle a \rangle$ is a normal subgroup of G if and only if a is in the center of the group G.

Proof. Let us denote center of group G as $C = \{x \in G : \ (\forall y \in G)(xy = yx)\}$. We also have $|\langle a \rangle| = 2$, by definition. *Necessity.* Suppose $\langle a \rangle$ is a normal subgroup of G. Then, for all $g \in G$ we have $gag^{-1} \in \langle a \rangle$. But, that means that, either $a = gag^{-1}$ or $e = gag^{-1}$. That is equivalent to (after multiplying both equalities by g on the right) either $ag = ga$, or $g = ga$. The second equality would imply that $a = e$, and, as $\operatorname{ord}(e) = 1$, we would have $\operatorname{ord}(a) = 1$, which is a contradiction to the assumption that $\operatorname{ord}(a) = 2$. Therefore, it must be that $ag = ga$, for all $g \in G$, and that implies that $a \in C$.

Sufficiency. Suppose $a \in C$. Then, $ag = ga$, for all $g \in G$. After multiplying that equality with g^1 on the right we have $a = gag^{-1}$, for all $g \in G$. That means that $gag^{-1} \in \langle a \rangle$ for all $g \in G$. Now, the only other element in $\langle a \rangle$ is e. But, $e = geg^{-1}$, for all $g \in G$ and we have that $geg^{-1} \in \langle a \rangle$, for all $g \in G$. Thus, as $gxg^{-1} \in \langle a \rangle$, for all $g \in G$ and $x \in \langle a \rangle$ (as either $x = e$ or $x = a$), it follows that $\langle a \rangle$ is a normal subgroup of G.

□

Lemma. Let G be a group, $x, y \in G$ and $n \in \mathbb{Z}$. Then, $(x^{-1}yx)^n = x^{-1}y^n x$.

Proof. For $n = 1$ we have $(x^{-1}yx)^1 = x^{-1}y^k x$ by definition. Then, suppose the statement is true for $n = k$, i.e. $(x^{-1}yx)^k = x^{-1}y^k x$. Let us prove that it is valid for $n = k+1$. We have $(x^{-1}yx)^{k+1} = (x^{-1}yx)^k (x^{-1}yx)$. By using assumption of induction we obtain $(x^{-1}yx)^{k+1} = x^{-1}y^k xx^{-1}yx = x^{-1}y^{k+1}x$. Thus, the statement is true for all $n \in \mathbb{N}$. Now, for $n = 0$ we would have $(x^{-1}yx)^0 = e$. But, we could write $e = x^{-1}x = x^{-1}ex = x^{-1}y^0 x$. Now let us prove the statement for $n \in \mathbb{Z}$, i.e. $n = -k$, where $k \in \mathbb{N}$. We have $(x^{-1}yx)^{-k} = \left((x^{-1}yx)^k\right)^{-1} = \left(x^{-1}y^k x\right)^{-1} = x^{-1}\left(x^{-1}y^k\right)^{-1} = x^{-1}y^{-k}x$. Thus we have proved the statement is valid for all $n \in \mathbb{Z}$.

□

Proposition. Let G be a group and $a \in G$. Then, $\langle a \rangle$ is a normal subgroup of G if and only if for all $x \in G$, there exists $k \in \mathbb{N}$ such that $xa = a^k x$.

Proof. *Necessity.* Let $\langle a \rangle$ be a normal subgroup of G. Then, for all $x \in G$ and $y \in \langle a \rangle$ we have $xyx^{-1} \in \langle a \rangle$. But, that is also true for $a \in \langle a \rangle$, i.e. for all $x \in G$, we have $xax^{-1} \in \langle a \rangle$. Therefore, $xax^{-1} = a^k$, for some $k \in \{1, \ldots, \mathrm{ord}\,(a)\}$. Multiplying that equality by x on the right, we have $xa = a^k x$.

Sufficiency. Let for all $x \in G$ exist $k \in \mathbb{N}$ such that $xa = a^k x$. Then, multiplying that equality by x^{-1} on the right gives us $a^k = x^{-1}ax$. Let $a^l \in \langle a \rangle$. Then $a^{kl} = (x^{-1}ax)^l$. By a previous lemma we have $a^{kl} = x^{-1}a^l x$. As $a^{kl} \in \langle a \rangle$, then also $x^{-1}a^l x \in \langle a \rangle$, for all $x \in G$ and all $a^l \in \langle a \rangle$ and $\langle a \rangle$ is normal.

□

Definition. Let G be a group. A **commutator** is any product of the form $aba^{-1}b^{-1}$, where $a, b \in G$.

Proposition. Let G be a group and H a subgroup of G. If H contains all the commutators of G, then H is normal.

Proof. Let us define the set containing all commutators of G as

$$C = \{aba^{-1}b^{-1} \in G : \ a, b \in G\}.$$

Now, let $C \subseteq H$. If we take $x \in G$ and $y \in H \subseteq G$, then $xyx^{-1}y^{-1} \in C \subseteq H$. As H is a subgroup then also $xyx^{-1}y^{-1}y \in H$, i.e. $xyx^{-1} \in H$. Therefore, H is normal.

□

Proposition. If H and K are subgroups of G, and K is normal, then

$$HK = \{hk \in G : \ h \in H \ \wedge \ k \in K\}$$

is a subgroup of G.

Proof. By definition we have $HK \subseteq G$. Then, if we take $x, y \in HK$, we have $x = h_1k_1$ and $y = h_2k_2$, for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. From that we have $h_1^{-1}x \in K$ and $h_2^{-1}y \in K$. But also, $xh_1^{-1} \in K$ and $yh_2^{-1} \in K$. We have $h_1^{-1}xyh_2^{-1} \in K$ and, as K is closed with respect to conjugates, we also have $h_2^{-1}h_1^{-1}xyh_2^{-1}h_2 \in K$, that is $h_2^{-1}h_1^{-1}xy \in K$. As $h_1h_2 \in H$, we have $(h_1h_2)(h_1h_2)^{-1}xy \in HK$, which means $xy \in HK$. Therefore HK is closed with respect to products. Now, if we take $x \in HK$, we have $x = hk$, for some $h \in H$ and $k \in K$. Multiplying that by x^{-1} on the right and k^{-1} on the left, we have $x^{-1}h = k^{-1}$. Note that $x^{-1}h \in K$ as $k^{-1} \in K$. But, as K is normal, it is closed with respect to conjugates, so it must be that $hx^{-1}hh^{-1} \in K$, i.e. $hx^{-1} \in K$. As $h^{-1} \in H$, we have $h^{-1}hx^{-1} \in HK$, that is $x^{-1} \in HK$. As HK is closed with respect to inverses also, it is a subgroup of G.

□

Proposition. Let G be a group and H a subgroup of G. Let

$$S = \bigcup \{Ha : \ Ha = aH, \ a \in G\}.$$

Then S is a subgroup of G and H is a normal subgroup of S.

Proof. *S is a subgroup of G.* If we take $x \in S$, then $x \in Ha$, for some $a \in G$, and $Ha \subseteq G$, so $S \subseteq G$. If we take $x, y \in S$, then $x \in Ha$ and $y \in Hb$, for some $a, b \in G$. We have $Ha = aH$ and $Hb = bH$ so by a previous proposition we have that $(ab)H = H(ab)$. Thus, it must be that $H(ab) \subseteq S$. We have $x = h_1a$ and $y = h_2b$ for some $h_1, h_2 \in H$. So, we have $xy = h_1ah_2b$. But, as $ah_2 \in aH$ and $aH = Ha$, there exists $h_3 \in H$ such that $ah_2 = h_3a$. From that we have $xy = h_1h_3ab$, and as $h_1h_3 \in H$, we have $xy \in H(ab) \subseteq S$. If we take $x \in Ha$, where $a \in G$, we have $x = h_1a$, for some $h_1 \in H$. Then, multiplying by x^{-1} on the right gives us $e = h_1ax^{-1}$, and multiplying by $(h_1a)^{-1}$ on the left yields $x = a^{-1}h^{-1}$. Therefore, $x \in a^{-1}H$. But, as $aH = Ha$ implies $a^{-1}H = Ha^{-1}$ by a previous proposition, we have $Ha^{-1} \subseteq S$. As we have $x = a^{-1}h^{-1}$ and $a^{-1}H = Ha^{-1}$, there exists $h' \in H$ such that $a^{-1}h^{-1} = h'a^{-1}$. To conclude, $x^{-1} = h'a^{-1}$ and $h'a^{-1} \in Ha^{-1} \subseteq S$. Therefore, S is closed with respect to inverses and products and it is a subgroup of G.

H is a normal subgroup of S. As $H = He = eH$, we have $H \subseteq S$. If we take $x, y \in H \subseteq S$, then, as H is a subgroup of G, we have $xy \in H$. Also, for $x \in H$, as H is a subgroup of G, we have $x^{-1} \in H$. But, if we take $x \in S$ and $y \in H$, we have $x \in Ha$, for some $a \in G$ and $x = h_1 a$, for some $h_1 \in H$. But, as $x \in S$, and S is a subgroup of G, we also have $x^{-1} \in S$ and $x^{-1} = a^{-1}h_1^{-1}$. Therefore, $xyx^{-1} = h_1 aya^{-1}h_1^{-1}$. As $y \in H$ we have $ay \in aH$. As $aH = Ha$, we have that $ay = h'a$ for some $h' \in H$. That implies $xyx^{-1} = h_1 h'aa^{-1}h_1^{-1} = h_1 h'h_1^{-1}$. As H is a subgroup of G we have $h_1 h'h_1^{-1} \in H$ and from that $xyx^{-1} \in H$. Therefore, H is a normal subgroup of S.

□

Theorem. Let $f : G \to H$ be a homomorphism from group G to group H, $n \in \mathbb{N}$ and $a \in G$. Then, $f(a^n) = [f(a)]^n$.

Proof. Let us prove that the statement holds for $n = 1$. We have $f(a^1) = f(a) = [f(a)]^1$. Suppose statement is true for $n = k$, i.e. $f\left(a^k\right) = [f(a)]^k$. Now, let us prove that it is true for $n = k + 1$. We have $f\left(a^{k+1}\right) = f\left(a^k a\right)$. As f is a homomorphism we have $f\left(a^k a\right) = f\left(a^k\right) f(a)$. Now, due to the assumption of induction, we have $f\left(a^k\right) = [f(a)]^k$. So, we get $f\left(a^{k+1}\right) = [f(a)]^k f(a) = [f(a)]^{k+1}$. Thus, by the principle of mathematical induction, we have proved the statement for all $n \in \mathbb{N}$.

□

Corollary. Let G and H be groups, $f : G \to H$ a homomorphism and $a \in G$. Then[56], $f(\langle a \rangle) = \langle f(a) \rangle$.

Proof. Take $f(a^k) \in f(\langle a \rangle)$, for some $k \in \mathbb{N}$. By a previous theorem we have $f(a^k) = [f(a)]^k$, which is in $\langle f(a) \rangle$. Therefore, $f(\langle a \rangle) \subseteq \langle f(a) \rangle$. Now, if we take $[f(a)]^k \in \langle f(a) \rangle$, for some $k \in \mathbb{N}$, we have $[f(a)]^k = f(a^k)$ and $f(a^k) \in f(\langle f \rangle)$. As also $\langle f(a) \rangle \subseteq f(\langle a \rangle)$, we have $f(\langle a \rangle) = \langle f(a) \rangle$.

Remark. Notice that from previous corollary we have $|f(\langle a \rangle)| = |\langle f(a) \rangle|$.

Corollary. Let $f : G \to H$ be a homomorphism and $a \in G$. Then, $\operatorname{ord}(f(a)) \mid \operatorname{ord}(a)$.

Proof. Suppose $\operatorname{ord}(a) = n$. That implies that $a^n = e$. As $f(e) = e$ and $a^n = e$, we have $f(a^n) = e$. From the previous theorem we have $f(a^n) = [f(a)]^n = e$. Therefore, as from $x^n = e$ follows that $\operatorname{ord}(x) \mid n$, we have that $\operatorname{ord}(f(a)) \mid n$, i.e. $\operatorname{ord}(f(a)) \mid \operatorname{ord}(a)$.

□

[56] Note that $f(\langle a \rangle) = \{f(a^k) : \ a^k \in \langle a \rangle\}$.

Remark. Note that by Lagrange's theorem we have that $\operatorname{ord}(a)$ divides $|G|$. Therefore, $\operatorname{ord}(f(a))$ also divides $|G|$. Furthermore, as $\operatorname{ran}(f)$ is a subgroup of H, for $f(a) \in \operatorname{ran}(f)$ we have that $\operatorname{ord}(f(a))$ divides $|H|$. Therefore, if $b \in \operatorname{ran}(f)$, then $\operatorname{ord}(b)$ is a common divisor of $|G|$ and $|H|$.

Problem. Let $f : G \to H$ be a homomorphism from group G to group H. Prove:

1. If $|\operatorname{ran}(f)| = n$, then $a^n \in \ker(f)$, for every $a \in G$;
2. Let $m \in \mathbb{Z}$ such that $\gcd(m, |H|) = 1$. For any $a \in G$, if $a^m \in \ker(f)$, then $a \in \ker(f)$;
3. Let $|\operatorname{ran}(f)| = m$ and $a \in G$. If $\operatorname{ord}(a) = n$, where $\gcd m, n = 1$, then $a \in \ker(f)$;
4. Let $p \in P$. If $\operatorname{ran}(f)$ has an element of order p, then G has an element of order p.

Solution.

1. *If* $|\operatorname{ran}(f)| = n$, *then* $a^n \in \ker(f)$, *for every* $a \in G$. Let $f(a) \in \operatorname{ran}(f)$. From Lagrange's theorem we have that $\operatorname{ord}(f(a)) | n$. So it must be $[f(a)]^n = e$. From a previous theorem we have $[f(a)]^n = f(a^n) = e$, therefore $a^n \in \ker(f)$.
2. *Let* $m \in \mathbb{Z}$ *such that* $\gcd(m, |H|) = 1$. *For any* $a \in G$, *if* $a^m \in \ker(f)$, *then* $a \in \ker(f)$. Suppose $a^m \in \ker(f)$. Then, $f(a^m) = e$ and from that, by a previous theorem, we have $f(a^m) = [f(a)]^m = e$. Therefore $\operatorname{ord}(f(a)) | m$. But, by Lagrange's theorem, also $\operatorname{ord}(f(a))$ divides $|H|$. But, as m and $|H|$ are relatively prime, they have no common divisors except ± 1. So it can only be that $\operatorname{ord}(f(a)) = 1$, and from that it follows that $f(a) = e$ and $a \in \ker(f)$.
3. *Let* $|\operatorname{ran}(f)| = m$ *and* $a \in G$. *If* $\operatorname{ord}(a) = n$, *where* $\gcd m, n = 1$, *then* $a \in \ker(f)$. Let $a \in G$. Then, $f(a) \in \operatorname{ran}(f)$. We have that $\operatorname{ord}(f(a)) | \operatorname{ord}(a)$, i.e. $\operatorname{ord}(f(a)) | n$, and $\operatorname{ord}(f(a)) | m$ (order of $f(a)$ divides $|\operatorname{ran}(f)|$). But, as m and n are relatively prime, we have $\operatorname{ord}(f(a)) = 1$, that is $f(a) = e$ and $a \in \ker(f)$.
4. *Let* $p \in P$. *If* $\operatorname{ran}(f)$ *has an element of order* p, *then* G *has an element of order* p. Suppose $f(a) \in \operatorname{ran}(f)$ such that $\operatorname{ord}(f(a)) = p$. We have $\operatorname{ord}(f(a)) | \operatorname{ord}(a)$, i.e. $p | \operatorname{ord}(a)$ so it must be $\operatorname{ord}(a) = pk$, for some $k \in \mathbb{N}$. As, by Lagrange's theorem, $\operatorname{ord}(a)$ divides order of G, we have $|G| = pkl$, for some $l \in \mathbb{N}$. As p divides $|G|$, by Cauchy's theorem (not yet proved), it has an element of order p.

Definition. We say that a group G is **finitely generated** if the set of its generators is finite.

Proposition. Let G and H be groups and $f : G \to H$ a homomorphism such that[57] $H = \text{ran}\,(f)$. Then:

1. If G is Abelian, then H is Abelian.
2. If G is cyclic, then H is cyclic.
3. If every element of G has finite order, then every element of H has finite order.
4. If every element of G is its own inverse, every element of H is its own inverse.
5. If every element of G has a square root, then every element of H has a square root.
6. If G is finitely generated, then H is finitely generated.

Proof. *Ad* 1. Let us take $y_1, y_2 \in H$. As $H = \text{ran}\,(f)$, then $y_1 = f(x_1)$ and $y_2 = f(x_2)$ for some $x_1, x_2 \in G$. Then, $y_1 y_2 = f(x_1)f(x_2)$. As f is a homomorphism, we have $y_1 y_2 = f(x_1 x_2)$. But, as G is Abelian, $x_1 x_2 = x_2 x_1$. As f is a function, for all $a, b \in G$, $a = b$ implies $f(a) = f(b)$. Therefore, $x_1 x_2 = x_2 x_1$ implies $f(x_1 x_2) = f(x_2 x_1)$. So, we have $y_1 y_2 = f(x_2 x_1)$, and again as f is a homomorphism, we have $y_1 y_2 = f(x_2)f(x_1) = y_2 y_1$, and so H is Abelian.

Ad 2. As G is cyclic, then $G = \langle a \rangle$ for some $a \in G$ and every element is of the form $a^k \in \langle a \rangle$, for some $k \in \{0, 1, \ldots, \text{ord}\,(a) - 1\}$. Let us take $y \in \text{ran}\,(f)$. Then there exists $a^k \in G$ such that $y = f(a^k)$. By a previous proposition, we have $f(a^k) = [f(a)]^k$, so $y = [f(a)]^k$. In other words, every $y \in \text{ran}\,(f)$ can be shown as a power of $f(a)$; that implies that $f(a)$ generates $\text{ran}\,(f)$ and we have $H = \text{ran}\,(f) = \langle f(a) \rangle$.

Ad 3. Assume that all $x \in G$ have finite order. Suppose that there is some $y \in H$ that has infinite order, i.e. there does not exist $n \in \mathbb{N}$ such that $y^n = e$. As $H = \text{ran}\,(f)$, we have $y \in \text{ran}\,(f)$, which means that there exists some $x \in G$ such that $y = f(x)$. Now, as $x \in G$, it has finite order, e.g. $\text{ord}\,(x) = m$, for some $m \in \mathbb{N}$. Thus, $x^m = e$. When we apply f we get $f(x^m) = e$, and by a previous theorem $[f(x)]^m = e$. But, $y = f(x)$, so we have $y^m = e$, which is contrary to our assumption that there does not exist such natural number. Furthermore, $\text{ord}\,(y) \,|m$.

Ad 4. We have that $x^2 = e$ for all $x \in G$. Take $y \in H$, then as $H = \text{ran}\,(f)$, we have $y \in \text{ran}\,(f)$ and there exists $x \in G$ such that $y = f(x)$. Then, $y^2 = [f(x)]^2$. As f is homomorphism, that is equivalent to $y^2 = f(x^2)$. But, $x^2 = e$, so $y^2 = f(e)$. Again, as f is a homomorphism, by a previous theorem, we have that $f(e) = e$ and $y^2 = f(e) = e$. Therefore, $y^2 = e$, for all $y \in H$.

[57] Same as $H = f(G)$ or $H = \text{Im}(f)$.

Ad 5. Suppose that for all $a \in G$, there exists $b \in G$ such that $a = b^2$. Let $y_1 \in H$, i.e. $y_1 \in \operatorname{ran}(f)$. We must show that there exists $y_2 \in \operatorname{ran}(f)$ such that $y_1 = y_2^2$. As $y_1 \in \operatorname{ran}(f)$, there exists $x_1 \in G$ such that $y_1 = f(x_1)$. But, $x_1 \in G$, so there exists $x_2 \in G$ such that $x_1 = x_2^2$. Applying f gives us $f(x_1) = f(x_2^2)$ and, as f is a homomorphism, $f(x_1) = [f(x_2)]^2$. Therefore $y_1 = [f(x_2)]^2$. Also, as $f(x_2) \in \operatorname{ran}(f)$, we can take $y_2 = f(x_2)$ so to get $y_1 = y_2^2$. Therefore, each $y_1 \in H$ has a square root.

Ad 6. Suppose that the set $S = \{s_1, \ldots, s_n\}$, where $n \in \mathbb{N}$, generates G. Let $T = S \cup \{s^{-1} \in G : \ s \in S\}$ and $\phi : T^k \to G$, for some $k \in \mathbb{N}$, be a function defined as:

$$\phi(t_1, \ldots, t_k) = \prod_{i=1}^{k} t_i.$$

Then, for every $a \in G$ there exist $k \in \mathbb{N}$ and $X \in T^k$ such that $\phi(X) = a$. Let $y \in H = \operatorname{ran}(f)$. Then there exists $x \in G$ such that $f(x) = y$. But, as $x \in G$, then there exists $k \in \mathbb{N}$ and $(t_1, \ldots, t_k) \in T^k$ such that $\phi(t_1, \ldots, t_k) = x$, i.e. $x = \prod_{i=1}^{k} t_i$. As f is homomorphism we have:

$$y = f(x) = f\left(\prod_{i=1}^{k} t_i\right) = \prod_{i=1}^{k} f(t_i).$$

Notice that $f(t_i) \in f(T) = \{f(t) : \ t \in T\}$. Also, as S is finite so is T and $f(T)$. Now, as each $y \in H$ can be shown as a product of $f(t_i) \in f(T)$, then H is generated by $f(T)$. As $f(T)$ is finite, H is finitely generated.

□

Lemma. Let G be a group with normal subgroups H and K such that $H \cap K = \{e\}$. Then:

1. For any $h_1, h_2 \in H$ and $k_1, k_2 \in K$, from $h_1k_1 = h_2k_2$ follows $h_1 = h_2$ and $k_1 = k_2$.
2. For any $h \in H$ and $k \in K$, $hk = kh$.

Proof. *Ad* 1. Suppose $h_1, h_2 \in H$, $k_1, k_2 \in K$ and $h_1k_1 = h_2k_2$. That expression is equivalent to $h_2^{-1}h_1 = k_2k_1^{-1}$ (after multiplying by h_2^{-1} on the left and k_1^{-1} on the right). As $h_2^{-1}h_1 \in H$ and it equals $k_2k_1^{-1}$ (which is in K), it also has to be in K. So, $h_2^{-1}h_1 \in H \cap K$. But, the only element in $H \cap K$ is e, so it must be $h_2^{-1}h_1 = e$. That implies, after multiplying by $h_2 \in H$ on the left, that $h_1 = h_2$. Now, $h_1k_1 = h_2k_2$ implies $hk_1 = hk_2$ (where $h = h_1 = h_2$) and, as G is a group and $k_1, k_2 \in K \subseteq G$ and $h \in H \subseteq G$, we multiply by $h^{-1} \in G$ on the left (cancellation law) to get $k_1 = k_2$.

Ad 2. Let $h \in H$ and $k \in K$. Also, $h^{-1} \in H$ and $k^{-1} \in K$ (as H and K are subgroups). As H and K are normal, $khk^{-1} \in H$ and $hk^{-1}h^{-1} \in K$. Furthermore, as

$khk^{-1} \in H$, then $(khk^{-1})h^{-1} \in H$. Similarly, as $hk^{-1}h^{-1} \in K$, then $k(hk^{-1}h^{-1}) \in K$. Then, as $khk^{-1}h^{-1}$ in H and K, it is in $H \cap K$. So it must be $khk^{-1}h^{-1} = e$. Multiplying by (hk) on the right gives us $kh = hk$.

□

Theorem. If H and K are normal subgroups of group G, such that $H \cap K = \{e\}$ and $G = HK$, then $G \cong H \times K$.

Proof. Let $f : H \times K \to G$ be a mapping such that $f(h, k) = hk$. It is unique and defined for all $(h, k) \in H \times K$. *Surjectivity.* Choose $y \in G$. Then, as $G = HK$, there exist $h \in H$ and $k \in K$ such that $y = hk$. As $h \in H$ and $k \in K$, then $x = (h, k) \in H \times K$. Therefore, for each $y \in G$ there exists $x \in H \times K$ such that $f(x) = y$. *Injectivity.* Let $f(h_1, k_1) = f(h_2, k_2)$. Then, $h_1k_1 = h_2k_2$. By a previous lemma we have $h_1 = h_2$ and $k_1 = k_2$, which implies $(h_1, k_1) = (h_2, k_2)$ and the function is injective. As it is injective and surjective, it is bijective. Now, if we take $(h_1, k_1), (h_2, k_2) \in H \times K$, we have $f((h_1, k_1)(h_2, k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2$. As, by a previous lemma, $hk = kh$, for all $h \in H$ and $k \in K$, then $h_1(h_2k_1)k_2 = (h_1k_1)(h_2k_2) = f(h_1, k_1)f(h_2, k_2)$. Thus, f is an isomorphism from $H \times K$ to G and we have $H \times K \cong G$. As $\cong$ is an equivalence relation, it is also symmetric, so $G \cong H \times K$.

□

Remark. Group G from the previous theorem is sometimes called **direct inner product** of H and K.

Definition. Let G be a group, H a subgroup of G and $a \in G$. A **conjugate** of H is the set:

$$aHa^{-1} = \left\{aha^{-1} : \ h \in H\right\}.$$

Proposition. Let G be a group and H a subgroup of G. Then:

1. aHa^{-1} is a subgroup of G, for each $a \in G$.
2. $H \cong aHa^{-1}$, for each $a \in G$.
3. H is a normal subgroup of G if and only if $H = aHa^{-1}$ for every $a \in G$.

Proof. *Ad* 1. Let $a \in G$. Then, if we take $y \in aHa^{-1}$ it is of the form $y = xax^{-1}$, where $x \in H \subseteq G$. As $x \in G$ and $a^{-1} \in G$ then $axa^{-1} \in G$. Therefore $aHa^{-1} \subseteq G$. If we take $x, y \in aHa^{-1}$, then $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$, for some $h_1, h_2 \in H$. Then,

$xy = ah_1a^{-1}ah_2a^{-1} = ah_1h_2a^{-1}$. As H is a subgroup of G, we have $h_1h_2 \in H$ and that implies $xy \in aHa^{-1}$. Now, if we multiply expression for x by x^{-1} on the left and by $(ah_1a^{-1})^{-1}$ on the right we get $x^{-1} = (ah_1a^{-1})^{-1} = (h_1a^{-1})^{-1}\,a^{-1} = ah_1^{-1}a^{-1}$. As H is a subgroup of G, then $h_1^{-1} \in H$ and $x^{-1} \in aHa^{-1}$. Therefore, aHa^{-1} is closed with respect to products and inverses and is a subgroup of G.

Ad 2. Let $f : H \to aHa^{-1}$ be a function such that $f(h) = aha^{-1}$ (obviously it is a function as it is defined for all $h \in H$ and returns a unique element in aHa^{-1}). *Surjectivity.* Let $y \in aHa^{-1}$. Then there exists $h \in H$ such that $y = aha^{-1}$. Then, after multiplying by a on the right and a^{-1} on the left we have $h = a^{-1}ya$. As $h \in H$, we have $f(h) = aha^{-1} = aa^{-1}yaa^{-1} = y$. Thus, f is surjective. *Injectivity.* Suppose $f(h_1) = f(h_2)$. Then, $ah_1a^{-1} = ah_2a^{-1}$. After multiplying by a on the right we have $ah_1 = ah_2$, and after multiplying by a^{-1} on the left $h_1 = h_2$. Therefore, f is surjective and injective and by that a bijection. Now take $h_1, h_2 \in H$. Then $f(h_1h_2) = ah_1h_2a^{-1} = ah_1a^{-1}ah_2a^{-1} = f(h_1)f(h_2)$ and f is an isomorphism from H to aHa^{-1}, i.e. $H \cong aHa^{-1}$.

Ad 3. *Necessity.* Suppose H is a normal subgroup of G. Take $a \in G$ and $aha^{-1} \in aHa^{-1}$. Then, $h \in H$. As H is normal and $a \in G$ with $h \in H$, then $aha^{-1} \in H$ and $aHa^1 \subseteq H$. Now, if we take $h \in H$, then, as H is normal, $h' = a^{-1}ha \in H$. But, also, as $h' \in H$, we have $ah'a^{-1} \in aHa^{-1}$, that is $aa^{-1}haa^{-1} = h \in aHa^{-1}$, for all $a \in G$. As $h \in H$ implied $h \in aHa^{-1}$, we have $H \subseteq aHa^{-1}$ and, from the previous subset relation, $H = aHa^{-1}$, for all $a \in G$. *Sufficiency.* Suppose $H = aHa^{-1}$ for every $a \in G$. So, if we take $h \in H$, then $h \in aHa^{-1}$, i.e. there exists $h' \in H$ such that $h = ah'a^{-1}$. Multiplying that expression on the left by a^{-1} and by a on the right yields $h' = a^{-1}ha$. As $h' \in H$, then $a^{-1}ha \in H$, so H is closed with respect to conjugates and is therefore a normal subgroup of G.

□

Definition. Let G be a finite group and H a subgroup of G. Set

$$N(H) = \left\{a \in G :\ (\forall h \in H)\left(aha^{-1} \in H\right)\right\}$$

is called **normalizer** of H.

Proposition. Let G be a finite group and H a subgroup of G. Then:

1. If $a \in N(H)$, then $aHa^{-1} = H$.
2. $N(H)$ is a subgroup of G.
3. H is a normal subgroup of $N(H)$.

Proof. *Ad* 1. Suppose $a \in N(H)$. Then $aha^{-1} \in H$, for all $h \in H$. If we take $aha^{-1} \in aHa^{-1}$, then, by the forementioned property, $aha^{-1} \in H$. That implies $aHa^{-1} \subseteq H$. But, from a previous proposition we have $H \cong aHa^{-1}$, which implies $|H| = |aHa^{-1}|$. From a previous lemma we have that $aHa^{-1} = H$.

Ad 2. By definition, $N(H) \subseteq G$. Then, if we take $a, b \in N(H)$, then for $a, b \in G$ we have $aha^{-1} \in H$ and $bhb^{-1} \in H$, for all $h \in H$. As $aha^{-1} \in H$, then $aha^{-1}a \in Ha$, i.e. $ah \in Ha$, for all $ah \in aH$. That means that $aH \subseteq Ha$. Now, as $|Ha| = |H| = |aH|$, we have $aH = Ha$. In the vein of the same reasoning we get $bH = Hb$. So, by a previous proposition, $(ab)H = H(ab)$. Therefore, for all $abh \in H$ there exists $h' \in H$ such that $abh = h'ab$. Multiplying that by $(ab)^{-1}$ we get $(ab)h(ab)^{-1} = h'$. As $h' \in H$, then $(ab)h(ab)^{-1} \in H$ and by definition $ab \in N(H)$. Now, as for $a \in N(H)$ we have that $aH = Ha$ we also have $a^{-1}H = Ha^{-1}$ by a previous proposition. Therefore if we take $a^{-1}h \in H$, then there exists $h' \in H$ such that $a^{-1}h = h'a^{-1}$. Multiplying that by $a \in G$ on the right we get $a^{-1}ha = h'$. As $h' \in H$ then $a^{-1}ha \in H$ and we have that $a^{-1} \in N(H)$. Therefore, $N(H)$ is a subgroup of G.

Ad 3. If we take $h \in H$, then $he \in H$, i.e. $hhh^{-1} \in H$, so $h \in N(H)$. That implies that $H \subseteq N(H)$. If we take $h_1, h_2 \in H$, then $h_1h_2 \in H$ and $h^{-1} \in H$, as H is a subgroup of G. Furthermore, if we take $h \in H$ and $a \in N(H)$, then, $aha^{-1} \in H$ (from definition of $N(H)$) which implies that H is a normal subgroup of $N(H)$.

□

Proposition. Let G be a group, H a subgroup of G and $N = N(H)$. Then, for all $a, b \in G$, the following statements are equivalent:

1. $aHa^{-1} = bHb^{-1}$;
2. $b^{-1}a \in N$;
3. $aN = bN$.

Proof. *$aHa^{-1} = bHb^{-1}$ implies $b^{-1}a \in N$.* If $aHa^{-1} = bHb^{-1}$, then for all $ah_1a^{-1} \in aHa^{-1}$ there exists $bh_2b^{-1} \in bHb^{-1}$ such that $ah_1a^{-1} = bh_2b^{-1}$. Multiplying that expression by b on the right and b^{-1} on the left we get $b^{-1}ah_1a^{-1}b = h_2$, that is, $(b^{-1}a)\, h_1\, (ab^{-1})^{-1} \in H$, so $ab^{-1} \in N(H)$.

$b^{-1}a \in N$ implies $aN = bN$. As $b^{-1}a \in N$, we can take $bb^{-1}a \in bN$, i.e. $a \in bN$. By a previos proposition, as $a \in bN$, we have $aN = bN$.

$aN = bN$ implies $b^{-1}a \in N$ implies $aHa^{-1} = bHb^{-1}$. As $aN = bN$, then for $an_1 \in aN$, there exists $bn_2 \in bN$ such that $an_1 = bn_2$. Multiplying that by b^{-1} on the left and by n_1^{-1} on the right, gives us $b^{-1}a = n_2n_1^{-1}$, i.e. $b^{-1}a \in N$. If we take $ah_1a^{-1} \in aHa^{-1}$, then, as $b^{-1}a \in N$, for all $h \in H$, $b^{-1}aha^{-1}b \in H$. So, it is also true

for h_1 and we have $b^{-1}ah_1a^{-1}b \in H$, i.e. $bb^{-1}ah_1a^{-1}bb^{-1} \in bHb^{-1}$. That means that $ah_1a^{-1} \in bHb^{-1}$ and $aHa^{-1} \subseteq bHb^{-1}$. If we take $bh_2b^{-1} \in H$, then, as $b^{-1}ah_2a^{-1}b \in H$, we have that there exists $h_3 \in H$, such that $h_3 = b^{-1}ah_2a^{-1}b \in H$. Multiplying that by $(b^{-1}a)^{-1}$ on the left and $b^{-1}a$ on the right gives us $a^{-1}bh_3b^{-1}a = h_2$, i.e. $a^{-1}bh_3b^{-1}a \in H$. Therefore, $aa^{-1}bh_3b^{-1}aa^{-1} \in aHa^{-1}$, which means $bh_3b^{-1} \in aHa^{-1}$ and $bHb^{-1} \subseteq aHa^{-1}$. Finally, $aHa^{-1} = bHb^{-1}$.

□

Proposition. Let G be a group and H a subgroup of G. Let $\mathcal{N} = \{Na : \ a \in G\}$ and $\mathcal{H} = \{aHa^{-1} : \ a \in G\}$. Then, there exists a bijection $f : \mathcal{N} \to \mathcal{H}$.

Proof. Let f be defined as above with $f(Na) = aHa^{-1}$. If we take $Na = Nb$, then it implies, by a previous proposition, that $aN = bN$ and then that $aHa^{-1} = bHb^{-1}$, i.e. $f(Na) = f(Nb)$. Therefore, f satisfies property of uniqueness and is defined for all $a \in G$. *Surjectivity.* If we take $aHa^{-1} \in \mathcal{H}$, we can always take $Na \in \mathcal{N}$ to get $f(Na) = aHa^{-1}$ (because f depends on a, and f is defined for all a, both ways). *Injectivity.* If $f(Na) = f(Nb)$, i.e. $aHa^{-1} = bHb^{-1}$, by a previous proposition, we have $aN = bN$. But, $aN = bN$ if and only if $Na = Nb$. Therefore, f is bijective.

□

Corollary. If G is a finite group and H a subgroup of G, then H has exactly $[G : N(H)]$ conjugates.

Proof. As, by a previous proposition, $|\mathcal{N}| = |\mathcal{H}|$, that means that the number of conjugates in G is the same as the number of cosets of $N(H)$ in G. But, the number of cosets of $N(H)$ is $[G : N(H)]$ and that implies $|\mathcal{H}| = [G : N(H)]$.

□

Proposition. Let G be a group and H and K subgroups of G. Let $\mathcal{N}_K = \{Na : \ a \in K\}$ and $\mathcal{H}_K = \{aHa^{-1} : \ a \in K\}$. There exists a bijection $f : \mathcal{N}_K \to \mathcal{H}_K$.

Proof. Let f be defined as $f(Na) = aHa^{-1}$. As K is a subgroup of G, it is also a group and the properties of uniqueness and injectivity hold for f, as in the latter proposition. Surjectivity holds as f is trivially defined for all $a \in K$.

□

Remark. From the previous proposition, the number of conjugates of K divides order of K, by Lagrange's theorem.

Quotient groups

Theorem. If H is a normal subgroup of G, then $aH = Ha$ for every $a \in G$.

Proof. Let H be a normal subgroup of G. Then, $aha^{-1} \in H$, for all $a \in G$ and $h \in H$. If we take $ah \in aH$, then, as $a \in G$ and $h \in H$ (and H being a normal subgroup of G) we have $aha^{-1} \in H$ which implies $aha^{-1}a \in Ha$, i.e. $ah \in Ha$. Thus, $aH \subseteq Ha$. Also, if we take $ha \in Ha$, then $a^{-1}ha \in H$ and, from that $aa^{-1}ha \in aH$, that is $ha \in aH$. Therefore, $Ha \subseteq aH$ and $aH = Ha$.

□

Definition. Let G be a group and H a normal subgroup of G. **Coset multiplication**, for $a, b \in G$, is defined as:

$$Ha \cdot Hb = H(ab).$$

Remark. If G is a group with additive-like operation then remember that we write $H + a$ instead of Ha. So we will also define *coset addition* as $[H + a] + [H + b] = [H + (a + b)]$. The difference is just in naming, everything else is the same.

Theorem. Coset multiplication, as defined above, satisfies the property of uniqueness.

Proof. Let $Ha = Hc$ and $Hb = Hd$. Then it has to be $H(ab) = H(cd)$. If we take $hab \in Hab$, then $(ha) \in Ha$ and there exists $h_1 \in Hc$ such that $ha = h_1c$. Therefore, $hab = h_1cb$. But, as H is normal, then there exists $h_2 \in H$ such that $h_2 = c^{-1}h_1c$, i.e. $ch_2c^{-1} = h_1$. From that we have $hab = ch_2c^{-1}cb$, that is $hab = ch_2b$. As $h_2b \in Hb$ and $Hb = Hd$, there exists $h_3 \in H$ such that $h_2b = h_3d$ and we have $hab = ch_3d$. Again, as H is normal, there exists $h_4 \in H$ such that $h_4 = ch_3c^{-1}$, i.e. $c^{-1}h_4c = h_3$. That implies $hab = cc^{-1}h_4cd$, which is equivalent to $hab = h_4cd$. As $h_4cd \in H(cd)$, then $hab \in H(cd)$ and it has to be $H(ab) \subseteq H(cd)$.

Now, if we take $hcd \in H(cd)$, then, as $hc \in Hc$ and $Hc = Ha$, there exists $h_1a \in Ha$ such that $hcd = h_1ad$. As H is normal, we have that there exists $h_2 \in H$ such that $h_2 = a^{-1}h_1a$, i.e. $ah_2a^{-1} = h_1$. So we have $hcd = ah_2d$. As $h_2d \in Hd$ and $Hd = Hb$, there exists $h_3 \in H$ such that $h_2d = h_3b$. We have $hcd = ah_3b$. As H is normal, there exists $h_4 \in H$ such that $h_4 = ah_3a^{-1}$, that is $a^{-1}h_4a = h_3$. From that follows that $hcd = aa^{-1}h_4ab$, id est $hcd = h_4ab$. As $h_4ab \in H(ab)$, then also $hcd \in H(ab)$. That means that $H(cd) \subseteq H(ab)$ and that, with $H(ab) \subseteq H(cd)$, implies $H(ab) = H(cd)$.

□

Definition. Let G be a group and H a normal subgroup of G. Let $G/H = \{Ha : a \in G\}$. Then, G/H with coset multiplication as respective operation is called a **quotient group**.

Theorem. Quotient group is a group.

Proof. Let G be a group and H a subgroup of G. Let quotient group G/H be defined as above. From the previous theorem, it follows that coset multiplication satisfies the property of uniqueness. It is also defined for all $Ha, Hb \in G/H$. *Associativity.* We have $Ha \cdot (Hb \cdot Hc) = Ha \cdot H(bc) = H(a(bc))$. As G is a group, it is associative and $a(bc) = abc$, so $H(a(bc)) = H(abc)$. Now, as $(Ha \cdot Hb) \cdot Hc = H(ab) \cdot Hc = H((ab)c)$, for the same reason $H((ab)c) = H(abc)$ and that means $Ha \cdot (Hb \cdot Hc) = (Ha \cdot Hb) \cdot Hc$. *Neutral element.* We can see that, as $H = He$, we have $Ha \cdot He = H(ae) = Ha$ and $He \cdot Ha = H(ea) = Ha$. Therefore, H is a neutral element. *Inverse elements.* For $Ha \in G/H$ we have $Ha^{-1} \in G/H$ and $Ha \cdot Ha^{-1} = H(aa^{-1}) = He = H$ with $Ha^{-1} \cdot Ha = H(a^{-1}a) = He = H$. To conclude, Ha^{-1} is the inverse element for Ha, and by all that G/H is a group.

□

Remark. Be reminded that a neutral element in G/H is H, and inverse of Ha is $H(a^{-1})$.

Proposition. Let G be a group and H a normal subgroup of G. Then, $|G/H| = [G : H]$.

Proof. Quotient group G/H contains all cosets of H in G and $[G : H]$ is a number of different cosets of H in G.

□

Theorem. Let G be a group and H a normal subgroup of G. There exists a homomorphism $f : G \to G/H$ such that $\operatorname{ran}(f) = G/H$ (G/H is a homomorphic image of G) and $\ker(f) = H$.

Proof. Let f be defined as above with $f(a) = Ha$. Then, f is defined for all $a \in G$. If $a = b$, then obviously also $Ha = Hb$, so f is uniquely defined for all $a \in G$. Also, f is surjective as for each $Ha \in G/H$ there exists $a \in G$ such that $f(a) = Ha$. That implies $G/H = \operatorname{ran}(f)$. Furthermore, $f(ab) = H(ab)$. By definition, $Ha \cdot Hb = H(ab)$, so we have $f(ab) = Ha \cdot Hb = f(a) \cdot f(b)$. Thus, G/H is a homomorphic image of H.

Now, $\ker(f) = \{a \in G : f(a) = H\} = \{a \in G : Ha = H\}$. By a previous proposition, from $Ha = H$ it follows that $a \in H$. Therefore, $\ker(f) = \{a \in G : a \in H\}$. As $H \subseteq G$, we have $\ker(f) = \{a \in H\} = H$.

□

Theorem. Let $Hx, Hy \in G/H$ and $m \in \mathbb{Z}$. Then:

1. $(Hx)^{-1} = H(x^{-1})$.
2. $(Hx)^m = H(x^m)$.

Proof. *Ad* 1. We have $Hx \cdot H(x^{-1}) = H(xx^{-1}) = He = H$. Therefore, $(Hx)^{-1} = H(x^{-1})$.

Ad 2. First we will prove that $(Hx)^n = H(x^n)$, for $n \in \mathbb{N}$. For $n = 1$ we have $Hx = Hx$, which is true. Suppose the statement is valid for $n = k$, i.e. $(Hx)^k = H\left(x^k\right)$. Now let us prove that it is valid for $n = k + 1$. We have $(Hx)^{k+1} = (Hx)^k \cdot Hx$. By using assumption of induction we have $(Hx)^{k+1} = H\left(x^k\right) \cdot Hx$. By definition of coset multiplication we have $(Hx)^{k+1} = H\left(x^k x\right) = H\left(x^{k+1}\right)$. Therefore, statement is true for all $n \in \mathbb{N}$. Now, if $m = 0$, we have $(Hx)^0 = H = He = H(x^0)$. Now, if $m = -n$, we have $(Hx)^{-n} = \left((Hx)^{-1}\right)^n = (H(x^{-1}))^n = H\left((x^{-1})^n\right) = H(x^{-n})$. So, statement is true for all $m \in \mathbb{Z}$.

□

Problem. In each of the following excercises G is a group and H a normal subgroup of G. List the elements of G/H and then write the table of G/H.

1. $G = \mathbb{Z}_6$ and $H = \{0, 3\}$;
2. $G = \mathbb{Z}_1 0$ and $H = \{0, 5\}$;
3. $G = S_3$ and $H = \{\epsilon, \beta, \delta\}$;
4. $G = D_4$ and $H = \{e, b^2\}$;
5. $G = D_4$ and $H = \{e, b^2, a, ab^2\}$;
6. $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ and $H = \langle(0, 1)\rangle$;
7. $G = \mathcal{P}_3$ and $H = \{\emptyset, \{1\}\}$;
8. $G = \mathbb{R} \times \mathbb{R}$ and $H = \{(x, 0) : \ x \in \mathbb{R}\}$;
9. $G = \mathbb{R} \times \mathbb{R}$ and $H = \{(x, y) : \ y = -x\}$;
10. $G = \mathbb{R} \times \mathbb{R}$ and $H = \{(x, y) : \ y = 2x\}$.

Solution.

1. $G = \mathbb{Z}_6$ *and* $H = \{0, 3\}$. We have $H = H+0 = H+3 = \{0, 3\}$ and $H+1 = H+4 = \{1, 4\}$, $H+2 = H+5 = \{2, 5\}$. Then, $G/H = \{H, H+1, H+2\}$. Notice that, by a previous proposition, as G/H is a homomorphic image of G, and G is cyclic, then also G/H is cyclic. Obviously, $G/H = \langle H+1 \rangle$ as $[H+1]+[H+1] = H+2$ and $[H+1]+[H+1]+[H+1] = [H+2]+[H+1] = H+3 = H$. To conclude, as G/H has three elements and is cyclic, it is, by a previous theorem, isomorphic to $\mathbb{Z}_3$, that is $\mathbb{Z}_6/\{0, 3\} \cong \mathbb{Z}_3$.

2. $G = \mathbb{Z}_{10}$ *and* $H = \{0, 5\}$. We have $H = H+5 = \{0, 5\}$, $H+1 = \{1, 6\}$, $H+2 = \{2, 7\}$, $H+3 = \{3, 8\}$ and $H+4 = \{4, 9\}$. Using the fact that H is normal subgroup of G and has a well-defined coset addition, we have $H+6 = [H+1]+[H+5] = [H+1]+H = H+1$, $H+7 = [H+2]+[H+5] = [H+2]+H = H+2$, $H+8 = [H+3]+[H+5] = [H+3]+H = H+4$ and $H+9 = [H+4]+[H+5] = [H+4]+H = H+4$. Notice that if we observe a homomorphism $f : G \to G/H$, where $f(x) = H + x$, then $\ker(f) = \{0, 5\} = H = H + 5$. As in the previous example, generator of G is 1 and then generator of G/H is $f(1) = H + 1$. We could also see that $\mathbb{Z}_{10}/\{0, 5\} \cong \mathbb{Z}_5$. Notice also that, as G/H is a family of cosets of G, it is also a partition of G. As $H = 2$, then $[G : H] = \frac{|G|}{|H|} = \frac{10}{2} = 5$.

3. $G = S_3$ *and* $H = \{\epsilon, \beta, \delta\}$. Refer to page 185. By $|H| = 3$ and $|S_3| = 3! = 6$ we have $[S_3 : H] = \frac{6}{2} = 3$. So there are two different cosets of H in S_3. We have $H = H\epsilon = H\beta = H\delta = \{\epsilon, \beta, \delta\}$ and $H\alpha = \{\alpha, \gamma, \kappa\} = H\gamma = H\kappa$. Using the definition (and of course, that we can as H is normal) we get $H\alpha \cdot H\alpha = H(\alpha\alpha) = H\epsilon = H$, the multiplication table is:

$\cdot$	H	$H\alpha$
H	H	$H\alpha$
$H\alpha$	$H\alpha$	H

4. $G = D_4$ *and* $H = \{e, b^2\}$. Refer to page 72. From $|D_4| = 8$ and $|H| = 2$ we have $|G/H| = \frac{8}{2} = 4$. We have $H = H(b^2) = \{e, b^2\}$, $Ha = H(ab^2) = \{a, ab^2\}$, $Hb = H(b^3) = \{b, b^3\}$, $H(ab) = H(ab^3) = \{ab, ab^3\}$. Notice that $Ha \cdot Ha = H(a^2) = He = H$, $Hb \cdot Ha = H(ba) = H(ab^3) = H(ab)$, etc. The multiplication table for G/H is:

$\cdot$	H	Ha	Hb	$H(ab)$
H	H	Ha	Hb	$H(ab)$
Ha	Ha	H	$H(ab)$	Hb
Hb	Hb	$H(ab)$	H	Ha
$H(ab)$	$H(ab)$	Hb	Ha	H

5. $G = D_4$ *and* $H = \{e, b^2, ab, ab^3\}$. Here $|G/H| = 2$. We have $H = H(b^2) = H(ab) = H(ab^3)$, $Ha = \{b, b^3, ab^2, a\} = H(ab^2) = H(b^3) = Hb$. As $a^2 = e$, then $Ha \cdot Ha = H(a^2) = H$ and therefore:

$\cdot$	H	Ha
H	H	Ha
Ha	Ha	H

6. $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ *and* $H = \langle(0,1)\rangle$. We have only $H = \{(0,1),(0,0)\}$ and $|H| = 2$. Also, $G = \{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1),(3,0),(3,1)\}$ and $|G| = 8$. We will have $|G/H| = \frac{8}{2} = 4$. So, $H = H + (0,0) = H + (0,1)$, $H + (1,0) = H + (1,1) = \{(0,1),(1,1)\}$, $H + (2,0) = H + (2,1) = \{(2,0),(2,1)\}$, $H + (3,0) = H + (3,1) = \{(3,0),(3,1)\}$. The addition table is:

$+$	H	$H+(1,0)$	$H+(2,0)$	$H+(3,0)$
H	H	$H+(1,0)$	$H+(2,0)$	$H+(3,0)$
$H+(1,0)$	$H+(1,0)$	$H+(2,0)$	$H+(3,0)$	H
$H+(2,0)$	$H+(2,0)$	$H+(3,0)$	H	$H+(1,0)$
$H+(3,0)$	$H+(3,0)$	H	$H+(1,0)$	$H+(2,0)$

If we observe $f : G/H \to \mathbb{Z}_4$ we will see that, with $f(H + (x,0)) = x$, f is an isomorphism from G/H to $\mathbb{Z}_4$. In other words, $\mathbb{Z}_4 \times \mathbb{Z}_2/\langle(0,1)\rangle = \mathbb{Z}_4$. Actually, we have eliminated $\mathbb{Z}_2$ from the direct product by taking $(0,1)$ (as 0 is a neutral element for $\mathbb{Z}_4$ and 1 a generator for $\mathbb{Z}_2$, it left all elements of $\mathbb{Z}_4$ intact while sweeping across all of $\mathbb{Z}_2$).

7. $G = \mathcal{P}_3$ *and* $H = \{\emptyset,\{1\}\}$. We have $|\mathcal{P}_3| = 2^3 = 8$ (refer to page 18) and $|H| = 2$, so $|G/H| = 4$. First we have $H = H\Delta\{0\} = H\Delta\{1\}$, $H\Delta\{2\} = H\Delta\{1,2\} = \{\{2\},\{1,2\}\}$, $H\Delta\{3\} = H\Delta\{1,3\} = \{\{3\},\{1,3\}\}$ and $H\Delta\{2,3\} = H\Delta\{1,2,3\} = \{\{1,2,3\},\{2,3\}\}$. The multiplication table is:

$\cdot$	H	$H\Delta\{2\}$	$H\Delta\{3\}$	$H\Delta\{2,3\}$
H	H	$H\Delta\{2\}$	$H\Delta\{3\}$	$H\Delta\{2,3\}$
$H\Delta\{2\}$	$H\Delta\{2\}$	H	$H\Delta\{2,3\}$	$H\Delta\{3\}$
$H\Delta\{3\}$	$H\Delta\{3\}$	$H\Delta\{2,3\}$	H	$H\Delta\{2\}$
$H\Delta\{2,3\}$	$H\Delta\{2,3\}$	$H\Delta\{3\}$	$H\Delta\{2\}$	H

8. $G = \mathbb{R} \times \mathbb{R}$ *and* $H = \{(x,0) : \ x \in \mathbb{R}\}$. We have $G/H = \{H + (a,b) : \ (a,b) \in \mathbb{R} \times \mathbb{R}\}$. As $H + (a,b) = \{(x+a,b) : \ x \in \mathbb{R}\} = \{(x,b) : \ x \in \mathbb{R}\}$, cosets geometrically represent lines parallel to the x axis and the operation is addition which returns a line parallel to the x-axis, whose distance from the x-axis is the sum of distances from x-axis, of the two operands.

9. $G = \mathbb{R}\times\mathbb{R}$ *and* $H = \{(x,y) : \ y = -x\}$. It's $G/H = \{H+(a,b) : \ (a,b) \in \mathbb{R}\times\mathbb{R}\}$ and $H+(a,b) = \{(x+a,y+b) : \ y = -x\} = \{(x,y) : \ y-b = -x+a\} = \{(x,y) : y = -x + a + b\}$, i.e. a collection of lines parallel with $y = -x$. Operation is similar to the operation above, but with distances measured from $y = -x$.

10. $G = \mathbb{R} \times \mathbb{R}$ *and* $H = \{(x, y) : \ y = 2x\}$. We have $G/H = \{H + (a, b) : \ (a, b) \in \mathbb{R} \times \mathbb{R}\}$ with $H + (a, b) = \{(x, y) : \ y - b = 2x - 2a\} = \{(x, y) : \ y = 2x + b - 2a\}$, i.e. a collection of line parallel with. The operation is similar to the two previous operations.

Proposition. Let G be a group and H a normal subgroup of G. Then:

1. Every element of G/H is its own inverse if and only if $x^2 \in H$, for every $x \in G$.
2. The order of every element in G/H is a divisor of m if and only if $x^m \in H$, for every $x \in G$.
3. Every element of G/H has a finite order if and only if for every $x \in G$ there exists $n \in \mathbb{Z}^*$ such that $x^n \in H$.
4. Every element of G/H has a square root if and only if for every $x \in G$, there is some $y \in G$ such that $xy^2 \in H$.
5. G/H is cyclic if and only if there exists $a \in G$ such that for every $x \in G$ there exists $n \in \mathbb{Z}$ such that $xa^n \in H$.
6. If G is an Abelian group, let H_p be the set of all $x \in G$ whose order is a power of p. Then, H_p is a normal subgroup of G and G/H_p has no elements whose order is a nonzero power of p.
7. If G/H is Abelian, then H contains all the commutators of G.
8. Let K be a normal subgroup of G, and H a normal subgroup of K. If G/H is Abelian, then G/K and K/H are both Abelian.

Proof. *Ad* 1. *Necessity.* Let $Hx \in G/H$. Then, $Hx \cdot Hx = H$, i.e. $H(x^2) = H$, for all $x \in G$. As $x^2 \in H(x^2)$ it is also in H. So we have $x^2 \in H$, for all $x \in G$. *Sufficiency.* As H is normal, then G/H is a group and $Hx \in G/H$, for all $x \in G$ Let $x^2 \in H$, for every $x \in G$. Then we have[58] $H(x^2) = H$. By definition $Hx \cdot Hx = H(x^2)$ and we have $Hx \cdot Hx = H$. As $H \in G/H$ is a neutral element in G/H, Hx is its own inverse for all $x \in G$.

Ad 2. *Necessity.* Let $\operatorname{ord}(Hx) \mid m$, for every $Hx \in G/H$. That means that there exists $k \in \mathbb{Z}$ such that $m = k\operatorname{ord}(Hx)$. From that follows $(Hx)^m = (Hx)^{k\operatorname{ord}(Hx)} = \left((Hx)^{\operatorname{ord}(Hx)}\right)^k = e^k = e$. As, by definition, $(Hx)^m = H(x^m)$, $x^m \in H(x^m)$ and $(Hx)^m = H$ (so $H = H(x^m)$), we have $x^m \in H$, for all $x \in G$. *Sufficiency.* Let $x^m \in H$, for all $x \in G$. As H is normal, G/H is a group and $Hx \in G/H$ for all $x \in G$. As $x^m \in H$, for all $x \in G$, then $H = H(x^m)$. By definition, $H(x^m) = (Hx)^m$, so $H = (Hx)^m$. As H is a neutral element in G/H, we have $\operatorname{ord}(Hx) \mid m$, for all $x \in G$.

[58] Remember that $Ha = H$ if and only if $a \in H$.

Ad 3. *Necessity.* Suppose that for all $Hx \in G/H$ there exists $n \in \mathbb{N}$ such that $\operatorname{ord}(Hx) = n$. That implies $(Hx)^n = H$, i.e. $H(x^n) = H$. As $x^n \in H(x^n$, then also $x^n \in H$. In other words, there exists $n \in \mathbb{N} \subseteq \mathbb{Z}^*$, i.e. $\operatorname{ord}(Hx)$, such that $x^n \in H$. *Sufficiency.* As H is normal, we have G/H is a group and $Hx \in G/H$, for all $x \in G$. Suppose that for each $x \in G$ there exists $n \in \mathbb{Z}^*$ such that $x^n \in H$ and it follows that $H(x^n) = H$, for all $x \in G$. By definition, $(Hx)^n = H$ and then there also exists $m \in \mathbb{N}$ such that $(Hx)^m = H$. Therefore, $0 < \operatorname{ord}(Hx) \leq m$; in other words, order of each $Hx \in G/H$ is finite.

Ad 4. *Necessity.* Suppose that every $Hx \in G/H$ has a square root, i.e. there exists $Hy \in G/H$ such that $Hx = (Hy)^2$. That gives us $Hx = H(y^2)$. As $x \in Hx$, then also $x \in H(y^2)$, i.e. there exists $h \in H$ such that $x = hy^2$. Multiplying that by y^{-2} on the right gives us $xy^{-2} = h \in H$. We can take $z \in G$ such that $z = y^{-1}$, so $z^2 = y^{-2}$. Therefore, for all $x \in G$ there exists $z \in G$ such that $xz^2 \in H$. *Sufficiency.* Let for all $x \in G$ exist $y^2 \in G$ such that $xy^2 \in H$. As $xy^2 \in H$, then also $xz^{-2} \in H$, where $z^{-1} = y$. As $xz^{-2} \in H$, it follows that $H(xz^{-2}) = H$. By definition, $Hx \cdot H(z^{-2}) = H$, i.e. $Hx \cdot (Hz)^{-2} = H$. If we multiply that equality by $(Hz)^2 \in G/H$ on the right, we get $Hx = H \cdot (Hz)^2$. As H is a neutral element in G/H, we have $Hx = (Hz)^2$. In other words, for all $x \in G$ there exists $z \in G$ such that $Hx = (Hz)^2$. By that, every element in G/H has a square root.

Ad 5. *Necessity.* Suppose G/H is cyclic. Then, $G/H = \langle Ha \rangle$, for some $a \in G$. Also, any $Hx \in G/H$ can be written as a power of Ha, i.e. $Hx = (Ha)^k = H\left(a^k\right)$, for some $k \in \{0, 1, \ldots, \operatorname{ord}(Hx) - 1\}$. As $Hx = H\left(a^k\right)$, by a previous proposition it follows that $xa^{-k} \in H$. If we take $n = -k$, then we have that for all $x \in G$ there exists $n \in \mathbb{Z}$ such that $xa^n \in H$. *Sufficiency.* Let $a \in G$. Suppose that for all $x \in G$ there exists $n \in \mathbb{Z}$ such that $xa^n \in H$. From that we have $Hx = H(a^{-n})$, that is $Hx = (Ha)^{-n}$. If we take $k = -n$ we have that for all $x \in G$ there exists $k \in \mathbb{Z}$ such that $Hx = (Ha)^k$, for some $a \in G$. As $Hx, Ha \in G/H$ and G/H is a group, that means that $G/H = \langle Ha \rangle$.

Ad 6. Let G be an Abelian group, $p \in P$ and

$$H_p = \{a \in G : \ (\exists k \in \mathbb{N}_0)\left(\operatorname{ord}(a) = p^k\right)\}.$$

From definition we have $H_p \subseteq G$. If we take $a, b \in H_p$, then $\operatorname{ord}(a) = p^m$ and $\operatorname{ord}(b) = p^n$, for some $m, n \in \mathbb{N}_0$. Let $l = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) = p^{\min\{m,n\}}$. Let us denote $i = \min\{m, n\}$. Then, as $\operatorname{ord}(a) \mid l$ and $\operatorname{ord}(b) \mid l$, we have $a^l b^l = e$. From that, as G is Abelian, $(ab)^l = e$. That implies $\operatorname{ord}(ab) \mid l$, i.e. $\operatorname{ord}(ab) \mid p^i$. In other words, there exists $q \in \mathbb{N}$ (as order is positive integer) such that $p^i = q\operatorname{ord}(ab)$. Let, by fundamental theorem of arithmetic, $q = q_1 \cdots q_s$, for some $s \in \mathbb{N}$, where $q_j \in P$, for $j \in \{1, \ldots, s\}$. We have $p^i = q_1 \cdots q_s \operatorname{ord}(ab)$. Dividing by $q_1, \ldots, q_s$ give us:

$$\operatorname{ord}(ab) = \frac{p^i}{q_1 \cdots q_s}.$$

As $q_j \in P$ and $\operatorname{ord}(ab) \in \mathbb{N}$, there is only one possibility, and that is $q_j = p$, for all $j \in \{1, \ldots, s\}$. So we have:

$$\operatorname{ord}(ab) = \frac{p^i}{p^s} = p^{i-s}.$$

Also, notice that it is necessary that $i - s \geq 0$. So, order of ab is a power of p and $ab \in H_p$. Also, if we had $a \in H_p$ with $\operatorname{ord}(a) = p^m$, where $m \in \mathbb{N}_0$, then, as $\operatorname{ord}(a^{-1}) = \operatorname{ord}(a)$, we have $\operatorname{ord}(a^{-1}) = p^m$ and $a^{-1} \in H_p$. Now, let $x \in G$. If we took $y \in H_p$, we have $\operatorname{ord}(y) = p^m$, for some $m \in \mathbb{N}_0$. Let $k = \operatorname{ord}(y)$. Now, $xx^{-1} = e$ and $y^k = e$, we have $xy^k x^{-1} = e$. From a previous proposition, $xy^k x^{-1} = (xyx^{-1})^k$ and we have $(xyx^{-1})^k = e$. Therefore, $\operatorname{ord}(xyx^{-1}) \,|p^m$. That implies, following the same line of reasoning as for $\operatorname{ord}(ab)$, that order of xyx^{-1} is a power of p and $xyx^{-1} \in H_p$. Thus, H_p is a normal subgroup of G. From that follows that G/H_p is a quotient group.

Assume there exists $H_p x \in G/H_p$ such that $\operatorname{ord}(H_p x) = p^k$, for some $k \in \mathbb{N}$ and $x \in G$. Let us denote $l = p^k$. Then, $(H_p x)^l = H_p$, i.e. $H_p\left(x^l\right) = H_p$. That would mean that $x^l \in H_p$ and from that $\operatorname{ord}\left(x^l\right) = p^n$, for some $n \in \mathbb{N}_0$. From a previous proposition,

$$\operatorname{ord}\left(x^l\right) = \frac{\operatorname{lcm}(\operatorname{ord}(x), p^m)}{p^m}.$$

Therefore, as $\operatorname{ord}\left(x^l\right) = p^n$, we have:

$$p^n = \frac{\operatorname{lcm}(\operatorname{ord}(x), p^m)}{p^m}.$$

That equality multiplied by p^m is equivalent to $p^{n+m} = \operatorname{lcm}(\operatorname{ord}(x), p^m)$. Let $l = \operatorname{lcm}(\operatorname{ord}(x), p^m)$. That means that $l = p^{n+m}$ and, as $\operatorname{ord}(x) \,|\operatorname{lcm}(\operatorname{ord}(x), p^m)$, that $\operatorname{ord}(x) \,|p^m$. That would imply that $\operatorname{ord}(x)$ is a power of p and $x \in H_p$. But, that means that $G/H = \{H_p\}$. Then, as H_p is a neutral element, it must be $\operatorname{ord}(H_p) = 1 = p^0$, which is contrary to our assumption that there exists $H_p x \in G/H$ whose order is a non-zero power of $p \in P$.

Ad 7. Suppose G/H is an Abelian group. Then, $Hx \cdot Hy = Hy \cdot Hx$, for all $Hx, Hy \in G/H$. If we multiply that equality by $(Hy)^{-1}$ on the right and then by $(Hx)^{-1}$ on the right, we have $H = Hy \cdot Hx \cdot (Hy)^{-1} \cdot (Hx)^{-1}$. By definition, that is equivalent to $H = H(yxy^{-1}x^{-1})$. By a previous proposition, that implies $yxy^{-1}x^{-1} \in H$, for all $x, y \in H$. In other words, H contains all commutators of G.

Ad 8. Let H be a normal subgroup of K and K a normal subgroup of G. Then, H is a normal subgroup of G. Suppose G/H is Abelian. By the previous property, H contains all commutators of G. As H is a subset of K, then K also contains all commutators of G, i.e. $xyx^{-1}y^{-1} \in K$, for all $x, y \in G$. That implies, by a previous proposition, that $K\left(xyx^{-1}y^{-1}\right) = K$. As G/K is a quotient group, by definition we have $Kx \cdot Ky \cdot Kx^{-1} \cdot Ky^{-1} = K$, for all $x, y \in G$. Multiplying by $Ky \cdot Kx$ on the right, we have $Kx \cdot Ky = Ky \cdot Kx$, for all $x, y \in G$. Thus, G/K is Abelian. Similarly, as H contains all commutators of G, and K is a subset of G, then it also contains all the commutators of K. In the same line of reasoning, K/H is also Abelian.

□

Definition. Group G is called a **p-group** if the order of all elements of G is a power of p.

Proposition. Let G be a group, and H a normal subgroup of G. Then:

1. If every element of G/H has a finite order, and every element of H has finite order, then every element of G has finite order.
2. If G is Abelian, and if every element of G/H has a square root, and every element of H has a square root, then every element of G has a square root.
3. Let $p \in P$. If G/H and H are p-groups, then G is a p-group.
4. If G/H and H are finitely generated, then G is finitely generated.

Proof. *Ad* 1. Suppose that for all $Hx \in G/H$ exists $k \in \mathbb{N}$ such that $\operatorname{ord}(Hx) = k$. Furthermore, assume that for all $h \in H$ there exists $k \in \mathbb{N}$ such that $\operatorname{ord}(h) = k$. Let $a \in G$. Then there exists $Ha \in G/H$ with $\operatorname{ord}(Ha) = m$, for some $m \in \mathbb{N}$. So we have $(Ha)^m = H$, i.e. $H(a^m) = H$. From that we have $a^m \in H$ and there exists $n \in \mathbb{N}$ such that $\operatorname{ord}(a^m) = n$. By a previous proposition:

$$\operatorname{ord}(a^m) = \frac{\operatorname{lcm}(\operatorname{ord}(a), m)}{m}.$$

But, as $\operatorname{ord}(a^m) = n$, we get $mn = \operatorname{lcm}(\operatorname{ord}(a), m)$. As $\operatorname{ord}(a) \,|\operatorname{lcm}(\operatorname{ord}(a), m)$, there exists $k \in \mathbb{N}$ (as m is order of Ha) such that $\operatorname{lcm}(\operatorname{ord}(a), m) = k\operatorname{ord}(a)$. From that follows $mn = k\operatorname{ord}(a)$, and from that $\operatorname{ord}(a) = \frac{mn}{k}$. As m and n are finite by assumption, and $k \in \mathbb{N}$, then $\frac{mn}{k}$ is finite and so is $\operatorname{ord}(a)$, for all $a \in G$.

Ad 2. Let $x \in G$. Then there exists $Hx \in G/H$. Then, as all elements in G/H have a square root, there exists $Hy \in G/H$, for some $y \in G$, such that $Hx = (Hy)^2$, i.e. $Hx = H(y^2)$. But, that implies $xy^{-2} \in H$. So, as all elements in H have a square

root, there exists $h \in H$ such that $xy^{-2} = h^2$. If we multiply that equality by y^2 on the right, we have $x = h^2y^2$. As $x \in G$ (and by that also $h^2y^2 \in G$) and G is Abelian, we have $x = (hy)^2$. As $h \in H \subseteq G$ and $y \in G$ and G is a group, then $hy \in G$. We can denote $hy = z$. Therefore, for all $x \in G$ there exists $z \in G$ such that $x = z^2$, i.e. all elements in G have a square root.

Ad 3. Let $x \in G$. Then there exists $Hx \in G/H$. As G/H is a p-group, we have $\operatorname{ord}(Hx) = m$, where $m = p^k$, for some $k \in \mathbb{N}_0$. Thus, $(Hx)^m = H$, that is $H(x^m) = H$. From that we have $x^m \in H$. As H is a p-group, then $\operatorname{ord}(x^m) = n$, where $n = p^l$, for some $l \in \mathbb{N}_0$. By a previous proposition:

$$\operatorname{ord}(x^m) = \frac{\operatorname{lcm}(\operatorname{ord}(x), m)}{m}.$$

Multiplying by m and using the fact that $\operatorname{ord}(x^m) = p^l$ and $m = p^k$ we get:

$$p^{l+k} = \operatorname{lcm}\left(\operatorname{ord}(x), p^l\right).$$

As $\operatorname{ord}(x) \,|\operatorname{lcm}\left(\operatorname{ord}(x), p^l\right)$, i.e. $\operatorname{ord}(x) \,|p^{l+k}$, then, following the similar reasoning as in a previous proposition, we have $\operatorname{ord}(x) = p^s$, where $s \in \mathbb{N}_0$, for all $x \in G$.

Ad 4. Let $x \in G$. Then there exists $Hx \in G/H$. As G/H is finitely generated, then there exists a family $S = \{Hs_1, \ldots, Hs_m\}$, for some $m \in \mathbb{N}$, family $T = S \cup \{(Hs)^{-1} \in G : \ Hs \in S\}$ and a function $f : T^k \to G/H$, where $k \in \mathbb{N}$ defined with:

$$f(Ht_1, \ldots, Ht_n) = \prod_{i=1}^{k} (Ht_i).$$

But, as G/H is a group with coset multiplication such that $Hx \cdot Hy = H(xy)$, then:

$$\prod_{i=1}^{k} (Ht_i) = H\left(\prod_{i=1}^{k} t_i\right).$$

From that we have $f(Ht_1, \ldots, Ht_n) = H\left(\prod_{i=1}^{k} t_i\right)$. In addition, for every element $Hx \in G/H$ there exists $k \in \mathbb{N}$ and $X \in T^k$ such that $f(X) = Hx$. Also, as H is finitely generated then there exists $U = \{u_1, \ldots, u_n\}$, for some $n \in \mathbb{N}$, $V = U \cup \{u^{-1} \in G : \ u \in U\}$ and $g : V^k \to H$, where $k \in \mathbb{N}$ defined with:

$$g(v_1, \ldots, v_k) = \prod_{i=1}^{k} v_i.$$

Also, for every element $h \in H$ there exists $l \in \mathbb{N}$ and $Y \in V^k$ such that $g(Y) = h$. Let $x \in G$, then there exists $Hx \in G/H$, with forementioned property. As $f(X) = Hx$,

i.e. $H\left(\prod_{i=1}^{k} t_i\right) = Hx$, then, by a previous proposition $\left(\prod_{i=1}^{k} t_i\right) x^{-1} \in H$. Let $\left(\prod_{i=1}^{k} t_i\right) x^{-1} = h$. As $h \in H$, then it has a forementioned property with $g(Y) = h$, i.e. there exists $l \in \mathbb{N}$ such that $g(v_1, \ldots, v_l) = h$. But, $g(v_1, \ldots, v_l) = \prod_{i=1}^{l} v_i$, so:

$$\left(\prod_{i=1}^{k} t_i\right) x^{-1} = \prod_{i=1}^{l} v_i.$$

Multiplying the above equation by x on the right and $\left(\prod_{i=1}^{l} v_i\right)^{-1} = \prod_{i=l}^{1} \left(v_i^{-1}\right)$ on the left, we have:

$$x = \left(\prod_{i=1}^{k} t_i\right) \left(\prod_{i=l}^{1} \left(v_i^{-1}\right)\right).$$

Therefore, each $x \in G$ can be shown as a finite product of $t_i \in T$ and $v_i \in V$, i.e. a finite product of $g \in T \cup V$. As T and V are finite, then also is $T \cup V$ and that implies that G is finitely generated.

□

Proposition. Let G be a group and H a normal subgroup of G. Then,

1. For each $a \in G$, the order of the element $Ha \in G/H$ is a divisor of the order of $a \in G$.
2. If $[G : H] = m$, the order of every element of G/H is a divisor of m.
3. If $[G : H] = p$, for $p \in P$, then the order of every element[59] $a \in G \backslash H$ is a multiple of p.
4. If G has a normal subgroup of index p, where $p \in P$, then G has at least one element of order p.
5. If $[G : H] = m$, then $a^m \in H$ for every $a \in G$.

Proof. *Ad* 1. Let $a \in G$ and $\operatorname{ord}(a) = m$. Then there exists $Ha \in G/H$. From $\operatorname{ord}(a) = m$ we have $a^m = e$. As H is a normal subgroup of G, it must be that $e \in H$, that is $a^m \in H$. That implies $H(a^m) = H$. By a previous proposition that is equivalent to $(Ha)^m = H$. As H is a neutral element in G/H, then $\operatorname{ord}(Ha) \mid m$, i.e. $\operatorname{ord}(Ha) \mid \operatorname{ord}(a)$.

Ad 2. Let $[G : H] = m$, i.e. the number of different cosets of H in G equals m. But, G/H contains, by definition, all the cosets of H in G. From that it follows $|G/H| = m$.

[59] Be careful not to confuse G/H which is a quotient group and $G \backslash H$ which is set difference, i.e. the set containing all elements of G which are not in H.

By corollary of Lagrange's theorem, order of all $Ha \in G/H$ divide order of G/H; in other words, $\operatorname{ord}(Ha) \mid m$, for all $a \in G$.

Ad 3. Let $[G : H] = p$ and $a \in G \backslash H$ with $\operatorname{ord}(a) = m$. As $a \in G$, then there exists $Ha \in G/H$. We have $\operatorname{ord}(Ha) \mid \operatorname{ord}(a)$, i.e. $\operatorname{ord}(Ha) \mid m$. From that we have that there exists $q \in \mathbb{N}$ such that $m = \operatorname{ord}(Ha)\, q$. Also, as $\operatorname{ord}(Ha) \mid p$, we have that either $\operatorname{ord}(Ha) = 1$ or $\operatorname{ord}(Ha) = p$. Suppose $\operatorname{ord}(Ha) = 1$. That would mean that $Ha = H$ which would impliy $a \in H$ bringing us to a contradiction with $a \in G \backslash H$. So it can only be $\operatorname{ord}(Ha) = p$ and we have $m = pq$, i.e. $\operatorname{ord}(a) = pq$, for some $q \in \mathbb{N}$.

Ad 4. Let $[G : H] = p$ and $a \in G$. If it were $G \backslash H = \emptyset$, we would have that $G = H$ and that would mean $[G : H] = \frac{|G|}{|H|} = \frac{|G|}{|G|} = 1$, but $1 \notin P$. Therefore, there must exist $a \in G \backslash H$ and from a previous proposition, $\operatorname{ord}(a) = pq$, for some $q \in \mathbb{N}$, for all $a \in G \backslash H$. Suppose $a^p \neq e$, for all $a \in G \backslash H$. That would mean that $a^p \notin H$, for all $a \in G \backslash H$. As $a^p \notin H$, then $a^p \in G \backslash H$ and we have that $\operatorname{ord}(a^p) = pr$, for some $r \in \mathbb{N}$. But, also:

$$\operatorname{ord}(a^p) = \frac{\operatorname{ord}(a)}{\gcd(\operatorname{ord}(a), p)} = \frac{pq}{\gcd(pq, p)} = \frac{pq}{p} = q.$$

As $\operatorname{ord}(a^p) = q$, we have that p and q are relatively prime, which is a contradiction to the previous conclusion that $\operatorname{ord}(a^p) = pr$. Therefore, there must exist some $a \in G \backslash H$ such that $a^p = e$, i.e. $\operatorname{ord}(a) = p$.

Ad 5. Suppose $[G : H] = m$. Then, $\operatorname{ord}(Ha) \mid m$ and we have $(Ha)^m = H$. That is equivalent to $H(a^m) = H$, meaning $a^m \in H$.

□

Proposition. Let G be a group and $C = \{a \in G : (\forall x \in G)(xa = ax)\}$ center of G. If G/C is cyclic, then G is Abelian.

Proof. We already proved that C is a normal subgroup of G. Suppose $G/C = \langle Cx \rangle$ for some $x \in G$. Then, if we take $a, b \in G$, there exist $m, n \in \{0, 1, \ldots, \operatorname{ord}(Cx) - 1\}$ such that $Ca = (Cx)^m = C(x^m)$ and $Cb = (Cx)^n = C(x^n)$. Then, by previous proposition, $ax^{-m}, bx^{-n} \in C$, that is, there exist $c_1, c_2 \in C$ such that $ax^{-m} = c_1$ and $bx^{-n} = c_2$. Multiplying those two equalities by x^m and x^n, respectivily, we get $a = c_1 x^m$ and $b = c_2 x^n$. Then, $ab = c_1 x^m c_2 x_n$. As $c_1 x = x c_1$ and $c_2 x = x c_2$, for all $x \in G$, we can rearrange those elements to get $ab = x^m c_1 c_2 x_n = x^m c_2 c_1 x_n$, that is $ab = c_2 x^m x^n c_1$. As $x^m x^n = x^{m+n} = x^{n+m} = x^n x^m$, we have $ab = c_2 x^n x^m c_1$, and from that $ab = c_2 x^n c_1 x^m = ba$. Therefore, $ab = ba$, for all $a, b \in G$ and G is Abelian.

□

Proposition. Let G be a group. Then:

1. $G/G = \{G\}$ with $[G : G] = 1$.

2. $G/\{e\} = \{\{a\} : \ a \in G\}$ with $[G : \{e\}] = |G|$.

Proof. *Ad* 1. First, G is a subgroup of G as $ab \in G$, for all $a, b \in G$ and $a^{-1} \in G$, for all $a \in G$, by group axioms. Also if we take $x \in G$ and $y \in G$, then $y^{-1} \in G$, and also $xy^{-1} \in G$. But, also $yxy^{-1} \in G$. Therefore, G is a normal subgroup of G. Now, we will prove that $Ga = G$, for all $a \in G$. If we take $ga \in Ga$, for some $g \in G$, then also $ga \in G$ (G is a group and closed with respect to products), so $Ga \subseteq G$. If we take $g \in G$, we have $g = ge = g(a^{-1}a)$ which implies $(ga^{-1})a \in G$. But, also $(ga^{-1})a \in Ga$, i.e. $g \in Ga$. Therefore, $G \subseteq Ga$. From that we have $G = Ga$. So, $G/G = \{G\}$. The number of different cosets is obviously 1 so $[G : G] = 1$.

Ad 2. We have that $\{e\}$ is a trivial subgroup of G. It is also normal as $xex^{-1} = e \in \{e\}$, for all $x \in G$. Now, let $E = \{e\}$. Then $Ea = \{ea : \ e \in E\} = \{a\}$, for all $a \in G$. Therefore, $G/\{e\} = \{\{a\} : a \in G\}$. $G/\{e\}$ contains each $a \in G$ (altough embedded in a set) so $[G : \{e\}] = |G|$.

□

Proposition. Let $C = \{y \in G : \ (\forall x \in G)(xy = yx)\}$ be center of group G and $[x] = \{yxy^{-1} \in G : \ y \in G\}$ conjugacy class for $x \in G$. Then, $a \in C$ if and only if $|[a]| = 1$.

Proof. *Necessity.* Let $a \in C$. Then, for all $x \in G$, $xa = ax$. That is, for all $x \in G$, $a = xax^{-1}$. We have $[a] = \{xax^{-1} \in G : \ x \in G\} = \{a\}$. Therefore, $|[a]| = 1$. *Sufficiency.* Suppose $|[a]| = 1$. Now, taking that fact with $a \in [a]$, then $[a] = \{a\}$. That means that, for all $x \in G$, $xax^{-1} = a$. In other words, for all $x \in G$, $xa = ax$ and it must be that $a \in C$.

□

Proposition. Let G be a finite group, C center of a group and

$$\mathcal{K} = \{[x] : \ (x \in G) \wedge (|[x]| \neq 1)\}.$$

Then, $\mathcal{K} \cup \{C\}$ is a partition of G and

$$|G| = |C| + \sum_{K \in \mathcal{K}} |K|.$$

Proof. If we take $x \in G$, then $x \in [x]$. If $|[x]| \neq 1$, then $x \in [x] \in \mathcal{K} \cup \{C\}$ such that $x \in [x]$. If $|[x]| = 1$, then, by a previous proposition, $x \in C \in \mathcal{K} \cup \{C\}$. Let

$x_1, x_2 \in G$. Then, there exist $S_1, S_2 \in \mathcal{K} \cup \{C\}$ such that $x_1 \in S_1$ and $x_2 \in S_2$. Then, either $S_i = [x_i]$, or $S_i = C$, for $i \in \{1, 2\}$. Suppose $x_1 = x_2$. That way, $[x_1] = [x_2]$. If $|[x_1]| = |[x_2]| = 1$, we have $x_1, x_2 \in C$ and $S_1 = C = S_2$. If $|[x_1]|, |[x_1]| \neq 1$, then simply, $S_1 = [x_1] = [x_2] = S_2$. Therefore, $\mathcal{K} \cup \{C\}$ is a partition of G. The number of elements of G is equal to the sum of elements in C and sums of elements in each conjugacy class whose order is not 1.

□

Remark. From now on, we will denote $A - B = A \backslash B$ to aviod confusion with quotient group A/B.

Lemma. Let $p \in P$ and $k \in \mathbb{N}$. Then, $p \nmid (p^k - 1)$.

Proof. Suppose $p|(p^k - 1)$. Then, $p^k - 1 = pq$, for some $q \in \mathbb{Z}$. That implies $p^k - pq = 1$ and $p(p^{k-1} - q) = 1$. That would mean that $p = 1$ and $(p^{k-1} - q) = 1$. Yet, $p \in P$ and $1 \notin P$, so $p \notin P$ which is a contradiction to our assumption.

□

Proposition. Let $k \in \mathbb{N} - \{0\}$. Let G be a group with $|G| = p^k$, where $p \in P$. If C is a center of G, then $|C| = p^l$, where $l \in \mathbb{N} - \{0\}$ and $l \leq k$.

Proof. From a previos proposition we have $|G| = |C| + \sum_{K \in \mathcal{K}} |K|$, where $\mathcal{K}$ is a family of conjugacy classes whose order is not 1. Then, due to a previous proposition, each conjugacy class divides order of $|G|$. Also $|C|$ divides $|G|$ and it must be that $|C| = p^l$, where $l \in \mathbb{N}$ and $|K| = p^{f(K)}$, for all $K \in \mathcal{K}$. So, we have:

$$p^k = p^l + \sum_{K \in \mathcal{K}} p^{f(K)}.$$

Let $m = \min \{l\} \cup \{f(K) : \ K \in \mathcal{K}\}$. Then,

$$p^k = p^m \left(p^{l-m} + \sum_{K \in \mathcal{K}} p^{f(K)-m} \right).$$

As $k \in \mathbb{N} - \{0\}$, we have $p^k \neq 1$. Therefore, it must be that $p^m \neq 1$ or $p^{l-m} + \sum_{K \in \mathcal{K}} p^{f(K)-m} \neq 1$. The sum could equal 1 only if $p^m = p^k$ and if it had no conjugacy classes with $p^{l-m} = 1$ (as order of center can never be zero). But, that would mean that $l = m$ and we would have $p^k = p^l$, so $l = k$ and $|C| = p^l$, where $l \in \mathbb{N} - \{0\}$. Now, if it were that $p^m = 1$, the sum would have to equal p^k. But, as $p^m = 1$, i.e. $m = 0$ it would mean that either $f(K) = 0$ for some $K \in \mathcal{K}$ or $|C| = 1$. It cannot be that $f(K) = 0$,

for some $K \in \mathcal{K}$ as then that conjugacy class would have order 1 and its representative would be in C, contradicting our assumption. But, if it were that $|C| = 1$, we would have $p^k = 1 + pS$, where S is the sum of conjugacy class orders (we can factor out p as all $p^{f(K)} \neq 1$; that would put them in center of the group). Then, $p^k - 1 = pS$ would mean $p|(p^k - 1)$ which is, by a previous lemma, impossible. Therefore, all conjugacy classes must contain more that one element and so does center and we have $|C| = p^l$, $l \in \mathbb{N} - \{0\}$.

□

Lemma. Let G be a group with $|G| = p$, where $p \in P$. Then, G is cyclic.

Proof. Let $a \in G$, $a \neq e$. Then, due to corollary of Lagrange's theorem, we have $\operatorname{ord}(a) | p$. So, either $\operatorname{ord}(a) = 1$ or $\operatorname{ord}(a) = p$. But, only a neutral element has order 1 ($a^1 = e$ would imply $a = e$) so $\operatorname{ord}(a) = p$. We have, by a previous proposition, $|\langle a \rangle| = \operatorname{ord}(a) = p$. As also $\langle a \rangle \subseteq G$, it follows that $\langle a \rangle = G$, i.e. G is cyclic with generator a.

□

Proposition. Let G be a group with $|G| = p^2$, where $p \in P$. Then, G is Abelian.

Proof. By a previous proposition, either $|C| = p$ or $|C| = p^2$. If it were that $|C| = p^2$, we would have $|C| = |G|$ and, as $C \subseteq G$, that $C = G$. From that, as C is Abelian, G is Abelian. Now, assume $|C| = p$. Then, as C is a normal subgroup of G, we have $|G/C| = [G : C] = \frac{p^2}{p} = p$. From that we have, by a previous lemma, that G/C is cyclic. From a previous proposition it follows that G is Abelian.

□

Proposition. Let G be a group with $|G| = p^2$, where $p \in P$. Then, either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. By corollary of Lagrange's theorem, orders of elements in a group divide order of G. Therefore, for all $a \in G$, $\operatorname{ord}(a) \in \{1, p, p^2\}$. Only one element has order 1 and that is e, leaving $p^2 - 1$ other elements in disposal. Now, suppose there exists $a \in G$ such that $\operatorname{ord}(a) = p^2$. Then, $|\langle a \rangle| = p^2$. So, as $|\langle a \rangle| = |G|$ and $\langle a \rangle \subseteq G$, we have $G = \langle a \rangle$, i.e. G is cyclic group of order p^2. By a previous theorem, $G \cong \mathbb{Z}_{p^2}$.

If there does not exist $a \in G$ such that $\operatorname{ord}(a) = p^2$, there must be $p^2 - 1$ elements of order p. If we take $a \in G$, $a \neq e$, we have $\langle a \rangle = p$. Then $|G - \langle a \rangle| = p^2 - p$, i.e. $G - \langle a \rangle \neq \emptyset$. Then we can take $b \in G - \langle a \rangle$. Again, it must be that $\operatorname{ord}(b) = p$ and we have $|\langle b \rangle| = p$. Both $\langle a \rangle$ and $\langle b \rangle$ are normal subgroups of G. If it were that

$b^k \in \langle a \rangle$, we would have $\langle a \rangle = \langle b^k \rangle$ (as, by a previous proposition, $\operatorname{ord}(b^k) = p$ and $\operatorname{ord}(a) = p$ implies $\langle b^k \rangle = \langle a \rangle$). But, as $b^k \in \langle b \rangle$ and $\operatorname{ord}(b^k) = \operatorname{ord}(b)$ we have $\langle b^k \rangle = \langle b \rangle$, i.e. $\langle a \rangle = \langle b \rangle$. So, if we take $b \in \langle b \rangle$ then there exists $a^l \in \langle a \rangle$ such that $b = a^l$. But, that would mean that $b \in \langle a \rangle$ which is contrary to our assumption that $b \in G - \langle a \rangle$. Therefore, $\langle a \rangle \cap \langle b \rangle = \{e\}$. Now, let us observe $\langle a \rangle \langle b \rangle = \{a^k b^l \in G : \ k, l \in [0, \ldots, p-1] \cap \mathbb{Z}\}$. Obviously, $\langle a \rangle \langle b \rangle \subseteq G$ (as it contains only elements from G). And, as $a^k \neq b^l$, for all $k \in [1, \ldots, p-1] \cap \mathbb{Z}$ and $l \in [0, \ldots, p-1]$, we have $(p-1)p = p^2 - p$ different elements of the form $a^k b^l$. But if we allow $k = 0$, we have eb^l, where there are p elements, we have $|\langle a \rangle \langle b \rangle| = p^2 - p + p = p^2$. Therefore, we have $\langle a \rangle \langle b \rangle = G$. By a previous proposition, we have $G \cong \langle a \rangle \times \langle b \rangle$. But, as $|\langle a \rangle| = |\langle b \rangle| = p$ then $\langle a \rangle \cong \langle b \rangle \cong \mathbb{Z}_p$. So we have $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

□

Proposition. In $\mathbb{Q}/\mathbb{Z}$, every element has finite order.

Proof. As $\mathbb{Q}$ is Abelian, then $\mathbb{Z}$ is a normal subgroup of $\mathbb{Q}$ (as it also satisfies $a+b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$ and $-a \in \mathbb{Z}$ for all $a \in \mathbb{Z}$). Let $\mathbb{Z} + q \in \mathbb{Q}/\mathbb{Z}$. Let $q \in \mathbb{Q}$. Then there exists $\mathbb{Z} + q = \{z + q \in \mathbb{Q} : \ z \in \mathbb{Z}\}$. Suppose that for all $n \in \mathbb{N}$ we have $n(\mathbb{Z} + q) \neq \mathbb{Z}$. That expression is equivalent to $\mathbb{Z} + nq \neq \mathbb{Z}$. That would impliy that $nq \notin \mathbb{Z}$, for all $q \in \mathbb{Q}$. But, as $n \in \mathbb{N}$, and $\mathbb{Q} = \{\frac{m}{n} : \ m \in \mathbb{Z}, \ n \in \mathbb{N}\}$, there exists $q = \frac{m}{n} \in \mathbb{Q}$, where $m \in \mathbb{Z}$. Thus, $n\frac{m}{n} = m \in \mathbb{Z}$. Therefore, there exists $q \in \mathbb{Q}$ such that $nq \in \mathbb{Z}$, which is a contradiction to our assumption that for all $n \in \mathbb{N}$ we have $nq \notin \mathbb{Z}$. So there must exist $n \in \mathbb{N}$ such that $n(\mathbb{Z} + q) = \mathbb{Z}$. In other words, all $\mathbb{Z} + q \in \mathbb{Q}/\mathbb{Z}$ are of finite order.

□

The fundamental homomorphism theorem

Remark. From now on, we will denote homomorphism from G to H with kernel K as $f : G \underset{K}{\longrightarrow} H$.

Lemma. Let G be a group and H a subgroup of G. Let $f : G \underset{K}{\longrightarrow} H$ be a homomorphism. Then $f(a) = f(b)$ if and only if $Ka = Kb$.

Proof. *Necessity.* Let $f(a) = f(b)$. Then, $f(a)\left[f(b)\right]^{-1} = e$. As f is homomorphism, we have $f(a)f(b^{-1}) = f(ab^{-1}) = e$. But, that means that $ab^{-1} \in K$. From a previous proposition, as kernel is a normal subgroup of G, that implies $Ka = Kb$. *Sufficiency.* Let $Ka = Kb$. Then, by a previous proposition $ab^{-1} \in K$, i.e. $f(ab^{-1}) = e$. As f is a homomorphism, we have $f(a)f(b^{-1}) = f(a)\left[f(b)\right]^{-1} = e$. Multiplying by $f(b)$ on the right gives us $f(a) = f(b)$.

□

Theorem (FHT). Let $f : G \underset{K}{\longrightarrow} H$ be a homomorphism, where G is a group and H a subgroup of G. Suppose[60] $\operatorname{ran}(f) = H$. Then, $H \cong G/K$.

Proof. As K is a normal subgroup of G, quotient group G/K is well defined. Let us define a mapping $g : G/K \to H$ with $g(Kx) = f(x)$. As $Kx \in G/H$ if and only if $x \in G$, then g is defined for $x \in G$ as f is defined for all $x \in G$ (f is a function). If $Kx_1 = Kx_2$, then, by a previous lemma, $f(x_1) = f(x_2)$, i.e. $g(Kx_1) = g(Kx_2)$. Therefore, g satisfies property of uniqueness and is a function. *Injectivity.* Let $g(Kx_1) = g(Kx_2)$. Then, $f(x_1) = f(x_2)$. Previous lemma then implies $Kx_1 = Kx_2$. *Surjectivity.* As $H = \operatorname{ran}(f)$, we can take $f(x) \in H$, where $x \in G$. As $x \in G$, there exists $Kx \in G/K$. Therefore $g(Kx) = f(x)$. Thus, g is a bijection. Now, $g((Kx_1)(Kx_2)) = g(K(x_1x_2)) = f(x_1x_2)$. As f is a homomorphism, $f(x_1x_2) = f(x_1)f(x_2) = g(Kx_1)g(Kx_2)$. Then, g is an isomorphism and $H \cong G/K$.

□

Proposition. Let G and H be groups and $K \trianglelefteq G$. If $G/K \cong H$, then there exists a homomorphism $f : G \underset{K}{\longrightarrow} H$.

Proof. As $G/K \cong H$, then there exists an isomorphism $g : G/K \to H$. Also, by a previous proposition, G/K is a homomorphic image of G, so there exists a surjective

[60] If it is not, we can always disregard elements in H that have no originals by selecting $f : G \underset{K}{\longrightarrow} \operatorname{ran}(f)$.

homomorphism $k : G \underset{K}{\longrightarrow} G/K$ with $k(x) = Kx$. As g and k are well defined functions with $\text{dom}\,(g) = \text{cod}\,(k)$, then there exists a well-defined function $g \circ k : G \to H$. We will show that $g \circ k$ is a homomorphism. We have $[g \circ k](xy) = g(k(xy)) = g(K(xy)) = g((Kx)(Ky)) = g(Kx)g(Ky) = g(k(x))g(k(y)) = [g \circ k](x)[g \circ k](y)$. Therefore, $g \circ k$ is a homomorphism (and it is surjective, as projective homomorphism k is surjective and isomorphism g is surjective). Now, $\ker([g \circ k]) = \{x \in G : \ [g \circ k](x) = e\} = \{x \in G : g(Kx) = e\}$. But, $g(Kx) = e$ implies that $Kx \in \ker(g)$. But, as g is an isomorphism, kernel of g contains only one element, and that is the neutral element in G/K and that is K. In other words $\ker(g) = \{K\}$. So, if $Kx \in \ker(g)$, then $Kx \in \{K\}$ and it has to be $Kx = K$. From that we have $x \in K$. So, $\ker([g \circ k]) = \{x \in G : \ x \in K\} = K$. Thus, we can take $f(x) = [g \circ k](x)$, for all $x \in G$ and we have $f : G \underset{K}{\longrightarrow} H$.

□

Proposition. Map $f : \mathbb{Z}/(nk)\mathbb{Z} \underset{\langle n\mathbb{Z}+k\rangle}{\longrightarrow} \mathbb{Z}/k\mathbb{Z}$ defined with $f(n\mathbb{Z} + x) = k\mathbb{Z} + x$ is a homomorphism. Also, $(\mathbb{Z}/n\mathbb{Z}) / \langle n\mathbb{Z} + k\rangle = \mathbb{Z}/k\mathbb{Z}$.

Proof. Obviously, f is defined for all $n\mathbb{Z}+x \in \mathbb{Z}/n\mathbb{Z}$. If we take $n\mathbb{Z}+x = n\mathbb{Z}+y$, then $x \equiv y \pmod{n}k$. But, that implies that $x \equiv y \pmod{k}$, so $k\mathbb{Z} + x = k\mathbb{Z} + y$. Therefore, f is well-defined. Now, $f((n\mathbb{Z} + x) + (n\mathbb{Z} + y)) = f(n\mathbb{Z} + (x + y)) = k\mathbb{Z} + (x + y)$. By definition of coset multiplication (here addition), $k\mathbb{Z} + (x + y) = (k\mathbb{Z} + x) + (k\mathbb{Z} + y) = f(n\mathbb{Z} + x) + f(n\mathbb{Z} + y)$.

Now, $\ker(f) = \{n\mathbb{Z} + x \in \mathbb{Z}/n\mathbb{Z} : \ f(n\mathbb{Z} + x) = k\mathbb{Z}\}$. As $f(n\mathbb{Z} + x) = k\mathbb{Z}+x$, $k\mathbb{Z} + x = k\mathbb{Z}$ implies $x \in k\mathbb{Z}$, i.e. $x = km$, for some $m \in \mathbb{Z}$. In other words, $k|x$. Therefore, $\ker(f) = \{n\mathbb{Z} + x \in \mathbb{Z}/n\mathbb{Z} : \ k|x\}$. If we take $n\mathbb{Z} + km \in \ker(f)$, then $n\mathbb{Z} + km = m(n\mathbb{Z} + k)$. That is, $n\mathbb{Z} + km$ is a "power" (in additive notation) of $n\mathbb{Z} + k$, so $n\mathbb{Z} + km \in \langle n\mathbb{Z} + k\rangle$. That means that $\ker(f) \subseteq \langle n\mathbb{Z} + k\rangle$. If we take $m(n\mathbb{Z} + k) \in \langle n\mathbb{Z} + k\rangle$, then, $m(n\mathbb{Z} + k) = n\mathbb{Z}+km$. So, $m(n\mathbb{Z} + k) \in \ker(f)$. From that we have $\langle n\mathbb{Z} + k\rangle \subseteq \ker(f)$ and $\ker(f) = \langle n\mathbb{Z} + k\rangle$.

□

Remark. From the following theorem, we have, adopting less formal notations, that e.g. $\mathbb{Z}_{20}/\langle 5\rangle = \mathbb{Z}_5$, $\mathbb{Z}_6/\langle 2\rangle = \mathbb{Z}_2$, $\mathbb{Z}_6/\langle 3\rangle = \mathbb{Z}_3$, etc.

Problem. Let $\alpha : \mathcal{F}(\mathbb{R}) \to \mathbb{R}$ be defined by $\alpha(f) = f(1)$ and let $\beta : \mathcal{F} \to \mathbb{R}$ be defined by $\beta(f) = f(2)$.

1. Prove that α and β are homomorphisms from $\mathcal{F}(\mathbb{R})$ onto $\mathbb{R}$;
2. Let $J = \{f \in \mathcal{F}(\mathbb{R}) : \ f(1) = 0\}$ and $K = \{f \in \mathcal{F}(\mathbb{R}) : \ f(2) = 0\}$. use the FHT to prove that $\mathbb{R} \cong \mathcal{F}/J$ and $\mathbb{R} \cong \mathcal{F}/K$.

Solution. *Ad* 1. As $\mathcal{F}(\mathbb{R})$ contains all functions that are defined on $\mathbb{R}$ and so in $1, 2 \in \mathbb{R}$, then α and β are also defined. Same goes for uniqueness. Then, $\alpha(f+g) = [f+g](1)$. By definition, $[f+g](x) = f(x) + g(x)$, for all $x \in \mathbb{R}$. Then, $\alpha(f+g) = f(1) + g(1) = \alpha(f) + \alpha(g)$. Same goes for β, i.e. they are both homomorphisms from $\mathcal{F}(\mathbb{R})$ onto $\mathbb{R}$. *Ad* 2. We have $\ker(\alpha) = \{f \in \mathcal{F}(\mathbb{R}) : \ \alpha(f) = 0\} = \{f \in \mathcal{F}(\mathbb{R}) : \ f(1) = 0\}$. Similarly, $\ker(\beta) = \{f \in \mathcal{F}(\mathbb{R}) : \ f(2) = 0\}$. We see that $\ker(\alpha) = J$ and $\ker(\beta) = K$. By FHT, we have $\mathbb{R} \cong \mathcal{F}/J$ and $\mathbb{R} \cong \mathcal{F}/K$.

Proposition. Let G be an Abelian group. Let $H = \{x^2 : \ x \in G\}$ and $K = \{x \in G : x^2 = e\}$. Then, $H \cong G/K$.

Proof. We have $H \subseteq G$ by definition. Then, if we take $x^2, y^2 \in H$, then $x^2, y^2 \in G$ and, as G is Abelian, $x^2y^2 = (xy)^2$. Therefore, as $(xy)^2 \in H$, also $x^2y^2 \in H$. Also, as $x^2 \in H$ then $x^2 \in G$ and there exists $x^{-2} \in G$ such that $x^2x^{-2} = e$. But, $x^{-2} = (x^{-1})^2$, so $(x^{-1})^2 \in H$. Thus, H is a subgroup of G and by a previous proposition, as G is Abelian, then H is a normal subgroup of G. Let $f : G \to H$ be a mapping with $f(x) = x^2$. Then, f is obviously a well-defined function. We have $f(xy) = (xy)^2$. As G is Abelian, so is H and $(xy)^2 = x^2y^2 = f(x)f(y)$, for all $x, y \in G$. Therefore, f is a homomorphism and $\ker(f) = \{x \in G : \ f(x) = e\} = \{x \in G : \ x^2 = e\} = K$. By FHT we have $G/K \cong H$.

□

Proposition. Let G be a group, $I(G) = \{\phi_a \in \mathrm{Aut}(G) : \ a \in G\}$, where $\phi_a(x) = axa^{-1}$, and let C be the center of G. Then, $I(G) \cong G/C$.

Proof. We have already proved that $\mathrm{Aut}(G)$ is a group (page 139) and that ϕ_a is an automorphism (page 138). Also, C is a normal subgroup of G. Let's prove that $I(G)$ is a subgroup of $\mathrm{Aut}(G)$. By definition, $I(G) \subseteq \mathrm{Aut}(G)$. Then, if we take $\phi_a, \phi_b \in I(G)$, we have $\phi_a(\phi_b(x)) = \phi_a(bxb^{-1}) = abxb^{-1}a^{-1} = \phi_{ab}(x)$. So, as $\phi_{ab} \in I(G)$, also $\phi_a\phi_b \in I(G)$. We have $a^{-1}axa^{-1}a = x$ and that means that $\phi_{a^{-1}}(\phi_a(x)) = x$ (and $x = exe^{-1}$), i.e. $\phi_{a^{-1}}\phi_a = \phi_e$. From that we have $\phi_{a^{-1}} = [\phi_a]^{-1}$. Therefore, $\phi_{a^{-1}} \in I(G)$ and so $[\phi_a]^{-1} \in I(G)$. Thus, $I(G)$ is a subgroup of $\mathrm{Aut}(()\, G)$.

Let $f : G \to I(G)$ such that $f(a) = \phi_a$, for all $a \in G$. Mapping is thus defined for all $a \in G$. Assume $a = b$. Then, $ax = bx$, for all $x \in G$. As $a = b$, then also $a^{-1} = b^{-1}$. From that we get $axa^{-1} = bxb^{-1}$, i.e. $\phi_a(x) = \phi_b(x)$, for all $x \in G$. That means that $\phi_a = \phi_b$ (as they also have the same domain and the same codomain). From that follows $f(a) = f(b)$. Therefore, f satisfies property of uniqueness. Now, $f(ab) = \phi_{ab}$. But, $\phi_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1} = a\phi_b(x)a^{-1} = \phi_a(\phi_b(x))$, for all $x \in G$. So, $\phi_{ab} = \phi_a\phi_b$ and we have $f(ab) = \phi_{ab} = \phi_a\phi_b = f(a)f(b)$ and f is a homomorphism.

Now, $\ker(f) = \{a \in G : \ f(a) = \phi_e\}$. That means, using $f(a) = \phi_a$ and $\phi_e(x) = x$, for all $x \in G$, that $\ker(f) = \{a \in G : \ (\forall x \in G)(\phi_a(x) = x)\}$. Furthermore, as $\phi_a(x) = axa^{-1}$, we have $\ker(f) = \{a \in G : \ (\forall x \in G)(axa^{-1} = x)\}$. When we multiply the equality $axa^{-1} = x$ by a on the right, we get $ax = xa$. So, $\ker(f) = \{a \in G : (\forall x \in G)(ax = xa)\}$, and that is obviously the definition of the center C of G and we have $\ker(f) = C$. By FHT, we have $G/C \cong I(G)$.

□

Proposition. Let G and H be groups and J and K normal subgroups of G and H, respectively. Then, $(G \times H)/(J \times K) \cong (G/J) \times (H/K)$.

Proof. We have already proved that $G \times H$ and $J \times K$ are groups as G, H, J and K are groups. We want a homomorphism from $(G \times H)$ to $(G/J) \times (H/K)$. We will also want to map from G to G/J and from H to H/K (those quotient groups exist as J and K are normal). We will use a sort of projective homomorphism, i.e. $f : G \times H \to (G/J) \times (H/K)$ defined with $f(x, y) = (Jx, Ky)$. Then, f is defined for all $(x, y) \in G \times H$. Also, $(x, y) = (z, w)$ implies $x = z$ and $y = w$. So, $Jx = Jz$ and $Ky = Kw$. From definition of ordered pair, we have $(Jx, Ky) = (Jz, Kw)$. Therefore f satisfies property of uniqueness. Then, $f((x, y)(z, w)) = f(xz, yw) = (J(xz), K(yw))$. From definition of coset multiplication, $(J(xz), K(yw)) = (Jx \cdot Jz, Ky \cdot Kw)$. By definition of direct product, $(Jx \cdot Jz, Ky \cdot Kw) = (Jx, Ky)(Jy, Kw) = f(x, y)f(y, w)$. Thus, f is a homomorphism.

Now, $\ker(f) = \{(x, y) \in G : \ f(x, y) = (J, K)\}$. As $f(x, y) = (Jx, Ky)$, then $\ker(f) = \{(x, y) \in G : \ (Jx, Ky) = (J, K)\}$. From $(Jx, Ky) = (J, K)$ we get $Jx = J$ and $Ky = K$. From that we gat $x \in J$ and $y \in K$, respectively. Therefore, $\ker(f) = \{(x, y) \in G : \ (x \in J) \wedge (y \in K)\}$. That yields, by definition of Cartesian product, $\ker(f) = J \times K$. Thus, by FHT, we get $(G \times H)/(J \times K) \cong (G/J) \times (H/K)$.

□

Second isomorphism theorem. Let G be a group, H and K subgroups of G. Also, let H be a normal subgroup of G. Then, $K/(H \cap K) \cong HK/H$.

Proof. We have already proved that HK is a subgroup of G. Now, we will prove that H is a normal subgroup of HK. If we take $h \in H$, then $he \in HK$, so $H \subseteq HK$. As H is contained in HK and both are subgroups of G, then H is also a subgroup of HK, by previous proposition. Then, as H is normal, we have that for all $x \in G$ and $h \in H$, $xhx^{-1} \in H$. As it is true for all G and $HK \subseteq G$, then it is true for all $x \in HK$. So, H is a normal subgroup of HK and HK/H is a well-defined quotient group. Then $Hx \in HK/H$, for all $x \in HK$. Let us take $f : K \to HK/H$ with

$f(x) = Hx$, for all $x \in K$. So, if we take $x \in K$, there exists $ex \in HK$ such that $f(x) = H(ex) = Hx$. Also, if $x = y$, then obviously $Hx = Hy$, for all $x, y \in K$. Also, if $x, y \in K$, then $f(xy) = H(xy)$. By definition of coset multiplication $H(xy) = Hx \cdot Hy$, so $f(xy) = f(x)f(y)$. Thus f is a homomorphism from K onto HK/H.

Then, $\ker(f) = \{x \in K : \ f(x) = H\} = \{x \in K : \ Hx = H\}$. But, $Hx = H$ implies $x \in H$, so $\ker(f) = \{x \in K : \ x \in H\}$. That is, by definition equal to $K \cap H$. Therefore, by FHT we have $HK/H \cong K/(H \cap K)$.

□

Theorem (Cayley). Let H be a subgroup of G and $\mathcal{H} = \{xH : \ x \in G\}$. If H contains no normal subgroups of G, except for $\{e\}$, then $G \cong S_{\mathcal{H}}$, where $S_{\mathcal{H}}$ is a group of permutations on $\mathcal{H}$.

Proof. Let $\pi_a : \mathcal{H} \to \mathcal{H}$ be defined with $\pi_a(xH) = (ax)H$, for all $a \in G$. We will show that π_a is a permutation of $\mathcal{H}$. First, it is defined for all $Hx \in \mathcal{H}$, as $ax \in G$, for all $a, x \in G$. Assume $xH = yH$. If we take $axh_1 \in (ax)H$, then $axh_1 = h_2$, for some $h_2 \in H$. That is equivalent to $axh_1 = h_2$. As $xh_1 \in xH$, then there exists $yh_3 \in yH$ such that $xh_1 = yh_3$. So, $ayh_3 = h_2$, i.e. $ayh_3 \in (ay)H$. That is really $axh_1 \in (ay)H$ and from that we have $(ax)H \subseteq (ay)H$. If we take $ayh_1 \in (ay)H$, then there exists $h_2 \in H$ such that $ayh_1 = h_2$. Again, as $xH = yH$ and $yh_1 \in yH$, then there exists $h_3 \in H$ such that $yh_1 = xh_3$. We have $axh_3 = h_2$, i.e. $axh_3 \in (ax)H$ (which is really $ayh_1 \in (ax)H$). That implies $(ay)H \subseteq (ax)H$ and we have $(ax)H = (ay)H$, i.e. from $xH = yH$ we get $\pi_a(xH) = \pi_a(yH)$. Therefore, π_a is a well-defined function. *Injectivity.* Suppose $\pi_a(xH) = \pi_a(yH)$, i.e. $(ax)H = (ay)H$. Then, for all $axh_1 \in (ax)H$, there exists $ayh_2 \in H$ such that $axh_1 = ayh_2$. But, that implies that for all $h_1 \in H$ there exists $h_2 \in H$ such that $xh_1 = yh_2$, i.e. $xH \subseteq yH$. Then, for all $ayh_1 \in H$ there exists $axh_2 \in (ax)H$ such that $ayh_1 = axh_2$. That implies that for all $h_1 \in H$ there exists $h_2 \in H$ such that $yh_1 = xh_2$ and then $yH \subseteq xH$. That is, $xH = yH$. *Surjectivity.* If we take $yH \in \mathcal{H}$, then, as $ya^{-1} \in G$, we can take $(a^{-1}y)H \in \mathcal{H}$ so that $f((a^1y)H) = (a(a^{-1}y))H = yH$. Therefore, π_a is bijective and, as $\mathrm{dom}(\pi_a) = \mathrm{cod}(\pi_a) = \mathcal{H}$, it is a permutation of $\mathcal{H}$.

As we have $S_{\mathcal{H}} = \{\pi_a : \ a \in G\}$, we will consider $f : G \to S_{\mathcal{H}}$, such that $f(a) = \pi_a$, for all $a \in G$. Obviously f is defined for all $a \in G$ in this way. But, if $a = b$ and if we take $axh_1 \in (ax)H$, we have $axh_1 = h_2$, for some $h_2 \in H$. But, as $a = b$, then $bxh_1 = h_2$, so $axh_1 = bxh_1 \in (bx)H$ and $(ax)H \subseteq (bx)H$. Now, if we take $bxh_1 \in (bx)H$, we have $bxh_1 = h_2$, i.e. $axh_1 = h_2$ for some $h_2 \in H$. Then, $axh_1 \in (ax)H$ and $bxh_1 \in (ax)H$. Thus, $(bx)H \subseteq (ax)H$ and $(ax)H = (bx)H$. Therefore, f is well-defined. Then, $f(ab) = \pi_{ab}$. But, $\pi_{ab}(xH) = ((ab)xH) = (a(bx)H) = a\pi_b(xH) = \pi_a(\pi_b(xH))$, for all $xH \in \mathcal{H}$. That means that $\pi_{ab} = \pi_a\pi_b$ and we have $f(ab) = \pi_{ab} = \pi_a\pi_b = f(a)f(b)$ and f is a homomorphism from G onto $S_{\mathcal{H}}$.

Now, $\ker(f) = \{a \in G : \ f(a) = \pi_e\} = \{a \in G : \ (\forall xH \in \mathcal{H})(\pi_a(xH) = xH)\}$. Now, as $\pi_a(xH) = (ax)H$, we have $\ker(f) = \{a \in G : \ (\forall x \in G)(axH = xH)\}$. From $axH = xH$ we conclude that $axx^{-1} \in H$, i.e. $a \in H$. Therefore $\ker(f) = \{a \in H : \ (\forall x \in G)(axH = xH)\}$. From $axH = xH$, we have that for all $h_1 \in H$ there exists $h_2 \in H$ such that $axh_1 = xh_2$. But, that means that $x^{-1}ax = h_2h_1^{-1}$. And, as $h_2h_1^{-1} \in H$, we can say that $\ker(f) = \{a \in H : \ (\forall x \in G)(x^{-1}ax \in H)\}$. By FHT, we have $G/\ker(f) \cong S_{\mathcal{H}}$. But, if only $\ker(f) = \{e\}$, i.e. there are no $a \in H$ such that $(\forall x \in G)(x^{-1}ax \in H)$ (except for $e \in G$), then $G/\{e\} \cong S_{\mathcal{H}}$. But, we have shown that $G/\{e\} = \{\{a\} : \ a \in G\}$. Obviously, $G/\{e\} \cong G$, so, by transitivity of relation of isomorphism, we have $G \cong S_{\mathcal{H}}$.

□

Theorem. Let $\operatorname{cis}(\phi) := \cos\phi + i\sin\phi$. Then $S' = \{\operatorname{cis}(\phi) \in \mathbb{C} : \ \phi \in [0, 2\pi\rangle\}$ is the set of all complex numbers lying on the unit circle. Then, S' with multiplication of complex numbers is a group and $S' \cong \mathbb{R}/\mathbb{Z}$.

Proof. We have already proved that $\mathbb{C}^*$ with multiplication is an Abelian group. Obviously $S' \subset \mathbb{C}^*$ (notice that $0 \notin S'$). Then, if we take $\operatorname{cis}(x), \operatorname{cis}(y) \in S'$, we have, by an already familiar result from elementary algebra, $\operatorname{cis}(x)\operatorname{cis}(y) = \operatorname{cis}(x+y)$ and, as $\operatorname{cis}(x+y) \in S'$, then $\operatorname{cis}(x)\operatorname{cis}(y) \in S'$. If we take $\operatorname{cis}(x) \in S'$, then $\operatorname{cis}(x)\operatorname{cis}(2\pi - x) = \operatorname{cis}(2\pi)$. As $\operatorname{cis}(2\pi) = \cos(2\pi) + i\sin(2\pi) = 1 + i \cdot 0 = 1$, and as $1 \in \mathbb{C}^*$ is a neutral element with respect to multiplication, then $\operatorname{cis}(-x) \in S'$ is an inverse of $\operatorname{cis}(x)$. Thus, S' is a subgroup of $\mathbb{C}^*$ and a group by itself, when it comes to multiplication.

Now, we will consider $f : \mathbb{R} \to S'$ with $f(x) = \operatorname{cis}(kx)$, where $k \in \mathbb{R}$. Then, f is defined for all $x \in \mathbb{R}$. Also, if $x = y$, then obviously $\operatorname{cis}(kx) = \operatorname{cis}(ky)$. Now, $f(x+y) = \operatorname{cis}(k(x+y)) = \operatorname{cis}(kx)\operatorname{cis}(ky) = f(x)f(y)$ and f is a homomorphism. Also, $\ker(f) = \{x \in \mathbb{R} : \ f(x) = 1\} = \{x \in \mathbb{R} : \ \operatorname{cis}(kx) = 1\}$. When is $\operatorname{cis}(kx) = 1$? Obviously, if and only if $\sin kx = 0$ and $\cos kx = 1$. That is true for $kx = 2n\pi$, for all $n \in \mathbb{Z}$. So, $\operatorname{cis}(kx) = 1$ when $x = \frac{2n\pi}{k}$, where $n \in \mathbb{Z}$, and we have $\ker(f) = \{\frac{2n\pi}{k} \in \mathbb{R} : n \in \mathbb{Z}\}$. By choosing $k = 2\pi$, we have $\ker(f) = \{n \in \mathbb{R} : \ n \in \mathbb{Z}\} = \mathbb{Z}$. Then, by FHT, $S' \cong \mathbb{R}/\mathbb{Z}$. Similarly, if we chose $k = 1$, we would get $\ker(f) = \{2n\pi \in \mathbb{R} : \ n \in \mathbb{Z}\}$. But, that is actually $\ker(f) = \langle 2\pi\rangle$, so $S' \cong \mathbb{R}/\langle 2\pi\rangle$, which makes sense as, by a previous theroem, both $\mathbb{Z}$ and $\langle 2\pi\rangle$ are cyclic groups of infinite order so $\mathbb{Z} \cong \langle 2\pi\rangle$.

□

Remark. From now on, we will introduce notation, $H \leq G$ will denote the fact that H is a subgroup of G. Also, let $H \trianglelefteq G$ denote the fact that H is a normal subgroup of G. It is a trivial fact that if $K \trianglelefteq H \trianglelefteq G$ that $K \triangleleft G$ and $H \triangleleft G$. Also we will denote coset multiplication $Kx \cdot Ky$ as $(Kx)(Ky)$.

Third isomorphism theorem. Let G be a group and $K \trianglelefteq H \trianglelefteq G$. Then $H/K \leq G/K$ and

$$(G/K)\,/\,(H/K) \cong G/H.$$

Proof. Let $f : G/K \to G/H$. Groups G/K and G/H are well defined quotient groups as $K \trianglelefteq G$ and $H \trianglelefteq G$. Let $f(Kx) = Hx$, for all $x \in G$. If we take $Kx \in G/K$, then $x \in G$ and there exists $Hx \in G/H$ such that $f(Kx) = Hx$. If $Kx = Ky$, by a previous theorem we have that $xy^{-1} \in K$. But, as $K \trianglelefteq H$, we have $xy^{-1} \in H$. From that we have $Hx = Hy$, i.e. $f(Kx) = f(Ky)$. Now, $f((Kx)(Ky)) = f(K(xy))$, by definition of coset multiplication. Then, $f(K(xy)) = H(xy) = (Hx)(Hy) = f(Kx)f(Hy)$. From that we have that f is a homomorphism from G/K onto G/H.

If we take $Kx \in H/K$, then as $x \in H$, it is also in G (as $H \subseteq G$). So, $Kx \in G/K$ and $H/K \subseteq G/K$. As H/K is itself a group, as is G/K, it follows that $H/K \leq G/K$.

Furthermore, $\ker(f) = \{Kx \in G/K : \ f(Kx) = H\}$, that is $\ker(f) = \{Kx \in G/K : \ Hx = H\}$. As $Hx = H$ if and only if $x \in H$, then $\ker(f) = \{Kx \in G/K : \ x \in H\}$. From that $\ker(f) = K/H$ (due to the fact that $H/K \subseteq G/K$). By FHT, $(G/K)\,/\,(H/K) \cong G/H$.

□

Correspondence theorem. Let $f : G \longrightarrow_K H$ be a homomorphism. Also, let $S \leq H$ and $S^* = \{x \in G : \ f(x) \in S\}$. Then $S^* \leq G$ and $S \cong S^*/K$. In addition, if $S \trianglelefteq H$ then $S^* \trianglelefteq G$.

Proof. First, $S^* \subseteq G$. Then, $x, y \in S^*$ implies $f(x), f(y) \in S$. As $f(x)f(y) = f(xy)$ and $f(xy) \in S$ (it is a subgroup of H), it must be that $xy \in S^*$. Also, as $f(x) \in S$, then, as $S \leq H$, $[f(x)]^{-1} \in S$, i.e. $f(x^{-1}) \in S$. So, $x^{-1} \in S^*$. Therefore, $S^* \leq G$. Let $g : S^* \to S$ be a mapping with $g(x) = f(x)$. Then, for $x \in S^*$ there exists $f(x) \in S$, by definition; so $f(x) = g(x)$ makes g defined for all $x \in S^*$. Then, uniqueness follows from uniqueness of f. Also, g is a homomorphism as f is a homomorphism.

We have $\ker(f) = \{x \in S^* : \ g(x) = e\}$, i.e. $\ker(f) = \{x \in S^* : \ f(x) = e\}$. If we take $x \in K$, then $f(x) = e$ (and $e \in S$ as $S \leq H$) and $x \in G$, meaning $x \in S^*$ and, as $f(x) = e$, also $x \in \ker(f)$. Therefore, $K \subseteq \ker(f)$. Then, if we take $x \in \ker(f)$, then $x \in S^*$ and $f(x) = e$. As $S^* \leq G$ and $f(x) = e$, then $x \in K$. So, $\ker(f) \subseteq K$ and $\ker(f) = K$. We have, by FHT, $S^*/K \cong S$.

We have already proved that $S^* \leq G$ if $S \leq H$. Suppose $S \triangleleft H$. Now, if we take $g \in G$ and $x \in S^*$, then it must be $f(x) \in S \subseteq H$. As also $f(g) \in H$, then it must be that $f(g)f(x)[f(g)]^{-1} \in S$ (due to the fact that $S \trianglelefteq H$). But, $f(g)f(x)[f(g)]^{-1} = f(gxg^{-1})$

(due to f being a homomorphism), so we have $f(gxg^{-1}) \in S$. Then, by definition, $gxg^{-1} \in S^*$ from which follows that $S^* \trianglelefteq G$.

□

Cauchy's theorem. Let G be a group such that $|G| = m$ and $p \in P$ so that $p|m$. Then, there exists $a \in G$ such that $\operatorname{ord}(a) = p$.

Proof. First we will prove that the statement is true for Abelian groups. Let $p \in P$. Let $a \in G$ where $a \neq e$. Such element exists as G cannot be a trivial group ($p > 1$ so $|G| > 1$). The statement holds for $|G| = p$ as then $G \cong \mathbb{Z}_p$, i.e. G is cyclic of order p. Then there must exist $x \in G$ such that $G = \langle x \rangle$. Then $\operatorname{ord}(x) = p$. The statement, specifically holds for $m = 2$.

Now, assume that the following statement is true for all $2 < n < m$: *if G_n is an Abelian group with $|G_n| = n$ and $p|n$ then there exists $a \in G$ such that* $\operatorname{ord}(a) = p$.

We will prove that it is also true for $|G| = m$. Then, $p|m$ and there exists $q \in \mathbb{Z}$ such that $m = qp$. by Lagrange's theorem, it must be that $\operatorname{ord}(a) \,|qp$. We choose $a \neq e$ so that $\operatorname{ord}(a) \neq 1$. If $\operatorname{ord}(a) = p$, then we are done. If $\operatorname{ord}(a) = kp$, where $k|q$, then:

$$\operatorname{ord}\left(a^k\right) = \frac{kp}{\gcd(kp, k)} = \frac{kp}{k} = p.$$

Now, assume $\operatorname{ord}(a) = k$, where $k|q$. As G is Abelian, then $\langle a \rangle \trianglelefteq G$ and we have a well-defined quotient group $G/\langle a \rangle$. Let us denote $\langle a \rangle$ with H. Then,

$$|G/H| = [G : H] = \frac{|G|}{|H|} = \frac{qp}{k} = \frac{q}{k}p.$$

Let us denote $r = \frac{q}{k}$. As $a \neq e$, then $k \neq 1$ and $\frac{q}{k}p < qp$, i.e. $|G/H| < m$. Then, by assumption of induction there exists $Hb \in G/H$ such that $\operatorname{ord}(Hb) = p$. Then, $(Hb)^p = H(b^p) = H$. From that we have $b^p \in H = \langle a \rangle$. That means that for some $l \in \mathbb{N}$, $b^p = a^l$. As $\operatorname{ord}(a) = k$, $b^{pk} = a^{kl}$, i.e. $b^{kp} = e$. From that we have $\left(b^k\right)^p = e$ and, as $\operatorname{ord}\left(b^k\right) |p$, it can only be that either $\operatorname{ord}\left(b^k\right) = 1$ or $\operatorname{ord}\left(b^k\right) = p$. If $\operatorname{ord}\left(b^k\right) = p$, we are done. However, if $\operatorname{ord}\left(b^k\right) = 1$, then $b^k = e$ and we would have $\operatorname{ord}(b) \,|k$. Then, as there exists a projective homomorphism $f : G \to G/H$, with $f(x) = Hx$, from $f(b^k) = f(e)$, (where we have $f(b^k) = H\left(b^k\right) = (Hb)^k$ and $f(e) = H$) it follows that $(Hb)^k = H$. Then, it must be that $\operatorname{ord}(Hb) \,|k$, i.e. $p|k$. Then, $k = k'p$, for some $k' \in \mathbb{Z}$ and $\operatorname{ord}(b) = k'p$ gives us:

$$\operatorname{ord}\left(b^{k'}\right) = \frac{k'p}{\gcd(k'p, k')} = \frac{k'p}{k'} = p.$$

Thus we have proved that there exists an element of order p in an Abelian group G where p divides order of G.

Suppose G is not Abelian. As G is not Abelian C is a proper subgroup of G, i.e. $G - C \neq \emptyset$. Let us observe $C_a = \{x \in G : \ xa = ax\}$. We know that $C_a \leq G$, so $|C_a|$ divides order of $|G| = np$. If $|C_a| = lp$, where $l|n$, then, as C_a is Abelian, it must be that, by first part of the proof, there exists $a \in C_a \subseteq G$ such that $\operatorname{ord}(a) = p$ and we are done. But, assume $|C_a| = l$, for all $a \in G - C$, where $l|n$, i.e. there exists $q \in \mathbb{N}$ such that $n = ql$. Then, $|G| = |C_a|qp$. From that we have $[G : C_a] = \frac{|G|}{|C_a|} = \frac{|C_a|qp}{|C_a|} = qp$. Therefore, p divides $|G/C_a|$. But, by a previous proposition, $|[a]| = [G : C_a]$. Therefore, p divides conjugacy classes of all $a \in G - C$. Let us observe class equation $|C_a|qp = |C| + k_1 + \cdots + k_t$, where k_i is the order of i-th conjugacy class that is not of order 1. As $k_i = ps_i$, for some $s_i \in \mathbb{N}$, we have $|C_a|qp - p(s_1 + \cdots + s_t) = |C|$, i.e. $p(q|C_a| - (s_1 + \cdots + s_t)) = |C|$ and from that p divides order of C. As C is Abelian, then, by first part of the proof, there exists $a \in C$ such that $\operatorname{ord}(a) = p$.

□

Proposition. Let G be a group, $m, n \in \mathbb{N}$, $n < m$ and $|G| = p^m$. Then, there exists $H \trianglelefteq G$ such that[61] $|H| = p^n$.

Proof. If $|G| = p^2$, by previous lemma there exists $a \in G$ such that $\operatorname{ord}(a) = p$ and then $|\langle a \rangle| = p$. Assume that the statement is true for all $1 < k < m$. Let $n \in \mathbb{N}$ and $n < m$. By a previous proposition, as G is a p-group, it has a non-trivial center C of the order p^l, for some $0 < l \leq m$. Then, $|C| = pp^{l-1}$, i.e. p divides $|C|$. Also, as C is Abelian, by Cauchy's theorem, we have that there exists $a \in C$ such that $\operatorname{ord}(a) = p$. Now, let us observe $\langle a \rangle$ (notice that $|\langle a \rangle| = p$). As $a \in C$, then $\langle a \rangle \leq C$. But, as C is Abelian, then $\langle a \rangle \trianglelefteq C$. As $\langle a \rangle$ is a normal subgroup of C, for all $x \in C \subseteq G$ and $y \in \langle a \rangle$, we have $x^{-1}yx \in \langle a \rangle$. It is obvious that $\langle a \rangle \trianglelefteq G$. Let us observe $G/\langle a \rangle$. We have $[G : \langle a \rangle] = \frac{p^m}{p} = p^{m-1}$. By assumption, as $m - 1 < m$ and $n < m$, then $n \leq m - 1$. But, surely then $n - 1 < m - 1$, so there exists $H \trianglelefteq G/\langle a \rangle$ such that $|H| = p^{n-1}$. Also, as $G\langle a \rangle$ is a homomorphic image of G, there exists a projective homomorphism $f : G \to G\langle a \rangle$ with $f(x) = \langle a \rangle x$, for all $x \in G$. Obviously $H = \{f(x) \in H : \ x \in G\} \trianglelefteq \operatorname{ran}(f)$. Let us denote $H' = \{x \in G : \ f(x) \in H\}$. Then, by the correspondence theorem, $H' \trianglelefteq G$ and $H \cong H'/\ker(f)$. But, $\ker(f) = \{x \in G : \ \langle a \rangle x = \langle a \rangle\} = \{x \in G : \ x \in \langle a \rangle\} = \langle a \rangle$, i.e. $H \cong H'/\langle a \rangle$. As $|H| = p^{n-1}$ and $H \cong H'/\langle a \rangle$, then $|H'/\langle a \rangle| = p^{n-1}$. Furthermore, $p^{n-1} = [H' : \langle a \rangle] = \frac{|H'|}{p}$, so $|H'| = p^n$. As also $H' \trianglelefteq G$, G has a normal subgroup of order p^n.

[61] Notice that as $n < m$ then $p^n < p^m$, we have that H is a proper subgroup of G. Also, obviously it has to be $m \geq 2$.

□

Proposition. Let G be a group. For all $a \in G$, $\operatorname{ord}(a) = p^{k(a)}$, where $k(a) \in \mathbb{N}$, if and only if $|G| = p^m$ for some $m \in \mathbb{N}$.

Proof. *Necessity.* Assume for all $a \in G$ we have $\operatorname{ord}(a) = p^{k(a)}$. Then, as $|\langle a \rangle| = p^{k(a)}$, and $\langle a \rangle \leq G$, for all $a \in G$, by Lagrange's theorem, $p^{k(a)}$ divide order of G. Therefore, $|G| = p^k m$, for some $m \in \mathbb{N}$ where $k = \max\{k(a) : \ a \in G\}$. Assume that $p \nmid m$. By fundamental theorem of arithmetic, m can be written as a product of distinct powers of prime numbers $q \in P$ (and they are different from p). Then, as each q divides m, they divide order of G. By Cauchy's theorem there must exist element of order q for each $q \in P$, where $q \neq p$. But, G has only elements of order $p^{k(a)}$, for all $a \in G$. Therefore, $p|m$, and $m = pr$, for some $r \in \mathbb{N}$. Then, as we cannot have infinite regression, $|G| = p^t$, for some $t \in \mathbb{N}$ and $t \geq k$.

Sufficiency. If $|G| = p^m$, suppose there exists some element $a \in G$ such that $\operatorname{ord}(a) = q$ and $q \neq p^l$, for all $l \in \mathbb{N}$. But, as $\langle a \rangle \leq G$, by Lagrange's theorem it must be that $q|p^m$, which is possible only if $q = p^l$, for some $l \in \mathbb{N}$ and $l \leq m$, and that is contrary to our assumption.

□

Remark. Previous proposition actually proves equivalence of two definitions of p-groups. Therefore, either one we choose, we can freely interchange it with another.

Sylow's theorems

Definition. Let G be a group and $H \leq G$. Let $p \in P$. If H is a p-group we say that H is a p-**subgroup** of G.

Definition. Let G be a group, $p \in P$ and $H \leq G$ a p-subgroup of G. We say that H is a p-**Sylow subgroup** of G if there does not exist p-subgroup $K \leq G$ such that $H \leq K$.

Definition. Let G be a group acting on set S. Then,

$$\mathrm{Fix}_G(S) = \{s \in S : \ (\forall g \in G)(g.s = s)\}.$$

Remark. Notice that the difference from stabilizer of some element $s \in S$, that is $\mathrm{Stab}_G(s)$ is that a point s is in $\mathrm{Fix}_G(S)$ if all elements of group G hold it fixed (it cannot be moved to another point by any element of the group). Stabilizer of s is, on the other hand, set of elements of G which fix s. We will clarify that with the following proposition.

Proposition. Let G be a group acting on set S. Then the following statements are equivalent:

1. $s \in \mathrm{Fix}_G(S)$;
2. $|\mathrm{Orb}_G(s)| = 1$;
3. $\mathrm{Orb}_G(s) = \{s\}$;
4. $|\mathrm{Stab}_G(s)| = |G|$;
5. $\mathrm{Stab}_G(s) = G$.

Proof. 1 *implies* 2. If $s \in \mathrm{Fix}_G(S)$, then $g.s = s$, for all $g \in G$. We know that $s \in \mathrm{Orb}_G(s)$ as $e.s = s$, so it must be $|\mathrm{Orb}_G(s)| \geq 1$. Assume that $|\mathrm{Orb}_G(s)| > 1$. Then there exists $t \in \mathrm{Orb}_G(s)$, $t \neq s$, such that $h.s = t$, for some $h \in G$. But, as $s \in \mathrm{Fix}_G(S)$, then $h.s = s$ and we get $s = t$, which is contrary to our assumption that $s \neq t$ and that $|\mathrm{Orb}_G(s)| > 1$. It must be that $|\mathrm{Orb}_G(s)| \leq 1$ and, combined with $|\mathrm{Orb}_G(s)| \geq 1$ we have $|\mathrm{Orb}_G(s)| = 1$.

2 *implies* 3. We have $|\mathrm{Orb}_G(s)| = 1$ and $s \in \mathrm{Orb}_G(s)$, as $e.s = s$. Therefore, $\mathrm{Orb}_G(s) = \{s\}$.

3 *implies* 4. From orbit stabilizer theorem, $|G| = |\mathrm{Orb}_G(s)| \cdot |\mathrm{Stab}_G(s)|$. As $\mathrm{Orb}_G(s) = \{s\}$, then $|\mathrm{Orb}_G(s)| = 1$. From that it follows $|G| = 1 \cdot |\mathrm{Stab}_G(s)| = |\mathrm{Stab}_G(s)|$.

4 *implies* 5. We have $|\mathrm{Stab}_G(s)| = |G|$. If we take $g \in \mathrm{Stab}_G(s)$, then $g \in G$ such that $g.s = s$. As $g \in \mathrm{Stab}_G(s)$ implies $g \in G$, then $\mathrm{Stab}_G(s) \subseteq G$. That, and $|\mathrm{Stab}_G(s)| = |G|$ implies $\mathrm{Stab}_G(s) = G$.

5 *implies* 1. As $\mathrm{Stab}_G(s) = G$, then for all $g \in G$ there exists $h \in \mathrm{Stab}_G(s)$ such that $g = h$. But, as $h \in \mathrm{Stab}_G(s)$ implies $h.s = s$, and as $g = h$, it also implies that $g.s = s$. Therefore, for all $g \in G$, we have $g.s = s$ and from that, by definition, $s \in \mathrm{Fix}_G(S)$.

□

Theorem (Fixed point congruence). Let S be a set and G a group acting on S such that $|G| = p^m$, for some $m \in \mathbb{N}$ and $p \in P$. Then,

$$|S| \equiv |\mathrm{Fix}_G(S)| \pmod{p}.$$

Proof. Let for all $s, t \in S$, $s \sim t$ if and only if $|\mathrm{Orb}_G(s)| = |\mathrm{Orb}_G(t)|$. It is easy to see that $\sim$ is an equivalence relation. From orbit-stabilizer theorem we know that $|G| = |\mathrm{Orb}_G(s)| \cdot |\mathrm{Stab}_G(s)|$, that is $|\mathrm{Orb}_G(s)|$ divides $|G| = p^m$. Our choices for sizes of orbits are in $C = \{1, p, p^2, \ldots, p^m\}$. Therefore, there are $m + 1$ equivalence classes, disjoint and their union being all of S. Now, we know that $s \in \mathrm{Fix}_G(S)$ if and only if $|\mathrm{Orb}_G(s) = 1|$, from the previous proposition. So, there will be $|\mathrm{Fix}_G(S)|$ elements in the equivalence class where $|\mathrm{Orb}_G(s)| = 1$. For $|\mathrm{Orb}_G(s)| = p^i$, $i \in \mathbb{N}$, we can assume there are $c(i)$ different orbits ($c : \mathbb{N} \to \mathbb{N} \cup \{0\}$). Therefore,

$$|S| = |\mathrm{Fix}_G(S)| \cdot 1 + \sum_{i=1}^{m} c(i)p^i.$$

As $i > 1$, then $p^i = p \cdot p^{i-1}$ and we can write:

$$|S| = |\mathrm{Fix}_G(S)| + \sum_{i=1}^{m} c(i)p \cdot p^{i-1} = |\mathrm{Fix}_G(S)| + p\sum_{i=1}^{m} c(i) \cdot p^{i-1}.$$

Let us denote $\sum_{i=1}^{m} c(i) \cdot p^{i-1} = \Sigma$ for simplicity. Then, $|S| = |\mathrm{Fix}_G(S)| + p\Sigma$. That is equivalent to $|S| - |\mathrm{Fix}_G(S)| = p\Sigma$. From that we have that p divides $|S| - |\mathrm{Fix}_G(S)|$ and by definition of congruence that is equivalent to $|S| \equiv |\mathrm{Fix}_G(S)| \pmod{p}$.

□

Lemma. Let G be a group, $H \leq G$ and $a \in G$. Let H act on G/H with $h.Ha = H(ah)$. Then, $h.Ha = Ha$, for all $h \in H$, if and only if $Ha \in \mathrm{N}_G(H)/H$.

Proof. We can see that H and G/H satisfy axioms for group actions. We have $h_1.(h_2.Ha) = h_1.H(ah_2) = H(ah_2h_1) = (h_2h_1).Ha$, for all $h_1, h_2 \in H$ and $Ha \in G/H$. Also, $e.Ha = H(ae) = Ha$, for all $Ha \in G/H$. *Necessity.* Let $a \in G$. Then $Ha \in G/H$. We can see that $h.Ha = Ha$ is equivalent to $H(ah) = Ha$, for all $h \in H$. That is equivalent to $aha^{-1} \in H$, for all $h \in H$. That implies $a \in \mathrm{N}_G(H)$. As $a \in \mathrm{N}_G(H)$, then $Ha \in \mathrm{N}_G(H)/H$. *Sufficiency.* If we take $Ha \in \mathrm{N}_G(H)/H$, then $a \in \mathrm{N}_G(H)$. That implies that $aha^{-1} \in H$, for all $h \in H$. That is equivalent to $(ah)a^{-1} \in H$ which implies $H(ah) = Ha$, for all $h \in H$. Then, as $h.Ha = H(ah)$, we have $h.Ha = Ha$, for all $h \in H$.

□

Proposition. Let G be a group, $H \leq G$ with $|H| = p^m$, for some $m \in \mathbb{N}$ and $p \in P$. Then,

$$[G : H] \equiv [\mathrm{N}_G(H) : H] \pmod{p}.$$

Proof. Let H act on the set of all right cosets of H (G/H, but not necessarily a quotient group) with $h.Ha = H(ah)$, for all $h \in H$ and $Ha \in G/H$. By fixed point definition, we have:

$$\mathrm{Fix}_H(G/H) = \{Ha \in G/H : \ (\forall h \in H)(h.Ha = Ha)\}.$$

That implies that $h.Ha = Ha$ for all $h \in H$ if and only if $Ha \in \mathrm{Fix}_H(G/H)$. By previous lemma that is equivalent to $Ha \in \mathrm{N}_G(H)/H$ if and only if $Ha \in \mathrm{Fix}_H(G/H)$, giving us $\mathrm{N}_G(H)/H = \mathrm{Fix}_H(G/H)$. By fixed point congruence theorem,

$$|G/H| \equiv |\mathrm{Fix}_H(G/H)| \pmod{p}.$$

Combining that with previous result gives us:

$$|G/H| \equiv |\mathrm{N}_G(H)/H| \pmod{p}.$$

□

Theorem (Sylow I). Let G be a group with $|G| = p^m n$, where $\gcd(p, n) = 1$, $m \in \mathbb{N}_0$, $n \in \mathbb{N}$ and $p \in P$. Then, there exists a p-Sylow subgroup of G with order p^m.

Proof. We will show that there exists a subgroup of order k for all $k \in \{0, \ldots, m\}$. We have a trivial p-subgroup $H_0 = \{e\} \leq G$ (obviously $|H_0| = 1 = p^0$). By Cauchy's theorem, as p divides order of G, there exists $a \in G$ such that $\operatorname{ord}(a) = p$. Then, $H_1 = |\langle a \rangle| = p = p^1$. Now, assume that there exists $H_i \leq G$ such that $|H_i| = p^i$, for some $i \in \{2, \ldots, m-1\}$. By previous proposition, as $H_i \leq G$ and $|H_i| = p$, we have $[G : H_i] \equiv [\mathrm{N}_G(H_i) : H_i] \pmod{p}$. As $[G : H_i] = \frac{|G|}{|H_i|} = \frac{np^m}{p^i} = np^{m-i}$, then $np^{m-i} \equiv [\mathrm{N}_G(H_i) : H_i] \pmod{p}$. That means $np^{m-i} - pq = [\mathrm{N}_G(H_i) : H_i]$ for some $q \in \mathbb{N}$. Then, as $i < m$ we have $0 < m - i$ and it must be that $p^{m-i-1} \in \mathbb{N}$. So, $p(np^{m-i-1} - q) = [\mathrm{N}_G(H_i) : H_i]$. Therefore, p divides $[\mathrm{N}_G(H_i) : H_i]$ and we have $[\mathrm{N}_G(H_i) : H_i] = pr$, for some $r \in \mathbb{N}$. As p divides order of $\mathrm{N}_G(H_i)/H_i$ (which is a group because $H_i \trianglelefteq \mathrm{N}_G(H_i)$), then by Cauchy's theorem there exists $Ha \in \mathrm{N}_G(H_i)/H_i$ such that $\operatorname{ord}(Ha) = p$. Then, $\langle Ha \rangle \leq \mathrm{N}_G(H_i)/H_i$ and $|\langle Ha \rangle| = p$. Let $f : \mathrm{N}_G(H_i) \to_{H_i} \mathrm{N}_G(H_i)/H_i$ be a projective homomorphism, i.e. $f(x) = H_i x$, for all $x \in \mathrm{N}_G(H_i)$. Then, by correspondence theorem, $f^{-1}(\langle Ha \rangle)\, \mathrm{N}_G(H_i)$ and $f^{-1}(\langle H_i a \rangle)/H_i \cong \langle H_i a \rangle$. The latter implies $|f^{-1}(\langle H_i a \rangle)/H_i| = |\langle H_i a \rangle| = p$. In other words, $[f^{-1}(\langle H_i a \rangle) : H_i] = p$. Then,

$$p = \left[f^{-1}(\langle H_i a \rangle) : H_i\right] = \frac{|f^{-1}(\langle H_i a \rangle)|}{|H_i|} = \frac{|f^{-1}(\langle H_i a \rangle)|}{p^i}.$$

If we multiply the equation above with p^i, we get

$$\left|f^{-1}(\langle H_i a \rangle)\right| = p^{i+1}.$$

As $H_{i+1} = f^{-1}(\langle Ha \rangle) \leq \mathrm{N}_G(H_i) \leq G$, we have shown that existence of a p-subgroup of order p^i implies the existence of a p-subgroup of G of order p^{i+1}. The correspondence theorem also implies that $H_i \trianglelefteq f^{-1}(\langle H_i a \rangle)$ (as $\ker(f) = H_i$). The process obviously stops at H_m with $|H_m| = p^m$. We can assume that there exists $H_s \leq G$ such that $H_m \leq H_s \leq G$ and $|H_s| = p^s$, where $s \in \mathbb{N}$ and $s \geq m$. But, $|H_s|$ divides $|G|$ and we have $|G| = p^s t$, for some $t \in \mathbb{N}$. That implies $p^m n = p^s t$. Then, as $m \leq s$ we have $n = p^{s-m}t$. If $s - m \neq 0$ we get that $p|n$ which brings us into contradiction with assumption that $p \nmid n$. Therefore it must be that $s - m = 0$, i.e. $s = m$. From that we have $|H_s| = |H_m|$. As also $H_m \leq H_s$ then $H_s = H_m$. That actually means that H_m is a p-Sylow subgroup of G.

□

Proposition. If G is a group with $|G| = p^m n$, for some $p \in P$, $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$, and H is a p-Sylow subgroup of G, then $|H| = p^m$.

Proof. If $m = 0$, then the only p-Sylow subgroup is $\{e\}$, so $|H| = |\{e\}| = 1$. If $m = 1$, then by Cauchy's theorem there exists $a \in G$ such that $\operatorname{ord}(a) = p$. We have that $\langle a \rangle$ is a p-subgroup of G. If it were that H was a p-Sylow subgroup of order 1, we would have $H = \{e\}$. But, as $\{e\} \leq \langle a \rangle$, H would be contained in $\langle a \rangle$ and could not be a p-Sylow subgroup of G. Therefore, $|H| = p$. Assume $m > 1$. and $|H| < p^m$, i.e. $|H| = p^k$, where $k < m$. Then, as H is a p-Sylow (and a) p-subgroup of G, by a previous lemma, we have:

$$[G : H] \equiv [\mathrm{N}_G(H) : H] \pmod{p}.$$

That implies, as $\frac{|G|}{|H|} = \frac{p^m}{p^k} = p^{m-k} = p^l$, where $l \in \mathbb{N}$ (due to $m > k$), $|\mathrm{N}_G(H)/H| - p^l = pq$, for some $q \in \mathbb{Z}$. That is, $|\mathrm{N}_G(H)/H| = p(q + p^{l-1})$. By Cauchy's theorem, there exists $Ha \in \mathrm{N}_G(H)/H$ such that $\operatorname{ord}(a) = p$. Then, by correspondence theorem, $\langle Ha \rangle \cong f^{-1}(\langle Ha \rangle)/H$, where f is a projective homomorphism $f : \mathrm{N}_G(H) \to_H \mathrm{N}_G(H)/H$ with $f(x) = Hx$. So, $|f^{-1}(\langle Ha \rangle)/H| = p$, which gives us that $\frac{|f^{-1}(\langle Ha \rangle)|}{|H|} = p$. That is, $|f^{-1}(\langle Ha \rangle)| = p^{l+1}$. As $H \trianglelefteq f^{-1}(\langle Ha \rangle)$, and $p^l < p^{l+1}$, H cannot be a p-Sylow subgroup of G with order less than p^m. So, $|H| = p^m$.

□

Remark. Previous proposition actually tells us that all p-Sylow subgroups are of the same size and that $[G : H] = m$, where $p \nmid m$. Also, it is obvious that, if $|G| = p^m n$, $\gcd(p, n) = 1$, it cannot be that $|H| = p^{m'}$, where $m' > m$. That would imply that, due to Lagrange's theorem, $p^{m'} | p^m n$, i.e. that there exists $q \in \mathbb{Z}$ such that $p^m n = p^{m'} q$. That is equivalent to $p^{m'-m} q = n$, i.e. $p(p^{m'-m-1} q) = n$. And, as $m' > m$, and we would have $p | n$.

Lemma. Let G be a group, $a \in G$ and $H, K \leq G$. If $aHa^{-1} \subseteq K$, then $H \subseteq a^{-1}Ka$.

Proof. Let $h \in H$. Then there exists $k \in K$ such that $aha^{-1} = k$. But, that is equivalent to $h = a^{-1}ka$. Thus, for all $h \in H$ there exists $k \in K$ such that $h = a^{-1}ka$. So, $h \in a^{-1}Ka$ and $H \subseteq a^{-1}Ka$.

□

Theorem (Sylow II). If H and K are p-Sylow subgroups of G, then:

1. For all $a \in G$, aHa^{-1} is a p-Sylow subgroup of G.
2. There exists $a \in G$ such that $H = aKa^{-1}$.

Proof. *Ad* 1. By a previous proposition, we know that $aHa^{-1} \cong H$ and $aHa^{-1} \leq G$. From that follows $|aHa^{-1}| = |H|$. As order of H is a power of p, then order of aHa^{-1} is a power of p. Thus, aHa^{-1} is a p-subgroup of G. Assume $aHa^{-1} \leq K$ where $K \leq G$ is a p-subgroup of G. Then, as $aHa^{-1} \subseteq K$, previous lemma implies $H \subseteq a^{-1}Ka$. But, $a^{-1}Ka \cong K$, so it is also a p-subgroup of G. Also, $a^{-1}Ka \leq G$ and that implies $H \leq a^{-1}Ka$. As H is a p-Sylow subgroup of G it cannot be contained in any p-subgroup of G and it must be $H = a^{-1}Ka$. That is equivalent to $aHa^{-1} = K$. As $aHa^{-1} \leq K$ implied $aHa^{-1} = K$ and both are p-subgroups of G, then aHa^{-1} is a p-Sylow subgroup of G.

Ad 2. Let H and K be p-Sylow subgroups of G. Then, let H act on G/K with $h.Ka = K(ah)$, for all $Ka \in G/K$ and $h \in H$. Obviously, $K(ah) = Ka$ if and only if $aha^{-1} \in K$, for all $h \in H$. That is equivalent to $aHa^{-1} \subseteq K$. But, as conjugate of a p-Sylow subgroup is a p-Sylow subgroup, it follows that $aHa^{-1} = K$. Also, if $aHa^{-1} = K$ it is obvious that $aHa^{-1} \subseteq K$. Therefore, $Ka \in \mathrm{Fix}_{G/K}(H)$ if and only if $aHa^{-1} = K$. But, by FPC theorem we have:

$$|G/K| \equiv \left|\mathrm{Fix}_{G/K}(H)\right| \pmod{p}.$$

Assume $\left|\mathrm{Fix}_{G/K}(H)\right| = 0$, i.e. $\mathrm{Fix}_{G/K}(H) = \emptyset$. Then, we would have $[G : K] \equiv 0 \pmod{p}$, meaning $[G : K] = pq$, for some $q \in \mathbb{Z}$. But, due to previous corollary, $[G : K] = m$, where $p \nmid m$. Therefore, $\mathrm{Fix}_{G/K}(H) \neq \emptyset$, i.e. there exists $Ka \in \mathrm{Fix}_{G/K}(H)$ such that $K = aHa^{-1}$.

□

Remark. From previous theorem, it also follows that all p-Sylow subgroups are conjugate.

Definition. Let G be a group and $p \in P$. Then we define $\mathrm{Syl}_p(G)$ as a set containing all p-Sylow subgroups of G.

Lemma. Let G be a group and H a p-Sylow subgroup of G, for some $p \in P$. Let $a \in G$ such that $\mathrm{ord}(a) = p^m$, for some $m \in \mathbb{N}_0$. Then, $aHa^{-1} = H$ implies $a \in H$.

Proof. First, as $aHa^{-1} = H$, it must be that $a \in \mathrm{N}_G(H)$, by definition of subgroup normalizer. Let $f : \mathrm{N}_G(H) \to_H \mathrm{N}_G(H)/H$ be a projective homomorphism. Then, $f(x) = Hx$, for all $x \in \mathrm{N}_G(H)$. Then, as $a \in \mathrm{N}_G(H)$, then $Ha \in \mathrm{N}_G(H)/H$. As $\mathrm{ord}(a) = p^m$, then $\langle Ha \rangle \leq \mathrm{N}_G(H)$ with $|\langle Ha \rangle| = p^m$. By correspondence theroem, it follows that

$$\ker(f) = H \trianglelefteq f^{-1}(\langle Ha\rangle) \leq \mathrm{N}_G(H),$$

with $f^{-1}(\langle Ha\rangle)/H \cong \langle Ha\rangle$. That implies $|f^{-1}(\langle Ha\rangle)/H| = |\langle Ha\rangle| = p^m$. As H is a p-subgroup, $|H| = p^k$, for some $k \in \mathbb{N}$. We have:

$$p^m = \left[f^{-1}(\langle Ha\rangle) : H\right] = \frac{|f^{-1}(\langle Ha\rangle)|}{|H|} = \frac{|f^{-1}(\langle Ha\rangle)|}{p^k}.$$

That implies $|f^{-1}(\langle Ha\rangle)| = p^{m+k}$, i.e. $f^{-1}(\langle Ha\rangle)$ is a p-subgroup of $\mathrm{N}_G(H)$ and by that also of G. As $\ker(f) = H \leq f^{-1}(\langle Ha\rangle)$, we have that H is contained in p-subgroup $f^{-1}(\langle Ha\rangle)$. But, as H is a p-Sylow subgroup of G, it must be that $f^{-1}(\langle Ha\rangle) = H$. That would imply

$$\left[f^{-1}(\langle Ha\rangle) : H\right] = 1 = |\langle Ha\rangle|.$$

From that we have $\mathrm{ord}(Ha) = 1$, and that implies $Ha = H$, i.e. $a \in H$.

□

Lemma. Let G be a group and $H \in \mathrm{Syl}_p(G)$. Then, $K \in \mathrm{Syl}_p(G)$ if and only if there exists $a \in G$ such that $aHa^{-1} = K$.

Proof. *Necessity.* Let $K \in \mathrm{Syl}_p(G)$. Then, by second Sylow's theorem, there exists $a \in G$ such that $aKa^{-1} = H$. *Sufficiency.* By second Sylow's theorem, $a^{-1}Ha$ is a p-Sylow subgroup of G, and that means that so is K, i.e. $K \in \mathrm{Syl}_p(G)$.

□

Theorem (Sylow III). Let G be a group with $|G| = p^m n$, where $p \in P$, $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$ such that $\gcd(p, n) = 1$. Then,

1. $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod{p}$.
2. If $H \in \mathrm{Syl}_p(G)$, then $\left|\mathrm{Syl}_p(G)\right| = [G : \mathrm{N}_G(H)]$.
3. $\left|\mathrm{Syl}_p(G)\right|$ divides $|G|$. Specifically, $\left|\mathrm{Syl}_p(G)\right|$ divides n.

Proof. *Ad* 1. By first Sylow theorem, as p divides $|G|$, we know that $\mathrm{Syl}_p(G) \neq \emptyset$. Take $H \in \mathrm{Syl}_p(G)$ and let H act on $\mathrm{Syl}_p(G)$ with $h.K = hKh^{-1}$, for all $h \in H$ and $K \in \mathrm{Syl}_p(G)$. Let us observe $\mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)$. As $h.H = hHh^{-1} = H$, for all $h \in H$, then $H \in \mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)$. That means that $\left|\mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)\right| \geq 1$. Assume

$\left|\mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)\right| > 1$. Then, there exists $K \in \mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)$ such that $H \neq K$. But, that also means that $h.K = K$, for all $h \in H$, i.e. $hKh^{-1} = K$ for all $h \in H$. As H is a p-group, all elements in it have order a power of p, i.e. $\mathrm{ord}(h) = p^{\alpha(h)}$, for all $h \in H$, where $\alpha : H \to \mathbb{N}_0$. Then, by previous lemma, $hKh^{-1} = K$ implies $h \in K$, for all $h \in H$. So, $H \subseteq K$, and as H is a group, $H \leq K$. As H is a p-Sylow subgroup of G, it cannot be that $H \leq K$ with $H \neq K$, and it must be $H = K$. That is in contradiction with assumption that $\left|\mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)\right| > 1$. So it is $\left|\mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)\right| \leq 1$. That, and $\left|\mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)\right| \geq 1$ imply $\left|\mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)\right| = 1$. Then, by FPC, we have $\left|\mathrm{Syl}_p(G)\right| \equiv \left|\mathrm{Fix}_H\left(\mathrm{Syl}_p(G)\right)\right| \pmod{p}$, i.e. $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod{p}$.

Ad 2. Let G act on $\mathrm{Syl}_p(G)$ so that $g.H = gHg^{-1}$, for all $g \in G$ and $H \in \mathrm{Syl}_p(G)$. Then, by Sylow II, we have that $gHg^{-1} \in \mathrm{Syl}_p(G)$. Also, $g.(h.H) = g.(hHh^{-1}) = ghHh^{-1}g^{-1} = (gh)H(gh)^{-1} = (gh).H$ and $e.H = eHe^{-1} = H$. Let $H \in \mathrm{Syl}_p(G)$ and let us observe:

$$\mathrm{Stab}_G(H) = \{g \in G : \ g.H = H\} = \{g \in G : \ gHg^{-1} = H\} = \mathrm{N}_G(H).$$

Now, the orbit of H in G is:

$$\begin{aligned} \mathrm{Orb}_G(H) &= \{K \in \mathrm{Syl}_p(G) : \ (\exists g \in G)(g.H = K)\} \\ &= \{K \in \mathrm{Syl}_p(G) : \ (\exists g \in G)(gHg^{-1} = K)\}. \end{aligned}$$

Notice that $K \in \mathrm{Orb}_G(H)$ if and only if there exists $g \in G$ such that $gHg^{-1} = K$. But, by previous lemma, $K \in \mathrm{Syl}_p(G)$ if and only if there exists $g \in G$ such that $gHg^{-1} = K$. That actually means that $K \in \mathrm{Orb}_G(H)$ if and only if $K \in \mathrm{Syl}_p(G)$. In other words, $\mathrm{Orb}_G(H) = \mathrm{Syl}_p(G)$. Therefore, by orbit-stabilizer theorem,

$$|G| = |\mathrm{Orb}_G(H)| \cdot |\mathrm{Stab}_G(H)| = \left|\mathrm{Syl}_p(G)\right| \cdot |\mathrm{N}_G(H)|.$$

If we divide the equality above with $|\mathrm{N}_G(H)|$, we get:

$$\left|\mathrm{Syl}_p(G)\right| = \frac{|G|}{\mathrm{N}_G(H)} = [G : \mathrm{N}_G(H)].$$

That concludes proof for 2.

Ad 3. From 2, we have that $|G| = \left|\mathrm{Syl}_p(G)\right| \cdot |\mathrm{N}_G(H)|$. Then, $\left|\mathrm{Syl}_p(G)\right|$ divides $|G| = p^m n$. But, as due to 1, we have $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod{p}$, i.e. $\left|\mathrm{Syl}_p(G)\right| = pq + 1$, for some $q \in \mathbb{Z}$. Assume p divides $\left|\mathrm{Syl}_p(G)\right|$, i.e. $p|pq+1$. Then, $pq + 1 = pr$, for some $r \in \mathbb{Z}$. We have $pq - pr = 1$, i.e. $p(q - r) = 1$ which would imply $p = 1$, but that is a

contradiction as $p \neq 1$. Therefore, $\gcd\left(\left|\mathrm{Syl}_p\left(G\right)\right|, p\right) = 1$. Then, $p^m n = \left|\mathrm{Syl}_p\left(G\right)\right| s$, where $s = \left|\mathrm{N}_G\left(H\right)\right|$. As $p \nmid \left|\mathrm{Syl}_p\left(G\right)\right|$, then $p^m \nmid \left|\mathrm{Syl}_p\left(G\right)\right|$, so by Euclid's lemma[62], $p^m | s$. We have $n = \left|\mathrm{Syl}_p\left(G\right)\right| \frac{s}{p^m}$, where $\frac{s}{p^m} \in \mathbb{Z}$ as $p^m | s$. That implies that $\left|\mathrm{Syl}_p\left(G\right)\right|$ divides n.

□

[62] Another way to prove this is by Lagrange's theorem: as $H \trianglelefteq \mathrm{N}_G\left(H\right)$, then $|H|$ divides $\mathrm{N}_G\left(H\right)$ and we have that $\mathrm{N}_G\left(H\right) = |H| t = p^m t$, for some $t \in \mathbb{Z}$.

Dihedral groups

Definition. Let $n \in \mathbb{N} - \{1, 2\}$ and $R \in \mathbb{R}^+$. Let V_n be the set of vertices of a regular polygon in Euclidean plane centered at origin, that is:

$$V_n = \left\{ \left(R\cos\frac{2k\pi}{n}, R\sin\frac{2k\pi}{n} \right) \in \mathbb{R}^2 : \ k \in \{0, \ldots, n-1\} \right\}.$$

Set of all rotations and reflections which leave A unchanged (i.e. for all $v \in V$, $r(v) \in V_n$ and $s(v) \in V_n$, for all rotations r and reflections s) along with composition as respective operation is called a **dihedral group** D_{2n}.

Proposition. For all $n \in \mathbb{N} - \{1, 2\}$, $|D_{2n}| = 2n$.

Proof. Here we can use the orbit-stabilizer theorem to show that $|D_{2n}| = 2n$. Choose any vertex, e.g. $v_1 \in V_n$, without loss of generality. Then, that vertex can be moved to all other vertices $v_2, \ldots, v_n$ (by rotations and reflections), including to itself (by identity). Therefore, $\mathrm{Orb}_{D_{2n}}(v_1) = \{v_1, \ldots, v_n\}$ which implies $|\mathrm{Orb}_{D_{2n}}(v_1)| = n$. All rotations, except identity, move all vertices, therefore, they cannot be in the stabilizer of v_1. Reflection s through vertex v_1, however, will leave v_1 unchanged (and so will identity). Thus, $\mathrm{Stab}_{=}(v_1)\{e, s\}$ from which we have $|\mathrm{Stab}_{D_{2n}}(v_1)| = 2$. Note that reflection through v_1 will be the bisector of the angle at v_1 and will pass through opposite vertex if n is even. If n is odd, it will bisect the opposite side. To conclude, by orbit-stabilizer theorem, $|D_{2n}| = |\mathrm{Stab}_{D_{2n}}(v_1)| \cdot |\mathrm{Orb}_{D_{2n}}(v_1)| = 2n$.

□

Remark. Note that we could have proven (at least argued) for the previous theorem by counting permutations (with certain properties). For example, if we fix $v(i)$, where $i \in \{0, \ldots, n-1\}$, then it can be sent to n different vertices (including itself). Say we chose $v(i) \to v(k)$. But, that leaves open the possibility of his neighbour, $v(i+1)$ to be sent to all other n vertices with us still having $n!$ bijections. Therefore, we will want to preserve the structure of the polygon, so that only rotation and reflection are considered. In both, if $v(i) \to v(k)$, then $v(i+1) \to v(k+1)$ (then it must be $v(i-1) \to v(k-1)$) or $v(i+1) \to v(k-1)$ (when it must be $v(i-1) \to v(k+1)$), where $i+1$, $i-1$, $k+1$, $k-1$ is taken modulo n. In other words, all adjacent vertices must remain adjacent after rotation and reflection. Thus, we have only two options left (either send $v(i+1)$ to $v(k+1)$ or to $v(k-1)$) and with n possibilities to choose for $v(i)$, that is $2 \cdot n$ permutations with desired properties.

Remark. Let $v(k) \in V_n$, for $k \in \{0, \ldots, n-1\}$, where $v(k) = \left(R\cos\frac{2k\pi}{n}, R\sin\frac{2k\pi}{n}\right)$.

We will now define rotation $r \in D_{2n}$ (for $\frac{2\pi}{n}$) as $r : V_n \to V_n$ such that $r\,(v(k)) = v(k+1)$. We will also define reflection $s \in D_{2n}$ (across x-axis) as $s : V_n \to V_n$ with $s\,(v(k)) = v(-k)$. Also, identity is $e : V_n \to V_n$ with $e\,(v(k)) = v(k)$. Note that $D_{2n} \leq S_{V_n}$, where S_{V_n} is the set of all permutations of V_n. Thus, all group axioms for D_{2n} are satisfied (except commutativity).

Remark. From now on, when considering D_{2n}, we will assume $n \in \mathbb{N} - \{1, 2\}$.

Proposition. Let $v(k) \in V_n$ be defined as above and $r \in D_{2n}$. Then[63], for all $m \in \mathbb{N}$, $r^m\,(v(k)) = v(k+m)$ and $r^n = e$. Also, $\text{ord}\,(r) = n$.

Proof. By definition, $r(v(k)) = v(k+1)$. Assume $r^m(v(k)) = v(k+m)$. Then,

$$r^{m+1}(v(k)) = [r^m \circ r](v(k)) = r^m(r(v(k))) = r^m(v(k+1)) = v(k+m+1).$$

Finally,

$$\begin{aligned} r^n(v(k)) &= v(k+n) = \left(R\cos\frac{2(k+n)\pi}{n}, R\sin\frac{2(k+n)\pi}{n}\right) \\ &= \left(R\cos\left(2\pi + \frac{2k\pi}{n}\right), R\sin\left(2\pi + \frac{2k\pi}{n}\right)\right) \\ &= \left(R\cos\frac{2k\pi}{n}, R\sin\frac{2k\pi}{n}\right) = v(k). \end{aligned}$$

That implies $r^n(v(k)) = v(k)$, that is $r^n = e$. Now, assume that $r^m = e$, where $0 < m < n$. That implies $r^m(v(k)) = v(k)$, that is:

$$r^m(v(k)) = \left(R\cos\frac{2(k+m)\pi}{n}, R\sin\frac{2(k+m)\pi}{n}\right) = \left(R\cos\frac{2k\pi}{n}, R\sin\frac{2k\pi}{n}\right).$$

By definition of ordered pair, and after cancelling out R, we have $\cos\frac{2(k+m)\pi}{n} = \cos\frac{2k\pi}{n}$. That implies $\frac{2(k+m)\pi}{n} = \frac{2k\pi}{n} + 2l\pi$, for all $l \in \mathbb{Z}$. That gives us $\frac{2m\pi}{n} = 2l\pi$, i.e. $\frac{m}{n} = l$. But, as $0 < m < n$, then $n \nmid m$ and $\frac{m}{n} \notin \mathbb{Z}$ while $l \in \mathbb{Z}$. This is a contradiction, therefore, there does not exist m such that $r^m = e$ and $0 < m < n$. The other possibility is that $\frac{2(k+m)\pi}{n} = -\frac{2k\pi}{n} + 2l\pi$. Then, $\frac{4k+2m\pi}{n} = 2l\pi$. After cancelling out equal terms, $\frac{2k}{n} + \frac{m}{n} = l$, i.e. $\frac{2k+m}{n} = l$. For the same case, but for sine function,

[63] Note that $r^m\,(v(k)) = \underbrace{r \circ r \circ \cdots \circ r}_{m \text{ times}}$.

from $\sin\frac{2(k+m)\pi}{n} = \sin\frac{2k\pi}{n}$ we get $\frac{2(k+m)\pi}{n} = \pi - \frac{2k\pi}{n} + 2l'\pi$, where $l' \in \mathbb{Z}$. Then, $\frac{k+m}{n} = \frac{1}{2} - \frac{k}{n} + l'$, i.e. $\frac{2k+m}{n} - \frac{1}{2} = l'$. Therefore, $l - \frac{1}{2} = l'$. But, if $l \in \mathbb{Z}$, then $l - \frac{1}{2} \notin \mathbb{Z}$ and that cannot be. If $l \notin \mathbb{Z}$, then, again, we are done. In conclusion, there does not exist $m \in \mathbb{Z}$ such that $0 < m < n$ and it must be that $\text{ord}\,(r) = n$.

□

Proposition. Let $i \in \mathbb{Z}$ and $r^i \in D_{2n}$. Then $r^i r^{-i} = e$ (in other words $(r^i)^{-1} = r^{-i}$).

Proof. Let $v(k) \in V_n$. Then $(r^i r^{-i})(v(k)) = r^i(r^{-i})(v(k)) = r^i(v(k-i)) = v(k-i+i) = v(k)$. Therefore, $r^i r^{-i} = e$.

□

Proposition. Let $s \in D_{2n}$. Then, $\text{ord}\,(s) = 2$.

Proof. Let $v(k) \in V_n$. We have $s(v(k)) = v(-k)$. Then,

$$s^2(v(k)) = [s \circ s](v(k)) = s(s(v(k))) = s(v(-k)) = v(-(-k)) = v(k).$$

Therefore, $s^2 = e$. As $s \neq e$ and $\text{ord}\,(s) = 1$ if and only if $s = e$, it must be that $\text{ord}\,(s) = 2$.

□

Proposition. Let $i \in \mathbb{N}$ and $r^i, s \in D_{2n}$. Then, $sr^i = r^{-i}s$. Also, $sr^k \neq sr^j$ and $sr^k \neq r^j$, for all $k \neq j$, $k, j \in \{0, \ldots, n-1\}$.

Proof. Let $v(k) \in V_n$. Then, $(sr^i)(v(k)) = [s \circ r^i](v(k)) = s(r^i(v(k))) = s(v(k+i)) = v(-k-i)$. Now, as $v(-k+(-i)) = r^{-i}(v(-k))$, we have $v(-k-i) = r^{-i}(v(-k)) = r^{-i}(s(v(k))) = (r^{-i}s)(v(k))$, i.e. $sr^i = r^{-i}s$. Assume $sr^k = sr^j$. Then, multiplying by s on the left, gives us $r^k = r^j$. But, $r^k \neq r^j$ for all $k \neq j$ such that $k, j \in \{0, \ldots, n-1\}$. Also, assume $sr^k = r^j$. That means that $s = r^{j-k}$. That cannot be as s would be a rotation.

□

Proposition. If $d \in D_{2n}$, then $d = s^i r^j$, where $i \in \{0, 1\}$ and $j \in \{0, \ldots, n-1\}$.

Proof. From a previous proposition, we have that $sr^i \neq sr^j$, for all $i \neq j$ and $i, j \in \{0, \ldots, n-1\}$. If we define $D = \{sr^i : i \in \{0, \ldots, n-1\}\}$, then $|D| = n$. Note that $s \in D$ as $s = sr^0$. Now, $|\langle r \rangle| = n$. Notice that $D \cap \langle r \rangle = \emptyset$. If we take $sr^i \in D$, then by a previous proposition $sr^i \neq r^j$, for all $r^j \in \langle r \rangle$. Therefore, $|D \cup \langle r \rangle| = 2n$. As $|D \cup \langle r \rangle| = D_{2n}$ and $D \cup \langle r \rangle \subseteq D_{2n}$, it follows that $D \cup \langle r \rangle = D_{2n}$. As $r^j = er^j = s^0 r^j$, for all $r^j \in \langle r \rangle$, and $sr^j \in D$, all elements of D_{2n} can be written as $s^i r^j$.

□

Proposition. Let $s^i r^j \in D_{2n}$, where $i \in \{0,1\}$ and $j \in \{0,\ldots,n-1\}$. Then, $(s^i r^j)^{-1} = r^{-j} s^i$.

Proof. Let $i = 1$. Then, $(sr^j)(r^{-j}s) = s^2 = e$. Let $i = 0$. Then $r^j r^{-j} = e$, by a previous proposition. That can be written as $(s^0 r^j)(r^{-j} s^0) = e$.

□

Proposition. Let $r, s \in D_{2n}$. Then, $\langle r \rangle \trianglelefteq D_{2n}$ and $D_{2n} = \langle r \rangle \langle s \rangle$.

Proof. Let $r^k \in \langle r \rangle$ and $s^i r^j \in D_{2n}$. Then, $(s^i r^j) r^k (r^{-j} s^i) = s^i r^{j+k-j} s^i = s^i r^k s^i$. Assume $i = 0$. Then $s^i r^k s^i = s^0 r^k s^0 = r^k$, so $(s^0 r^j) r^k (r^{-j} s^0) \in \langle r \rangle$. Assume $i = 1$. Then $(sr^k)s = (r^{-k}s)s$, by a previous proposition. Then, as $D_{2n} \leq S_{V_n}$, associativity implies $sr^k s = r^{-k} s^2 = r^{-k} \in \langle r \rangle$. Therefore, $(sr^j) r^k (r^{-j} s) \in \langle r \rangle$ and $\langle r \rangle \trianglelefteq D_{2n}$. If we take $s^i r^j \in D_{2n}$, then, if $i = 0$, $s^0 r^j = r^j = r^j e = r^j s^0 \in \langle r \rangle \langle s \rangle$ and, if $i = 1$, $sr^j = r^{-j} s \in \langle r \rangle \langle s \rangle$. That is, $D_{2n} \subseteq \langle r \rangle \langle s \rangle$. Now, if $r^j s^i \in \langle r \rangle \langle s \rangle$, then, if $i = 0$, $r^j \in D_{2n}$, and, if $i = 1$, $r^j s = sr^{-j} \in D_{2n}$. So, $\langle r \rangle \langle s \rangle \subseteq D_{2n}$ and $D_{2n} = \langle r \rangle \langle s \rangle$.

□

Remark. Notice that $\langle s \rangle$ is not a normal subgroup of D_{2n}. For example, $rsr^{-1} = sr^{-1}r^{-1} = sr^{-2} \notin \langle s \rangle$. That is why D_{2n} is not isomorphic to $\langle r \rangle \times \langle s \rangle$.

Proposition. Let $s, r \in D_{2n}$. Then $D_{2n} = \langle s, r : \ r^n = s^2 = e, \ rs = sr^{-1} \rangle$.

Proof. Let $D' = \langle s, r : \ r^n = s^2 = e, \ rs = sr^{-1} \rangle$. If we take $s^i r^j \in D_{2n}$, where $i \in \{0,1\}$, $j \in \{0,\ldots,n-1\}$, we know that $s^2 = e$ and $r^n = e$ for $s, r \in D_{2_n}$. But also, if we take $rs \in D_{2n}$, by using the rule $s^i r^j = r^{-j} s^i$, we have $rs = sr^{-1}$, when $i = 1$ and $j = 1$. Therefore, all $s^i r^j \in D_{2n}$satisfy rules set for D' and it must be that $D_{2n} \subseteq D'$.

Now, let us take $x \in D$. Then $x = x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$, where $x_1, \ldots, x_m \in \{s, r\}$ and $i_1, \ldots, i_m \in \mathbb{Z}$. By induction, using $s^2 = r^n = e$ and $rs = sr^{-1}$, we will show that x can be written as $s^i r^j$, for some $i, j \in \mathbb{Z}$. First, assume $x = x_1^{i_1} x_2^{i_2}$. *First case.* If $x_1 = s$ and $x_2 = s$, we have $x = s^{i_1} s^{i_2} = s^{i_1 + i_2}$. Set $i = i_1 + i_2$. Then $x = s^i = s^i e = s^i r^0$. Set $j = 0$. Then, $x = s^i r^0$. *Second case.* Assume $x_1 = r$ and $x_2 = r$. Then $x = r^{i_1} r^{i_2} = r^{i_1 + i_2}$. Set $j = i_1 + i_2$. Then, $x = r^j = er^j$ and $x = s^0 r^j$. Set $i = 0$ and then we have $x = s^i r^j$. *Third case.* If $x_1 = s$ and $x_2 = r$, we have $x = s^{i_1} r^{i_2}$. Then, $i = i_1$ and $j = i_2$ gives us $x = s^i r^j$. *Fourth case.* Finally, if $x_1 = r$ and $x_2 = s$, we have $x = r^{i_1} s^{i_2}$. As $i_2, 2 \in \mathbb{Z}$, then there exist $q, p \in \mathbb{Z}$ such that $i_2 = 2q + p$, where $0 \leq p < 2$, that is $p \in \{0,1\}$. Then, $s^{i_2} = s^{2q+p} = s^{2q} s^p$. Now, as $s^2 = r$ and $s^{2q} = (s^2)^q = e^q = e$, we have $s^{2q} s^p = es^p = s^p$ which implies $x = r^{i_1} s^p$, where $p \in \{0,1\}$. If $p = 0$, we have

$x = r^{i_1}s^0 = r^{i_1}e = r^{i_1} = er^{i_1} = s^0r^{i_1}$. Setting $i = 0$ and $j = i_1$ we have $x = s^ir^j$. Assume $p = 1$. Then $x = r^{i_1}s^1 = r^{i_1}s$. By induction we will prove that $r^{i_1}s = sr^{-i_1}$. For $i_1 = 0$ we have $r^0s = es = s = se = sr^0 = sr^{-0}$. Now, assume that $r^ks = sr^{-k}$. Then, $r^{k+1}s = r^krs = r^ksr^{-1} = sr^{-k}r^{-1} = sr^{-(k+1)}$. Therefore, we proved that if $m = 2$, we have $x = s^ir^j$, for some $i, j \in \mathbb{Z}$. Now, assume that $x = x_1^{i_1} \cdots x_m^{i_m} = s^ir^j$. Then, we need to prove that $y = x_1^{i_1} \cdots x_m^{i_m}x_{m+1}^{i_{m+1}} = s^zr^w$, for some $z, w \in \mathbb{Z}$. But, $y = xx_{m+1}^{i_{m+1}}$ and $x = s^ir^j$ by assumption of induction, for some $i, j \in \mathbb{Z}$, so $x = s^ir^jx_{m+1}^{i_{m+1}}$. If $x_{m+1} = s$, then, $y = s^ir^js^{i_{m+1}} = s^i(r^js^{i_{m+1}})$. Therefore, by using basis of induction, obviously $r^js^{i_{m+1}} = s^vr^w$, for some $v, w \in \mathbb{Z}$ and $y = s^is^vr^w = s^{i+v}r^w$. Setting $z = i+v$ we have $y = s^zr^w$. If $x_{m+1} = r$, then $y = s^ir^jr^{i_{m+1}} = s^ir^{j+i_{m+1}}$. Setting $z = i$ and $w = j + i_{m+1}$ we have $y = s^zr^w$. Therefore, every element $x \in D'$ can be shown as $x = s^ir^j$, where $i, j \in \mathbb{Z}$. By using division with remainder theorem, as $i, j, 2, n \in \mathbb{Z}$, we have $i = 2q_1 + r_1$ and $j = nq_2 + r_2$, where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \leq r_1 < 2$ (or equivalently, $r_1 \in \{0, 1\}$) and $0 \leq r_2 < n$ (that is, $r_2 \in \{0, \ldots, n-1\}$). We can see that then,

$$x = s^ir^j = s^{2q_1+r_1}r^{nq_2+r_2} = \left(s^2\right)^{q_1} s^{r_1} \left(r^n\right)^{q_2} r^{r_2}.$$

As $s^2 = e$ and $r^n = e$, then $x = s^{r_1}r^{r_2}$, where $r_1 \in \{0, 1\}$ and $r_2 \in \{0, \ldots, n-1\}$. Then, obviously $x \in D_{2n}$ and $D_{2n} \subseteq D'$. That implies, from the first part of the proof that $D_{2n} = D' = \langle s, r : \ r^n = s^2 = e, \ rs = sr^{-1} \rangle$.

□

Proposition. If $n \in 2\mathbb{Z}^+ - \{2\}$, $Z(D_{2n}) = \left\{e, r^{\frac{n}{2}}\right\}$. If $n \in (\mathbb{Z}^+ - \{1, 2\}) - 2\mathbb{Z}$, then $Z(D_{2n}) = \{e\}$.

Proof. We know that at least $e \in Z(D_{2n})$, for both cases. Take $r^i, s, r^j \in D_{2n}$, where $i, j \in \{0, \ldots, n-1\}$. First, we know that $r^ir^j = r^{i+j} = r^{j+i} = r^jr^i$. Therefore, r^i commutes with all r^j. Now, we check if it commutes with all other elements. Assume $r^i(sr^j) = (sr^j)r^i$. Then, that is equivalent to $sr^{-i}r^j = sr^jr^i$, i.e. to $r^{j-i} = r^{j+i}$ (after multiplying equality with s on the left). After multiplying by $r^{-(j-i)}$ on the left we have $r^{j+i-j+i} = e$, that is, $r^{2i} = e$. As $\text{ord}(r) = n$, it must be that $n|2i$. Then, there exists $q \in \mathbb{N}_0$ (as $n \in \mathbb{N}$ and $i \in \mathbb{N}_0$) such that $2i = nq$.

Assume n is even, i.e. $n = 2k$, for some $k \in \mathbb{N} - \{1\}$. Then, $2i = 2kq$, which is $i = kq$. For $q = 0$ we have $i = 0$, i.e. $r^0 = e$ (but we already know that $e \in Z(D_{2n})$. For $q = 1$ we have $i = k$, i.e. $r^k = r^{\frac{n}{2}}$. For $q = 2$ we have $i = 2k$, but $i < n$, so here we stop. Therefore, $r^{\frac{n}{2}} \in Z(D_{2n})$. Now, if we were considering sr^i, we would have to check first whether it commutes with r^j. But, then $sr^ir^j = r^jsr^i$ would give us $sr^{i+j} = sr^{i-j}$. That is, $r^{2j} = e$, and that can be either e or $r^{\frac{n}{2}}$. Now that sr^i would only commute

with e and $r^{\frac{n}{2}}$ it cannot be in the center (it has to commute with all elements of D_{2n}). Thus, $Z(D_{2n}) = \{e, r^{\frac{n}{2}}\}$ if n is even.

Assume n is odd, i.e. $n = 2k + 1$, for some $k \in \mathbb{N}$. Then, from $2i = nq$ we have $2i = 2kq + q$, i.e. $i = kq + \frac{q}{2}$. Now, if q is odd, $i \notin \mathbb{Z}$. So, we will only check when q is even, i.e. $q = 2q'$, for some $q' \in \mathbb{N}_0$. Then, $i = 2kq' + q'$. That gives us $i = 0$ for $q' = 0$ and $i = 2k + 1 = n$ if $q' = 1$. But, $i < n$, so we only have e that commutes. As we can only consider e for r^i, then, it is useless to check for sr^i (as then it would commute only with e, if viewing it in the same light as for when n is even). Therefore, $Z(D_{2n}) = \{e\}$ when n is odd.

□

Proposition. Let $n \in \mathbb{N} - \{1, 2\}$ and $s, r^i \in D_{2n}$, for some $i \in \{0, \ldots, n-1\}$. Then, $\text{ord}\,(sr^i) = 2$.

Proof. We have $(sr^i)(sr^i) = s(r^i s)r^i = s(sr^{-i})r^i = s^2 r^{-i+i} = ee = e$. Therefore, as $sr^i \neq e$, for all $i \in \{0, \ldots, n-1\}$, it must be that $\text{ord}\,(sr^i) = 2$.

□

Symmetries in $\mathbb{R}^3$

Proposition[64]. Let G be a group of rigid motions (without reflections, i.e. only reflections) and G_S a group of rotations and reflections of a Platonic solid. Then,

1. For a tetrahedron, $|G| = 12$ and $|G_S| = 24$.
2. For a cube and an octahedron, $|G| = 24$ and $|G_S| = 48$.
3. For a dodecahedron and an icosahedron, $|G| = 60$ and $|G_S| = 120$.

Proof. *Ad* 1. Tetrahedron has 4 vertices and 4 faces. Then, the number of edges is 6 as $4-6+4 = -2+4 = 2$. Let e be the number od edges that pass through each vertex. Then, that should be $\frac{e\cdot 4}{2} = 6$, as each edge contains two vertices. Then, $e \cdot 4 = 12$, so $e = 3$. Therefore, there are 3 edges through each vertex, and so each vertex has three adjacent vertices. For G, we will count only rotations. So, if we choose some vertex $v(i)$ we can send it to $v(k)$, which can be chosen in 4 different ways. Also, we want to send vertex adjacent to $v(i)$ some vertex adjacent to $v(k)$ (and there are three of them). Therefore, the total number is $|G| = 4 \cdot 3 = 12$. If we want to make our counting weaker, we can allow one of two remaining vertices adjacent to $v(i)$ to be sent to some of remaining vertices adjacent to $v(k)$ (two left). Therefore, we have two times more possibilities and that is $|G_S| = 4 \cdot 3 \cdot 2 = 24$.

Ad 2. Cube and octahedron are dual, so we will use a different counting method to grasp both. Now, cube has 6 faces with 4 vertices on each face. Octahedron has 8 faces with 3 vertices on each face. If we fix a face on a cube, it can be sent to 6 different faces and then rotated. There are 4 rotations, of course, so $|G| = 6 \cdot 4 = 24$. Same reasoning goes for octahedron, so $|G| = 8 \cdot 3 = 24$. If we allow reflections, we will allow not only rotations of faces, but also their reflections. That is the dihedral group D_8 for a cube and D_6 for octahedron (meaning, for each of their faces). Therefore, we have $|G_S| = 6 \cdot 8 = 8 \cdot 6 = 48$.

Ad 3. Same as above, we only need to know that dodecahedron has 20 vertices, 12 faces and 5 vertices on each. Icosahedron has 20 faces, as it is dual to dodecahedron. As it is composed of triangles, it has 3 vertices on each face. So, by the same reasoning as above, we have $|G| = 12 \cdot 5 = 20 \cdot 3 = 60$ and $|G_S| = 12 \cdot 10 = 20 \cdot 6 = 120$.

□

[64] Author's remark: as soon as I complete more precise drawings (which is a problem in all my writings), I will argue more strongly using the orbit-stabilizer theorem and preserve the following reasoning, perhaps, as a remark after the proposition. Then I will also add symmetries for pyramids and prisms and reaveal more about the group structure (which is not a big deal actually, just a lot of work).

Direct product

Theorem. Let G_1, G_2, H_1, H_2 be groups. If $G_1 \cong G_2$ and $H_1 \cong H_2$, then $G_1 \times H_1 \cong G_2 \times H_2$.

Proof. From $G_1 \cong G_2$ we have that there exists an isomorphism $g : G_1 \to G_2$ and from $H_1 \cong H_2$ that there exists an isomorphism $h : H_1 \to H_2$. Then, we define mapping $f : G_1 \times H_1 \to G_2 \times H_2$ with $f(x, y) = (g(x), h(y))$. We will show that f is well-defined. Take $(x, y) \in G_1 \times H_1$. Then, $x \in G_1$ and $y \in H_1$, and as g and h are well-defined we have $g(x) \in G_2$ and $h(y) \in H_2$, meaning $(g(x), h(y)) \in G_2 \times H_2$. If $(x_1, y_1) = (x_2, y_2)$, then $x_1 = x_2$ and $y_1 = y_2$, and, as g is well-defined that implies $g(x_1) = g(x_2)$ and, as h is well-defined, $h(y_1) = h(y_2)$. From that we have $(g(x_1), h(y_1)) = (g(x_2), h(y_2))$, i.e. $f(x_1, y_1) = f(x_2, y_2)$. Thus, f is also a well-defined function.

Now we will show that f is a bijection. *Surjectivity.* Take $(x', y') \in G_2 \times H_2$. Then, $x' \in G_2$ and $y' \in H_2$. As g and h are surjective, there exist $x \in G_1$ and $y \in H_1$ such that $g(x) = x'$ and $h(y) = y'$. Therefore, there exists $(g(x), h(y)) \in G_1 \times H_1$ such that $(g(x), h(y)) = (x', y')$ and f is surjective. *Injectivity.* Take $f(x_1, y_1) = f(x_2, y_2)$. From that follows $(g(x_1), h(y_1)) = (g(x_2), h(x_2))$. That implies $g(x_1) = g(x_2)$ and $h(y_1) = h(y_2)$. As g and h are injective, then that implies $x_1 = x_2$ and $y_1 = y_2$, i.e. $(x_1, y_1) = (x_2, y_2)$, so f is injective also. In conclusion it is also bijective. Finally, we have $f((x_1, y_1)(x_2, y_2)) = f(x_1x_2, y_1y_2) = (g(x_1x_2), h(y_1y_2)) = (g(x_1)g(x_2), h(y_1)h(y_2)) = (g(x_1), h(y_1))(g(x_2), h(y_2)) = f(x_1, y_1)f(x_2, y_2)$, so f is an isomorphism from $G_1 \times H_1$ to $G_2 \times H_2$.

□

Corollary. Let G, K and H be groups. If $G \cong K$, then $G \times H \cong K \times H$.

Proof. The relation of being isomorphic is a relation of equivalence, so it is reflexive, and for group H, we have $H \cong H$. Along with $G \cong K$, using the previous theorem, we get $G \times H \cong K \times H$.

□

Corollary. Let G, H, H_1, K be groups. If $G \cong H \times K$ and $H \cong H_1$, then $G \cong H_1 \times K$.

Proof. We have $H \cong H_1$ and $K \cong K$. Then, by previous theorem, $H \times K \cong H_1 \times K$. As relation of being isomorphic is a relation of equivalence, it is also transitive, so $G \cong H \times K$ and $H \times K \cong H_1 \times K$ implies $G \cong H_1 \times K$.

□

Definition. Let $n \in \mathbb{Z}^+$ and $G_1, \ldots, G_n$ be groups with $e_1, \ldots, e_n$ as their neutral elements, respectively, and $i \in \{1, \ldots, n\}$. Then, we define:

$$\widehat{G_i} = \{e_1\} \times \cdots \times \{e_{i-1}\} \times G_i \times \{e_{i+1}\} \times \cdots \{e_n\}.$$

Lemma. Let $n \in \mathbb{Z}^+$ and let $G_1, \ldots, G_n$ be groups. Then, for all $i \in \{1, \ldots, n\}$,

$$\widehat{G_i} \cong G_i.$$

Proof. Let us denote $\widehat{x_i} = (e_1, \ldots, e_{i-1}, x, e_{i+1}, \ldots, x_n)$, for all $x \in G_i$. We define $f : \widehat{G_i} \to G_i$ with $f(\widehat{x_i}) = x$. Then, f is well-defined because, if we take $\widehat{x_i} \in \widehat{G_i}$, we have $x \in G_i$, so $f(\widehat{x_i}) = x$. Also, f satisfies property of uniqueness, because if $\widehat{x_i} = \widehat{y_i}$, then obviously $x = y$ (that is, $f(\widehat{x_i}) = f(\widehat{y_i})$) as they are both on i-th place. *Surjectivity.* Take $x \in G_i$. Then, it is obvious that there exists $\widehat{x_i} \in \widehat{G_i}$, as then x is on the i-th place and is therefore in G_i, such that $f(\widehat{x_i}) = x$. *Injectivity.* Let $f(\widehat{x_i}) = f(\widehat{y_i})$, i.e. $x = y$. Then it is easy to see that $\widehat{x_i} = \widehat{y_i}$, because all other places have e_j, where $j \in \{0, \ldots, n\} - \{i\}$. Thus, f is bijective. Finally, $f(\widehat{x_i}\widehat{y_i}) = f(\widehat{xy_i}) = xy = f(\widehat{x_i})f(\widehat{y_i})$ and f is an isomorphism which brings us to $\widehat{G_i} \cong G_i$.

□

Lemma. Let $n \in \mathbb{Z}^+$ and let $G_1, \ldots, G_n$ be groups. Then,

$$\pi_i : G_1 \times \cdots \times G_n \to G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n,$$

defined with

$$\pi_i(x_1, \ldots, x_n) = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n),$$

for all $i \in \{1, \ldots, n\}$, is a surjective homomorphism and $\ker(\pi_i) \cong G_i$.

Proof. Let us denote $G = G_1 \times \cdots \times G_n$ and $G' = G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$. First, we will prove that π_i is well-defined. Take $X \in G$. Then, $X = (x_1, \ldots, x_n)$, where $x_j \in G_j$, for all $j \in \{1, \ldots, n\}$. That implies that $X' = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in G'$, so $\pi_i(X) = X'$. Now, if $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$, then, $x_j = y_j$, for all $j \in \{1, \ldots, n\}$, which implies $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = (y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n)$, that is $\pi_i(x_1, \ldots, x_n) = \pi_i(y_1, \ldots, y_n)$. Let $X' \in G'$. Then $X' = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$, where $x_j \in G_j$, for all $j \in \{1, \ldots, n\} - \{i\}$. But, we can take, e.g. $e_i \in G_i$, to have $\pi_i(x_1, \ldots, x_{i-1}, e_i, x_{i+1}, \ldots, x_n) = X'$. Therefore, π_i is well-defined and surjective. Finally,

$$\begin{aligned}\pi_i((x_1,\ldots,x_n)(y_1,\ldots,y_n)) &= \pi_i(x_1y_1,\ldots,x_ny_n)\\ &= (x_1y_1,\ldots,x_{i-1}y_{i-1},x_{i+1}y_{i+1},\ldots,x_ny_n)\\ &= (x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)(y_1,\ldots,y_{i-1},y_{i+1},\ldots,y_n)\\ &= \pi_i(x_1,\ldots,x_n)\pi_i(y_1,\ldots,y_n).\end{aligned}$$

Thus, π_i is a surjective homomorphism. Finally, $\ker(\pi_i) = \{(x_1,\ldots,x_n) \in \operatorname{dom}(\pi_i) : \pi_i(x_1,\ldots,x_n) = (e_1,\ldots,e_{i-1},e_{i+1},\ldots,e_n)\}$. But, that means $\ker(\pi_i) = \{(x_1,\ldots,x_n) \in \operatorname{dom}(\pi_i) : (x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n) = (e_1,\ldots,e_{i-1},e_{i+1},\ldots,e_n)\}$, i.e. $\ker(\pi_i) = \{(e_1,\ldots,e_{i-1},x,e_{i+1},\ldots,e_n) \in \operatorname{dom}(\pi_i) : x \in G_i\} = \widehat{G_i}$. By previous lemma, $\widehat{G_i} \cong G_i$, so $\ker(\pi_i) \cong G_i$.

□

Theorem. Let $n \in \mathbb{Z}^+$ and let $G_1,\ldots,G_n$ be groups and $i \in \{1,\ldots,n\}$. Then,

$$G_1 \times \cdots \times G_n/\widehat{G_i} \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

Proof. Follows directly from the previous lemma, by the fundamental homomorphism theorem (applicable as π_i is surjective homomorphism).

□

Corollary. Let $n \in \mathbb{Z}^+$ and let $G_1,\ldots,G_n$ be groups and $i \in \{1,\ldots,n\}$. Then,

$$\widehat{G_i} \trianglelefteq G_1 \times \cdots \times G_n.$$

Proof. Follows from the previous theorem and its lemma, as $\ker(\pi_i) = \widehat{G_i}$ and we know $\ker(\pi_i) \trianglelefteq \operatorname{dom}(\pi_i) = G_1 \times \cdots \times G_n$.

□

Remark. This is most easily seen in Euclidean spaces. For example, if we have $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ and $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, then getting the quotient group $\mathbb{R}^3/\widehat{\mathbb{R}_i} \cong \mathbb{R}^2$, for any $i \in \{1,2,3\}$, is the same as projecting the Euclidean space on the Euclidean plane.

Rings

Definition. Let A be a non-empty set, $+ : A \times A \to A$ (addition) and $\cdot : A \times A \to A$ (multiplication) binary operations defined on A. An ordered triple $(A, +, \cdot)$ is called a **ring** if the following axioms are satisfied:

1. $(A, +)$ is an Abelian group.
2. $(A, \cdot)$ is a semigroup[65].
3. Multiplication is distributive over addition. In other words, for all $a, b, c \in A$:

$$\begin{aligned} a(b+c) &= ab + ac, \\ (b+c)a &= ba + ca. \end{aligned}$$

Remark. A neutral element in A is denoted with 0 and inverse of $a \in A$ is denoted as $-a$. Also, as in group theory, we will denote ring $(A, +, \cdot)$ only with A. Notice that the corresponding set of $(A, +, \cdot)$ is A.

Definition. Let A be a ring. Then, we define **subtraction** as $- : A \times A \to A$ with $a - b = a + (-b)$, for all $a, b \in A$.

Remark. We can see that subtraction is well defined as each element in a A has an additive inverse (A with addition is an Abelian group).

Example. Here are some examples of rings:

- $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$;
- $\mathbb{Q} = (\mathbb{Q}, +, \cdot)$;
- $\mathbb{R} = (\mathbb{R}, +, \cdot)$;
- $\mathbb{C} = (\mathbb{C}, +, \cdot)$;
- $\mathbb{Z}_n = (\mathbb{Z}_n, +_n, \cdot_n)$;
- $\mathcal{F}(\mathbb{R}) = (\mathcal{F}(\mathbb{R}), +, \cdot)$ with $[f + g](x) = f(x) + g(x)$ and $[fg](x) = f(x)g(x)$, for all $x \in \mathbb{R}$.

[65] I.e. it is associative.

Definition. Let A be a ring. If corresponding set of ring A is finite, then we say that A is finite.

Theorem. Let A be a ring and $a, b \in A$. Then:

1. $a0 = 0a = 0$;
2. $a(-b) = -(ab)$ and $(-a)b = -(ab)$;
3. $(-a)(-b) = ab$.

Proof. *Ad* 1. We use the fact that $a + 0 = a$. We have $aa + 0 = aa$. But, also, as $a = a + 0$, we can write $aa + 0 = a(a + 0)$. By distributive law, $aa + 0 = aa + a0$. We can write that as $a^2 + 0 = a^2 + a0$. As A is closed with respect to multiplication, then $a^2 \in A$ and so a^2 has an additive inverse $-a^2$. We apply that on the left side of equality to get $-a^2 + a^2 + 0 = -a^2 + a^2 + a0$. That gives us $0 + 0 = 0 + a0$, i.e. $0 = a0$. Now to prove that $0a = 0$, we simply use again $aa + 0 = aa$, but substitute $a = a + 0$ so that $aa + 0 = (a + 0)a$. From that we have $a^2 + 0 = a^2 + 0a$. Again, applying $-a^2$ on the left gives us $-a^2 + a^2 + 0 = -a^2 + a^2 + 0a$. Then, $0 + 0 = 0 + 0a$, which is $0 = 0a$.

Ad 2. We have $a0 = 0$. Also, $b + (-b) = 0$. From that we get $a(b + (-b)) = 0$. By distributive law, $ab + a(-b) = 0$. As $ab \in A$ (closed with respect to multiplication), then $-(ab) \in A$ is the additive inverse of ab. Therefore, applying $-ab$ on the left we get $-ab + ab + a(-b) = -ab + 0$. From that we have $0 + a(-b) = -(ab)$, i.e. $a(-b) = -(ab)$. Similarly, as $0b = 0$ and $a + (-a) = 0$ we have $(a + (-a))b = 0$. By distributive law $ab + (-a)b = 0$. Then, using the inverse $-(ab)$ we get $(-a)b = -(ab)$.

Ad 3. We have $a + (-a) = 0$ and $0(-b) = 0$, so $(a + (-a))(-b) = 0$. By distributive law, $a(-b) + (-a)(-b) = 0$. From previous property, we have $a(-b) = -(ab)$. Therefore, $-(ab) + (-a)(-b) = 0$. As $-(-(ab)) = ab$ (result from group theory), we can apply ab on the left of the equality to get $ab + (-ab) + (-a)(-b) = ab + 0$. From that follows $0 + (-a)(-b) = ab$, i.e. $(-a)(-b) = ab$.

□

Definition. Let $(A, +, \cdot)$ be a ring. We say that A is:

- **Commutative ring** if $(A, \cdot)$ is a commutative semigroup, i.e. associativity holds $(a(bc) = (ab)c$, for all $a, b, c \in A)$ and $ab = ba$, for all $a, b \in A$.
- **Commutative ring with unity** if $(A, \cdot)$ is a commutative monoid, i.e. it has a neutral element usually designated as 1 $(1a = a1 = a$, for all $a \in A)$ and $ab = ba$, for all $a, b \in A$.
- **Skew field** if $(A - \{0\}, \cdot)$ is a group.

- **Field** if $(A - \{0\}, \cdot)$ is an Abelian group.

Proposition. Let A be a commutative ring with unity. Then, 0 has a multiplicative inverse if and only if A is trivial ($A = \{0\}$).

Proof. *Necessity.* Suppose 0 is invertible. Then, there exists $a \in A$ such that $a0 = 1$. But, by a previos theorem $a0 = 0$, so $0 = 1$. Suppose that there exists some $a \in A$, $a \neq 0, 1$. Then, as A is a commutative ring, $a1 = a$, but, as $0 = 1$, we have $a0 = a$, i.e. $a = 0$. Therefore, $A = \{0\}$. *Sufficiency.* Suppose $A = \{0\}$. Then, A is a commutative ring with unity. Neutral element for addition is 0. Inverse is $-0 = 0$ (as $0 + (-0) = 0$ and, as 0 is a neutral element, $-0 = 0$). It is commutative and associative. As for multiplication it is also commutative and associative. Neutral element is 0 as $00 = 0$. Inverse element is 0, again, as $00 = 0$.

□

Definition. Let A be a ring. Element $a \in A$, $a \neq 0$ is called **divisor of zero** if there exists $b \in A$, $b \neq 0$, such that $ab = 0$ or $ba = 0$.

Proposition. Let A be a ring. If there does not exist a divisor of zero in A, then $ab = 0$ implies $a = 0$ or $b = 0$.

Proof. Let A be a ring with no divisors of zero. Let $ab = 0$. Assume that $a \neq 0$ and $b \neq 0$. Then, from $ab = 0$ it follows by definition that a and b are divisors of zero, which is contrary to our assumption.

□

Definition. Let A be a ring. We say that A has the **cancellation property** if $ab = ac$ or $ba = ca$ implies $b = c$, for all $a, b, c \in A$ with $a \neq 0$.

Remark. Let A be a ring. Then $0b = 0c$ gives no information about the nature of $b = c$. For example, in $\mathbb{Z}$, $0 \cdot 5 = 0 \cdot 2$, but $5 \neq 2$. Thus, we have excluded 0 in the previous definition.

Proposition. Ring A has a cancellation property if and only if it has no divisors of zero.

Proof. *Necessity.* Assume that $ab = ac$ or $ba = ca$ implies $b = c$, for all $a, b, c \in A$, $a \neq 0$. Assume that there exist $d, e \in A$, $d \neq 0$ and $e \neq 0$ such that $de = 0$. As $e0 = 0$, then $de = 0e$. By cancellation property (applicable as $e \neq 0$), we have $d = 0$ which is contrary to our assumption that $d \neq 0$. Therefore, there do not exist divisors of zero in

A. Sufficiency. Assume A has no divisors of zero. Then, $ab = 0$ implies $a = 0$ or $b = 0$, for all $a, b \in A$. Assume $ab = ac$, with $a \neq 0$. As A is Abelian with respect to addition, then there exists $-(ac) \in A$ such that $ac + (-(ac)) = 0$. Applying $-(ac)$ on the right gives us $ab + (-(ac)) = ac + (-(ac))$, i.e. $ab + (-(ac)) = 0$. By a previous theorem, $-(ac) = a(-c)$. Therefore, $ab + a(-c) = 0$. By distributive law, $a(b + (-c)) = 0$. As A has no divisors of zero, it follows that $a = 0$ or $b + (-c) = 0$. But, we assumed $a \neq 0$, therefore the only remaining possibility is that $b + (-c) = 0$. From that we have, by applying $c \in A$ on the right, $b + (-c) + c = c$, i.e. $b = c$. Similarly we can prove that $ba = ca$ implies $b = c$.

□

Definition. Let A be a non-trivial commutative ring with unity such that it has cancellation property (or, equivalently, no divisors of zero). Then we say that A is an **integral domain**.

Problem. In each of the following, a set A with operation of addition and multiplication is given. Prove that A satisfies all the axioms to be a commutative ring with unity. Indicate the zero element, the unity, and the negative of an arbitrary a.

1. $A = (\mathbb{Z}, \oplus, \odot)$, where $a \oplus b = a + b - 1$ and $a \odot b = ab - (a + b) + 2$;
2. $A = (\mathbb{Q}, \oplus, \odot)$, where $a \oplus b = a + b + 1$ and $a \odot b = ab + a + b$;
3. $A = (\mathbb{Q} \times \mathbb{Q}, \oplus, \odot)$, where $(a, b) \oplus (c, d) = (a + c, b + d)$ and $(a, b) \odot (c, d) = (ac - bd, ad + bc)$;
4. $A = \{x + y\sqrt{2} : \ x, y \in \mathbb{Z}\}$ with conventional addition and multiplication.

Solution.

1. $A = (\mathbb{Z}, \oplus, \odot)$, *where* $a \oplus b = a + b - 1$ *and* $a \odot b = ab - (a + b) + 2$*;* From problem on page 2 we have that $\mathbb{R}$ with $\oplus$ is an Abelian group (reader will notice that all the properties on page 12 do not depend on properties of $\mathbb{R}$ specifically and can be narrowed down to $\mathbb{Z}$ without much problem). We will assume associativity for $\odot$, but we have already proved it for a similar operation on page 12. Now we will check distributive laws. We observe $a \odot (b \oplus c) = a \odot (b + c - 1) = a(b + c - 1) - (a + (b + c - 1)) + 2 = ab + ac - a - a - b - c + 1 + 2 = ab + ac - 2a - b - c + 3$. Now, $a \odot b \oplus a \odot c = (ab - (a + b) + 2) \oplus (ac - (a + c) + 2) = ab - (a + b) + 2 + ac - (a + c) + 2 - 1 = ab - 2a - b - c + 3$. Therefore, $a \odot (b \oplus c) = a \odot b \oplus a \odot c$. Similarly, we can show that $(a \oplus b) \odot c = a \odot c \oplus b \odot c$. But, we will first prove commutativity for $\mathbb{Z}$ with $\odot$. We have $a \odot b = ab - (a + b) + 2 = ba - (b + a) + 2 = b \odot a$. Therefore, A is commutative. So, $(a \oplus b) \odot c = c \odot (a \oplus b) = c \odot a \oplus c \odot b = a \odot c \oplus b \odot c$

and A is a commutative ring. It's zero element is the neutral element for $\oplus$ and that can be obtained from $a + e - 1 = a$, i.e. $e = 1$. So, here, zero is 1. Neutral element in $\mathbb{Z}$ with $\odot$ can be obtained from $ae - (a + e) + 2 = a$. From that we have $ae - a - e + 2 = a$, i.e. $e(a - 1) = 2a + 2$. That implies $e(a - 1) = 2(a - 1)$. Assume $a \neq 1$. Then $e = 2$. But, if $a = 1$, we have $2 \odot 1 = 2 \cdot 1 - (2 + 1) + 2 = 2 - 2 - 1 + 2 = 1 = 1 \odot 2$. Therefore, neutral element for $\odot$ in $\mathbb{Z}$ is 2. Therefore, A is a commutative ring with unity. Then, we will find multiplicative inverses. It must be that $a \odot a^{-1} = 2$, for all $a \neq 1$. That implies $aa^{-1} - (a + a^{-1}) + 2 = 2$, i.e. $a^{-1}(a - 1) = a$. From that we have, as $a \neq 1$, that $a^{-1} = \frac{a}{a-1}$. But, $\frac{a}{a-1} \in \mathbb{Z}$ if and only if $a - 1|a$, i.e. if there exists $q \in \mathbb{Z}$ such that $a = q(a - 1)$. From that we have that $q|a$ (assuming $q \neq 0$) and then it's $\frac{a}{q} = a - 1$. That is equivalent to (for $a \neq 1$, of course) $\frac{a}{q}\frac{1}{a-1} = 1$. Therefore, as $\frac{a}{q} = k$, for some $k \in \mathbb{Z}$, it must be that $\frac{1}{a-1} = \pm 1$. Then, $\pm 1 = a - 1$ implies $a = 2$ or $a = 0$. If $q = 0$ then it would mean that $a = 0$, again. Therefore, the only invertible elements in A are in $A^* = \{0, 2\}$.

2. $A = (\mathbb{Q}, \oplus, \odot)$, *where* $a \oplus b = a + b + 1$ *and* $a \odot b = ab + a + b$*;* We also know from page 12 that $(\mathbb{Q}, \oplus)$ is a commutative group (see reasoning from previous problem). We have proven associativity for the similar operation on page 12. Now, we will check distributivity. We have $a \odot (b \oplus c) = a \odot (b + c + 1) = a(b + c + 1) + a + (b + c + 1) = ab + ac + 2a + b + c + 1$. Then, $a \odot b \oplus a \odot c = (ab + a + b) \oplus (ac + a + c) = ab + a + b + ac + a + c + 1 = ab + 2a + b + c + 1$. Therefore, first distributive law holds. The second one will hold if we prove $\odot$ is commutative. We have $a \odot b = ab + a + b = ba + b + a = b \odot a$. Therefore, $(a \oplus b) \odot c = c \odot (a \oplus b)$, wherein follows the first distributive law. Then we seek zero element from $a \oplus e = a$, i.e. $a + e + 1 = a$. That gives us $e = -1$. Now, we get unity from $ae + a + e = a$. We have $e(a + 1) = 0$, so $e = 0$. Therefore, zero element is -1 and unity is 0. Multiplicative inverses are obtained from $aa^{-1} + a + a^{-1} = 0$. Then, $a^{-1}(a + 1) = -a$, i.e. $a^{-1} = \frac{-a}{a+1}$, where $a \neq -1$ (zero element). As $\frac{-a}{a+1} \in \mathbb{Q}$, for all $a \in \mathbb{Q}$, $a \neq -1$, all non-zero elements have an inverse and therefore, A is a field.

3. $A = (\mathbb{Q} \times \mathbb{Q}, \oplus, \odot)$, *where* $(a, b) \oplus (c, d) = (a + c, b + d)$ *and* $(a, b) \odot (c, d) = (ac - bd, ad + bc)$*;* We already know from a previous exercise that $\mathbb{Q} \times \mathbb{Q}$ with $\oplus$ is an Abelian group. Also, we know that $\mathbb{Q} \times \mathbb{Q} - \{(0, 0)\}$ is also an Abelian group (similar to multiplication of complex numbers). So, we will check distributive law. We have $(a, b) \odot ((c, d) \oplus (e, f)) = (a, b) \odot (c + e, d + f) = (a(c + e) - b(d + f), a(d + f) + b(c + e)) = (ac + ae - bd - bf, ad + af + bc + be)$. Similarly, $(a, b) \odot (c, d) \oplus (a, b) \odot (e, f) = (ac - bd, ad + bc) \oplus (ae - bf, af + be) = (ac + ae - bd - bf, ad + af + bc + be)$. Therefore, distributivity holds (as $\odot$ is commutative, second distributive law holds - see previous two exercises). As $\mathbb{Q} \times \mathbb{Q} - \{(0, 0)\}$

is an Abelian group, A is a field. Note that $(0,0)$ is zero and $(1,0)$ is unity (as $(1,0)(a,b) = (1a+0b, 1b+0a) = (a,b)$, etc.).

4. $A = \{x + y\sqrt{2} : \ x, y \in \mathbb{Z}\}$ *with conventional addition and multiplication.* We will prove that $(A,+) \leq \mathbb{R}$ and $(A,\cdot) \leq \mathbb{R}^*$. First, if $a \in A$, then $a = x + y\sqrt{2}$, where $x, y \in \mathbb{Z}$. Then, $a \in \mathbb{R}$. So, $A \subseteq \mathbb{R}$. If we take $a, b \in A$, then $a = x + y\sqrt{2}$ and $b = z + w\sqrt{2}$. We have $a + b = (x+z) + (y+w)\sqrt{2}$ so $a + b \in A$. Similarly, $ab = (x + y\sqrt{2})(z + w\sqrt{2}) = (xz + 2yw) + (yz + xw)\sqrt{2}$ and $ab \in A$. If $a \in A$, then $-a = (-x) + (-y)\sqrt{2}$ and $-a \in A$. But, $a^{-1} = \frac{1}{x+y\sqrt{2}}$ is not necessarily in A. Therefore, $(A,+)$ is an Abelian group and $(A,\cdot)$ is a commutative monoid. Distributivity is inherited from addition and multiplication in $\mathbb{R}$ and that means that $(A,+,\cdot)$ is a commutative ring with unity.

Problem. Verify that $\mathcal{F}(\mathbb{R})$ satisfies all the axioms for being a commutative ring with unity. Indicate the zero and unity, and desribe the negative of any f. Describe the divisors of zero and invertible elements in $\mathcal{F}(\mathbb{R})$ and explain why $\mathcal{F}(\mathbb{R})$ is neither a field nor an integral domain.

Solution. We know that $\mathcal{F}(\mathbb{R})$ when considering only addition is an Abelian group. Zero is obviously $f(x) = 0$. But, $\mathcal{F}(\mathbb{R})$ when observing multiplication is only a commutative monoid, as not all functions have multiplicative inverses. As $[fg](x) = f(x)g(x)$, for all $x \in \mathbb{R}$, we need $\left[ff^{-1}\right](x) = f(x)\frac{1}{f(x)} = x$, for all $x \in \mathbb{R}$. But, if e.g. $f(x) = x - a$, then $f^{-1}(a) = \frac{1}{a-a} = \frac{1}{0}$ is not defined. Unity is $f(x) = 1$. Distributive law holds as $f(x)(g(x)+h(x)) = f(x)[g+h](x) = [f(g+h)](x) = [fg+fh](x) = [fg](x)+[fh](x) = f(x)g(x)+f(x)h(x)$. Second distributive law holds as $\mathcal{F}(\mathbb{R})$ is commutative. Therefore, $\mathcal{F}(\mathbb{R})$ is a commutative ring with unity. If we have $f(x)g(x) = 0$, then, not necessarily $f(x) = 0$ or $g(x) = 0$. Take $f(x) = x\mathcal{I}_{\langle -\infty, 0\rangle}$ and $g(x) = x\mathcal{I}_{[0,\infty\rangle}$. Then obviously $f(x)g(x) = 0$, but $f(x) \neq 0$ and $g(x) \neq 0$. Thus, $\mathcal{F}(\mathbb{R})$ is not an integral domain.

Problem. Let $\mathcal{M}_2$ designate the set of all 2×2 matrices (with entries from $\mathbb{R}$) with usual addition and multiplication. Verify that $\mathcal{M}_r(\mathbb{R})$ satisfies the ring axioms and unity, but not commutativity. Explain why $\mathcal{M}_2(\mathbb{R})$ is not an integral domain or a field.

Solution. We know from previous exercises that $\mathcal{M}_2$ under matrix addition is an Abelian group and a monoid under matrix mulitiplication. Checking distributivity is easy but tedious (as I am really tired and want to focus on more important stuff). Thus, $\mathcal{M}_2$ is a ring with unity. Also, it is a trivial fact from linear algebra that $AB = 0$ does not imply $A = 0$ or $B = 0$, so $\mathcal{M}_2$ is not an integral domain.

Problem. If D is a set, then the power set of D is the set $\mathcal{P}_D$ of all the subsets of

D. Addition and multiplication are defined with $A + B = (A - B) \cup (B - A)$ and $AB = A \cap B$. Prove that $\mathcal{P}_D$ is a commutative ring with unity. Describe the divisors of zero and invertible elements in $\mathcal{P}_D$ and explain why it is neither a field nor an integral domain.

Solution. We know from a previous exercise that $\mathcal{P}_D$ with addition is an Abelian group and $\mathcal{P}_D$ with multiplication is a commutative monoid (we have no inverse for intersection). We will also assume distributivity. Proving it is a bit tedious but elementary. Zero is $\emptyset$ as $A + \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$. Unity is D as $A \cap D = A$. Now, from $AB = \emptyset$ we have $A \cap B = \emptyset$. Divisors of zero are sets that are disjoint as $A \cap B = \emptyset$ implies that. Invertible elements for addition is $-A = A$ as $A + A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$. Invertible elements for multiplication are $AA^{-1} = D$. But, that is $A \cap A^{-1} = D$. From that we have that the only invertible element is actually D whose inverse is D. Therefore, $\mathcal{P}_D$ is not a field, and as it has divisors of zero, it is not an integral domain.

Definition. Let $(G, +)$ be an Abelian group. An **endomorphism** of G is a homomorphism from G to G. By $\mathrm{End}\,(G)$ we denote the set of all endomorphisms of G and define $[f + g](x) = f(x) + g(x)$ and $[fg](x) = [f \circ g](x)$, for every $x \in G$.

Proposition. Let $(G, +)$ be an Abelian group. Then, $\mathrm{End}\,(G)$ is a ring with unity.

Proof. First we will check the group axioms for $+$. *Associativity.* For all $f, g, h \in \mathrm{End}\,(G)$ we have $[[f + g] + h](x) = [f + g](x) + h(x) = (f(x) + g(x)) + h(x)$. As G is associative, then $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x)) = f(x) + [g + h](x) = [f + [g + h]](x)$. *Identity (zero).* If $f \in \mathrm{End}\,(G)$ then we need $0 \in \mathrm{End}\,(G)$ such that $[f + 0](x) = [0 + f](x) = f(x)$, for all $x \in G$. As G is a group it has an identity $0 \in G$. Then, $0(x) = 0$ would work as $[f + o](x) = f(x) + 0(x) = f(x) + 0$. As $f(x) \in G$ (it is an endomorphism), then $f(x) + 0 = f(x)$. It is easy to see that 0 is an endomorphism, as $0 : G \to G$ and $o(x + y) = 0 = 0 + 0 = 0(x) + 0(y)$. Also, this works for $[0 + f](x) = f(x)$, as G is Abelian. *Inverses.* We need $-f \in \mathrm{End}\,(G)$ such that $[f + (-f)](x) = [-f + f](x) = 0(x)$. Then, as $f(x) \in G$, it has an inverse $-[f(x)] \in G$. Therefore, we will define $-f(x) = -[f(x)]$. Also, $-f$ is an endomorphism as $-f(x + y) = -[f(x + y)] = -[f(x) + f(y)] = -[f(y)] + (-[f(x)])$. As G is Abelian, $-[f(y)] + (-[f(x)]) = -[f(x)] + (-[f(y)]) = -f(x) + (-f(y))$. Now, $[f + (-f)](x) = f(x) + (-f(x))$. As $f(x) \in G$ and $-f(x) = -[f(x)]$, where $-[f(x)] \in G$ is an inverse of $f(x) \in G$, we have $f(x) + (-[f(x)]) = 0 = 0(x)$. As G is Abelian, $[-f + f](x) = 0(x)$, also. Now, from $f, g \in \mathrm{End}\,(G)$ we have $[f + g](x) = f(x) + g(x)$. As G is Abelian, $f(x) + g(x) = g(x) + f(x) = [g + f](x)$. Therefore, $\mathrm{End}\,(G)$ is an Abelian group.

We will check distributive laws. We have $[f[g + h]](x) = [f \circ [g + h]](x) = f([g +$

$h](x)) = f(g(x)+h(x))$. Now, as f is an endomorphism, i.e. a homomorphism from G to G, then $f(g(x)+h(x)) = f(g(x))+f(h(x)) = [f\circ g](x)+[f\circ h](x) = [fg](x)+[fh](x)$. In other words, $f(g+h) = fg+fh$. As composition is not generally commutative, we need to check $[[g+h]f](x) = [[g+h]\circ f](x) = [g+h](f(x)) = g(f(x))+h(f(x)) = [gf](x)+[hf](x)$, i.e. $(g+h)f = gf+hf$. *Associativity.* Function composition is associative and so is composition in $\mathrm{End}\,(G)$. *Identity (unity).* We need to find $1 \in \mathrm{End}\,(G)$ such that $[f1](x) = [1f](x) = f(x)$. If we take $1(x) = x$, for all $x \in G$, then $1 : G \to G$ is an endomorphism as $1(x+y) = x+y = 1(y)+1(y)$. Now, $[f1](x) = f(1(x)) = f(x)$ and $[1f](x) = 1(f(x)) = f(x)$. Therefore, $1 \in \mathrm{End}\,(G)$ is a unity and $\mathrm{End}\,(G)$ is a ring with unity. Notice that endomorphisms are not necessarily bijections and might have no inverses. Also, composition is not generally commutative.

□

Definition. Let A and B be rings. We define the **direct product of rings** A and B as $A \times B$ such that for all $(x_1, y_1), (x_2, y_2) \in A \times B$ it holds:

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &= (x_1 + x_2, y_1 + y_2),\\ (x_1, y_1)(x_2, y_2) &= (x_1x_2, y_1y_2).\end{aligned}$$

Proposition. Let A and B be rings. Then:

1. $A \times B$ is a ring.
2. If A and B are commutative, then so is $A \times B$.
3. If A and B have unity, then so does $A \times B$.
4. $A \times B$ can never be an integral domain or a field.

Proof. *Ad* 1. As A and B are Abelian groups when considering addition, then, by a previous proposition, set $A \times B$ with addition is an Abelian group. Similarly, from the proof of the same proposition, we can conclude that, when considering multiplication, from A and B are semigroups it follows that $A \times B$ is a semigroup. Therefore, we only need to check distributivity. First, $(x_1, y_1)((x_2, y_2) + (x_3, y_3)) = (x_1, y_1)(x_2 + x_3, y_2 + y_3) = (x_1(x_2+x_3), y_1(y_2+y_3))$. As $x_1, x_2, x_3 \in A$, and A is a ring, distributivity holds, so $x_1(x_2+x_3) = x_1x_2+x_1x_3$. Similarly, as B is a ring, $y_1(y_2+y_3) = y_1y_2+y_1y_3$. Therefore, $(x_1(x_2 + x_3), y_1(y_2 + y_3)) = (x_1x_2 + x_1x_3, y_1y_2 + y_1y_3) = (x_1x_2, y_1, y_2) + (x_1x_3, y_1y_3) = (x_1, y_1)(x_2, y_2) + (x_1, y_1)(x_3, y_3)$. Similarly we prove the second distributive law. Therefore, $A \times B$ is a ring.

Ad 2. If A and B are commutative rings, then for all $a_1, a_2 \in A$ we have $a_1a_2 = a_2a_1$ and for all $b_1, b_2 \in B$ that $b_1b_2 = b_2b_1$. Thus, if we take $(a_1, b_1), (a_2, b_2) \in A \times B$ we have $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2, b_2)(a_1, b_1)$.

Ad 3. Assume that there exists $1_A \in A$ and $1_B \in B$ such that $1_Aa = a1_A = a$, for all $a \in A$ and $1_Bb = b1_B = b$, for all $b \in B$. Then, $(1_A, 1_B) \in A \times B$ is unity in $A \times B$ as $(1_A, 1_B)(a, b) = (1_Aa, 1_Bb) = (a, b)$. Also $(a, b)(1_A, 1_B) = (a1_A, b1_B) = (a, b)$.

Ad 4. Zero in $A \times B$ is $(0_A, 0_B) \in A \times B$, such that $0_A + a = a + A_0 = a$ and $0_B + b = b + B_0 = b$, for all $a \in A$ and $b \in B$. Thus, let us observe $(a_1, b_1)(a_2, b_2) = (0_A, 0_B)$. Assume $(a_1, b_1) \neq (0_A, 0_B)$ and $(a_2, b_2) \neq (0_A, 0_B)$. Then, $(a_1a_2, b_1b_2) = (0_A, 0_B)$ which implies $a_1a_2 = 0_A$ and $b_1b_2 = 0_B$. As A and B are not integral domains, then $a_1a_2 = 0_A$ and $b_1b_2 = 0_B$ implies $a_1 \neq 0_A$ and $a_2 \neq 0_A$; similarly $b_1 \neq 0_B$ and $b_2 \neq 0_B$. Therefore, $(a_1, b_1)(a_2, b_2) = (0_A, 0_B)$ implies $(a_1, b_1) \neq (0_A, 0_B)$ and $(a_2, b_2) \neq (0_A, 0_B)$. Also, as there are non-invertible elements in A and B, say $a \in A$ and $b \in B$, then, $(a, b) \in A \times B$ is also not invertible.

□

Proposition. Let A be a ring and $a, b, c \in A$. Then:

1. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.
2. If $ab = -ba$, then $(a + b)^2 = (a - b)^2 = a^2 + b^2$.

Proof. *Ad* 1. As $a - b = a + (-b)$, we have $a(b - c) = a(b + (-c))$. By distributive law, from A is a ring, we have $a(b + (-c)) = ab + a(-c)$. From a previous proposition, $a(-c) = -ac$, we have $ab + a(-c) = ab - ac$. Similarly, we can prove that $(b - c)a = (b + (-c))a = ba + (-c)a = ba - ca$.

Ad 2. Assume $ab = -ba$. Then, $(a + b)^2 = (a + b)(a + b)$. By distributive law, $(a + b)(a + b) = (a + b)a + (a + b)b$. Again, by distributive law, $(a + b)a + (a + b)b = a^2 + ba + ab + b^2$. But, as $ab = -ba$, we have $a^2 + ba + ab + b^2 = a^2 + ba + (-ba) + b^2 = a^2 + 0 + b^2 = a^2 + b^2$.

□

Proposition. Let A be a commutative ring. Then $a^2 - b^2 = (a - b)(a + b)$.

Proof. By using distributivity, $(a - b)(a + b) = (a - b)a + (a - b)b = a^2 - ba + ab - b^2$. As A is commutative, $ba = ab$, so $a^2 - ba + ab - b^2 = a^2 - ab + ab - b^2 = a^2 - b^2$.

□

Proposition. Let A be a ring with unity. Then $a^2 - 1 = (a + 1)(a - 1)$.

Proof. We have $a^2 - 1 = a^2 + 0 - 1 = a^2 - a + a - 1 = aa - a1 + 1a - 11$. By using distributive law, $a^2 - 1 = a(a - 1) + 1(a - 1)$. Using the distributive law again, we get $a^2 - 1 = (a + 1)(a - 1)$.

□

Remark. If $a = b$ or $a = -b$ we will write $a = \pm b$.

Proposition. Let A be an integral domain and $a, b \in A$. Then,

1. $a^2 = b^2$ implies $a = \pm b$.
2. $a^n = 0$, for some $n \in \mathbb{Z}^+$, implies $a = 0$.

Proof. *Ad* 1. Let $a, b \in A$. We have $a^2 = b^2$, that is $a^2 - b^2 = 0$. From a previous proposition, as every integral domain is a commutative ring, $a^2 - b^2 = (a - b)(a + b) = 0$. As integral domain has no divisors of zero, $(a - b)(a + b) = 0$ implies $a - b = 0$ or $a + b = 0$. From first equation we get $a = b$, and from the second one, $a = -b$. Therefore, $a = b$ or $a = -b$, i.e. $a = \pm b$.

Ad 2. Let $a \in A$, $n \in \mathbb{Z}^+$ and $a^n = 0$. First, we will prove proposition for $n = 1$. We have $a^1 = 0$. Then, as $a^1 = a$ we get $a = 0$. Assume $a^n = 0$ implies $a = 0$, for some $n \in \mathbb{N}$. As $a^{n+1} = 0$ is equivalent to $aa^n = 0$ and, as A is an integral domain either $a = 0$ or $a^n = 0$. If $a = 0$ we are done. If $a^n = 0$, then, by assumption $a = 0$ and we are done.

□

Remark. Note that, if A is an integral domain, if $x \in A$ is its own multiplicative inverse, i.e. $x^2 = 1$, then it follows, from a previous proposition, that $x = \pm 1$.

Proposition. Let $(A, +)$ be a group and $(A, \cdot)$ a monoid such that $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$, for all $a, b, c \in A$. Then, $a + b = b + a$, for all $a, b \in A$.

Proof. We have $(a + b)(1 + 1) = (a + b)(1 + 1)$. Using the distributive law we get $(a+b)1+(a+b)1 = a(1+1)+b(1+1)$. That is, $(a+b)+(a+b) = a+a+b+b$. We apply $-(a+b)$ on the right and get $a+b = a+a+b+b-(a+b)$. But, $-(a+b) = -b+(-a)$, therefore $a+b = a+a+b+b+(-b)+(-a)$. That is equivalent to $a+b = a+a+b+(-a)$. We apply a on the right and get $a + b + a = a + a + b$. Finally, we apply $(-a)$ on the left and obtain $(-a) + a + b + a = (-a) + a + a + b$, i.e. $b + a = a + b$.

□

Proposition. Let A be a non-trivial ring with unity and $a, b \in A$. Then:

1. If $a^2 = 0$ then $a + 1$ and $a - 1$ are invertible.
2. If a and b are invertible, their product ab is invertible. The converse holds if A is commutative.

Proof. *Ad* 1. Let $a^2 = 0$. After some thinking (done on author's part), we have $(-a+1)(a+1) = (-a+1)a + (-a+1)1 = -a^2 + a - a + 1 = -0 + 0 + 1 = 1$. Also, $(a+1)(-a+1) = -a^2 - a + a + 1 = 1$. Therefore, $(a+1)^{-1} = (-a+1)$. Similarly, $(-a-1)(a-1) = (-a-1)a + (-a-1)(-1) = -a^2 - a + a + 1 = -0 + 0 + 1 = 1$. Similarly $(a-1)(-a-1) = (a-1)(-a) + (a-1)(-1) = a^2 + a - a + 1 = 0 + 0 + 1 = 1$.

Ad 2. Let a and b be invertible, i.e. there exist $a^{-1}, b^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$ and $bb^{-1} = b^{-1}b = 1$. Then, as $ab = ab$ and b is invertible, we can multiply equality with b^{-1} on the right to obtain $abb^{-1} = a$. Finally, multiplying by a^{-1} on the right gives us $abb^{-1}a^{-1} = 1$. That can be grouped as $(ab)(b^{-1}a^{-1}) = 1$. Therefore, $(ab)^{-1} = b^{-1}a^{-1}$. To prove the converse, assume A is commutative and there exists $(ab)^{-1} \in A$ such that $(ab)(ab)^{-1} = (ab)^{-1}(ab) = 1$. Then, $ab = ab$ implies, after multiplying by $(ab)^{-1}$ on the right and using associativity, $(ab)(ab)^{-1} = a(b(ab)^{-1})$. That is, $1 = a(b(ab)^{-1})$. As A is commutative, also $(b(ab)^{-1})a = 1$. Therefore, $a^{-1} = b(ab)^{-1}$. Similarly, we can show that $(ab)^{-1}(ab) = ((ab)^{-1}a)b$ implies $1 = ((ab)^{-1}a)b$. As A is commutative, then $b((ab)^{-1}a) = 1$ and $b^{-1} = (ab)^{-1}a$.

□

Proposition. Let $(A, +, \cdot)$ be a non-trivial ring with unity and

$$A^* = \left\{ a \in A : \ \left(\exists a^{-1} \in A\right) \left(aa^{-1} = a^{-1}a = 1\right) \right\}.$$

Then, $(A^*, \cdot)$ is a group.

Proof. As $1 \in A$ and $1 \cdot 1 = 1 \cdot 1 = 1$, then $1 \in A^*$, therefore, A^* has a neutral element and is non-empty. Also, due to $(A, \cdot)$ being associative (from A is a ring), then A^* is also associative (because $A^* \subseteq A$). By definition, every $a \in A^*$ has an inverse and from that we conclude that $(A^*, \cdot)$ is a group.

□

Remark. Assume $0 \in A^*$. Then, there exists $a^{-1} \in A$ such that $0a^{-1} = a^{-1}0 = 1$. As $0a^{-1} = 0$ and also $a^{-1}0 = 0$, then we get $0 = 1$, which is true only in a trivial ring.

Therefore $0 \notin A^*$. Furthermore, if A is a field, then all elements are invertible (except obviously zero). So, $A^* = A - \{0\}$.

Proposition. Let F be a finite field and $|F| = m$, for some $m \in \mathbb{N} - \{1\}$. Then, $x^{m-1} = 1$, for every $x \neq 0$.

Proof. As F is a field, then $F - \{0\}$ with multiplication is an Abelian group, by definition. But, as $|F| = m$, then $|F - \{0\}| = m - 1$. As $F - \{0\}$ is an Abelian group, then by a result from group theore, $x^{|F|} = 1$, for all $x \in F - \{0\}$. That implies $x^{m-1} = 1$, for all $x \in F - \{0\}$.

□

Proposition. Let A be a non-trivial ring. If $(A, +)$ is cyclic, then A is a commutative ring.

Proof. Let $(A, +)$ be cyclic, i.e. if $x \in A$, then $x = \underbrace{a + a + \cdots + a}_{n \text{ times}}$ (then, e.g. $-x = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ times}}$, just to remind ourselves of the difference in notation in group theory) , for some generator $a \in A$. Then, we can write $x = ma$ (remember that this is the same as a^m in group theory, but only in additive notation), where $m \in \mathbb{Z}$. Then, if we take $y \in A$, we have $y = na$, for some $n \in \mathbb{Z}$. Then, $xy = (ma)(na) = \left(\underbrace{a + \cdots + a}_{m \text{ times}}\right)\left(\underbrace{a + \cdots + a}_{n \text{ times}}\right)$. Now, when using distributive law, there will be mn elements of the form a^2, so, $xy = (mn)a^2 = (nm)a^2$. Following the same reasoning, obviously $(na)(ma) = \left(\underbrace{a + \cdots + a}_{n \text{ times}}\right)\left(\underbrace{a + \cdots + a}_{m \text{ times}}\right) = (nm)a^2$. Therefore, $xy = (nm)a^2 = (na)(ma) = yx$.

□

Problem. Let A be a non-trivial ring and $a, b \in A$. Then,

1. If $a \neq \pm 1$ and $a^2 = 1$, then $a + 1$ and $a - 1$ are divisors of zero;
2. If ab is a divisor of zero, then a or b is a divisor of zero;
3. In a commutative ring with unity, a divisor of zero cannot be invertible;
4. Suppose $ab \neq 0$ in a commutative ring. If either a or b is a divisor of zero, so is ab;
5. Suppose $a \neq 0$ nor a divisor of zero. If $ab = ac$, then $b = c$;

6. If A and B are rings, $A \times B$ always has divisors of zero.

Solution.

1. *If $a \neq \pm 1$ and $a^2 = 1$, then $a+1$ and $a-1$ are divisors of zero.* Let $a^2 = 1$ and $a \neq \pm 1$. From that we have $a^2 - 1 = 1 - 1$, i.e. $a^2 - 1 = 0$. From that we have $a^2 - a + a - 1 = 0$. By using distributive law, $a(a-1) + 1(a-1) = 0$. Then, using the distributive law again, $(a+1)(a-1) = 0$. As $a \neq 1$ and $a \neq 1$, we have that $a + 1 \neq 0$ and $a - 1 \neq 0$. From that, and $(a+1)(a-1) = 0$, it follows that $a + 1$ and $a - 1$ are divisors of zero.

2. *If ab is a divisor of zero, then a or b is a divisor of zero.* It must be that $ab \neq 0$. Also, we have that there exists $c \neq 0$ such that $(ab)c = 0$. As $ab \neq 0$, then $a \neq 0$ and $b \neq 0$. As $c \neq 0$, then $bc \neq 0$. From that we have, using associative law, $a(bc) = 0$, but $a \neq 0$ and $bc \neq 0$. Therefore, a is a divisor of zero. If it were that $c(ab) = 0$, then $(ca)b = 0$ would in the same manner imply that b is a divisor of zero. Therefore, a or b is a divisor of zero.

3. *In a commutative ring with unity, a divisor of zero cannot be invertible.* Assume $a \in A$, $a \neq 0$, is an invertible divisor of zero and A is commutative ring with unity. Then, there exists $b \in A$, $b \neq 0$, such that $ab = 0$ (or, equivalently as A is commutative, $ba = 0$). As a is invertible, there exists $a^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$. If we multiply $ab = 0$ with a^{-1} on the left, we would get $a^{-1}ab = a^{-1}0$, that is, $b = 0$, which is a contradiction with $b \neq 0$.

4. *Suppose $ab \neq 0$ in a commutative ring. If either a or b is a divisor of zero, so is ab.* Assume $ab \neq 0$. Assume a is a divisor of zero, without loss of generality (proof for b goes the same way). Then, $a \neq 0$ and there exists $c \in A$, $c \neq 0$, such that $ac = 0$. If we multiply that equality by b we would get $acb = 0b$, i.e. $(ab)c = 0$, as A is commutative. Then, as $(ab)c = 0$ and $(ab) \neq 0$ and $c \neq 0$, it follows that (ab) is a divisor of zero.

5. *Suppose a is neither 0 nor a divisor of zero. If $ab = ac$, then $b = c$.* We have that $ab = ac$ implies $ab - ac = 0$. By distributive law that is equivalent to $a(b-c) = 0$. As a is not a divisor of zero, then either $a = 0$ or $b - c = 0$. But, as $a \neq 0$ by assumption, then it must be that $b - c = 0$. That implies $b = c$.

6. *If A and B are non-trivial rings, $A \times B$ always has divisors of zero.* As A and B are non-trivial rings, we have that there exist $a \in A$ and $b \in B$ such that $a \neq 0$ and $b \neq 0$. Also, as $0_A \in A$ and $0_B \in B$, there exist $(a, 0_B), (0_A, b) \in A \times B$. Then, $(a, 0_B) \neq (0_A, 0_B)$ and $(0_A, b) \neq (0_A, 0_B)$, i.e. they are both non-zero. But, $(a, 0_B)(0_A, b) = (a0_A, 0_B b) = (0_A, 0_B)$, that is, their product is zero, making $(a, 0_B)$ and $(0_A, b)$ divisors of zero.

Definition. If A is a ring and $a^2 = a$ for every $a \in A$, then, we say that A is a **boolean ring**.

Proposition. Every boolean ring A is a commutative ring with no invertible elements except $1 \in A$.

Proof. Let $a, b \in A$. We have $(a+a)^2 = (a+a)(a+a) = (a+a)a + (a+a)a = a^2 + a^2 + a^2 + a^2$. But, $(a+a)^2 = a+a$ and $a^2 = a$, so $a+a+a+a = a+a$ from which we get $a+a = 0$, i.e. $a = -a$. Then, from $(a+b)^2 = a+b$ we get $(a+b)(a+b) = a+b$, i.e. $(a+b)a + (a+b)b = a+b$. By applying distributive law, $a^2 + ba + ab + b^2 = a+b$. Here we use the fact that $a^2 = a$ and $b^2 = b$. So we have $a + ba + ab + b = a + b$. Applying $-b$ on the right and $-a$ on the left gives us $ba + ab = 0$, i.e. $ba = -ab$. That is equivalent to $ba = (-a)b$. As $-a = a$, we have $ba = ab$.

Let $a \in A$, $a \neq 0$. Assume there exists $1 \in A$ such that $a1 = 1a = a$. Then, as $a^2 = a$, we have $a^2 - a = 0$, i.e. $aa - a1 = 0$. From that we get $a(a-1) = 0$. If a is not a divisor of zero, then $a = 0$ or $a - 1 = 0$. But that implies that either a is a divisor of zero, or a is 0 or 1. Therefore, all elements in A are divisors of zero, except 0 and 1. Note that 1 cannot be a divisor of zero as it would imply that there exists $x \in A$ such that $1x = 0$. But, $1x = x$, so $x = 0$, meaning that the ring is trivial. As all elements but 0 and 1 are divisors of zero, only $1 \in A$ (unity) is invertible.

□

Proposition. Let A be a boolean ring and $a \vee b = a + b + ab$. Then,

1. $a \vee bc = (a \vee b)(a \vee c)$.
2. $a \vee (1 + a) = 1$.
3. $a \vee a = a$.
4. $a(a \vee b) = a$.

Proof. *Ad* 1. $(a \vee b)(a \vee c) = (a+b+ab)(a+c+ac) = (a+b+ab)a + (a+b+ab)(c+ac) = a^2 + ba + a^2b + ac + bc + abc + a^2c + abc + a^2bc$. We use the fact that $a^2 = a = -a$, so $(a \vee b)(a \vee c) = a + ab - ab + ac + bc + abc - ac + abc - abc = a + bc + abc = a \vee bc$. *Ad* 2. $a \vee (1 + a) = a + (1 + a) + a(1 + a) = a + 1 - a + a + a^2 = 1 + a - a = 1$. *Ad* 3. $a \vee a = a + a + a^2 = a - a + a = a$. *Ad* 4. $a(a \vee b) = a(a + b + ab) = a^2 + ab + a^2b = a + ab - ab = a$.

□

Remark. Let us remind ourselves that if $(A, +)$ is a group, $a \in A$ and $n \in \mathbb{N}$, then $na = \underbrace{a \oplus a \oplus \cdots \oplus a}_{n \text{ times}}$, $(-n)a = \underbrace{(-a) \oplus (-a) \oplus \cdots \oplus (-a)}_{n \text{ times}}$, $0a = 0_A$, where $0_A \in A$ is zero.

Proposition. Let $(A, \oplus, \odot)$ be a ring[66], $a \in A$ and $n, m \in \mathbb{Z}$. Then,

1. $n(ma) = (nm)a$
2. $n(-a) = (-n)a = -na$.
3. $na \oplus ma = (n + m)a$.
4. $-n(-a) = -(-n)a = na$.
5. $1a = a$.
6. $(ma) \odot (nb) = (mn)(a \odot b)$.

Proof. The results for 1, 2, 3 and 4 are obvious if we denote na as a^n and use result from group theory that $n(ma)$ is actually $(a^n)^m = a^(nm)$. Then, it is easy to see that 2 and 3 and 4 are also true. *Ad* 5. Trivial, from $a^1 = a$. *Ad* 6. Let $n = 1$ and $m = 1$. Then $(1a) \odot (1b) = a \odot b$. Assume that is true for all m. Then, $((m + 1)a) \odot (1b) = (ma \oplus 1a) \odot (1b) = (ma) \odot (1b) \oplus (1a) \odot (1b)$. By assumption, $(ma) \odot (1b) \oplus (1a) \odot (1b) = m(a \odot b) \oplus (a \odot b) = (m+1)(a \odot b)$. Assume that statement is true for m and n. Then if we take $n+1$, we have $(ma) \odot ((n+1)b) = (ma) \odot (nb \oplus 1b) = (ma) \odot (nb \oplus 1b)$. From distributive law, $(ma) \odot (nb \oplus 1b) = (ma) \odot (nb) \oplus (ma) \odot (1b)$. By using assumption , we have $(ma) \odot (nb) \oplus (ma)(1b) = (mn)(a \odot b) \oplus (m1)(a \odot b) = (mn + m)(a \odot b) = (m(n + 1))(a \odot b)$. Similarly we can prove for $m + 1$.

□

Remark. What observations above really tell us is that we can deal with operations in ring as with multiplication and addition in elementary algebra (algebraic expressions), without using special symbols for addition and multiplication in a ring.

Remark. From now on, we will use following notation for a sum:

$$\sum_{i=k}^{n} f(i) = f(k) + f(k + 1) + \cdots + f(n - 1) + f(n),$$

where $n \in \mathbb{N}$, $k \in \mathbb{Z}$, $k \leq n$ and $f(i)$ is some expression involving i, e.g. $f(i) = a^i$, $f(i) = (i - 1)a + 2i$, etc.

[66] Note that $1 \in \mathbb{Z}$ in statement 5 is not unity $1_A \in A$.

Proposition. Let $n \in \mathbb{N}$, $k \in \mathbb{Z}$, $k \leq n$ and $j \in \mathbb{Z}$. Then,

$$\sum_{i=k}^{n} f(i) = \sum_{i=k+j}^{n+j} f(i-j).$$

Proof. We have:

$$\begin{aligned} \sum_{i=k+j}^{n+j} f(i-j) &= f((k+j)-j) + \cdots + f((n+j)-j) \\ &= f(k) + \cdots + f(n) = \sum_{i=k}^{n} f(i). \end{aligned}$$

□

Proposition. Let $n \in \mathbb{N}$, $k \in \mathbb{Z}$, $k \leq n$ and $j \in \mathbb{Z}$ such that $k < j \leq n$. Then,

$$\sum_{i=k}^{n} f(i) = \sum_{i=k}^{j-1} f(i) + \sum_{i=j}^{n} f(i).$$

Proof. By definition:

$$\begin{aligned} \sum_{i=k}^{j-1} f(i) + \sum_{i=j}^{n} f(i) &= f(k) + \cdots + f(j-1) \\ &+ f(j) + \cdots + f(n) = \sum_{i=k}^{n} f(i). \end{aligned}$$

□

Proposition. Let A be a commutative ring and $n \in \mathbb{N}$. Then, for all $a, b \in A$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Proof. Assume $n = 1$. Then,

$$(a+b)^1 = a + b = \binom{1}{0} a^{1-0} b^0 + \binom{1}{1} a^{1-1} b^1 = \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k.$$

Assume that the formula is true for some $n \in \mathbb{N}$. Then we will prove it is true for $n+1$. We have

$$(a+b)^{n+1} = (a+b)^n(a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k\right)(a+b).$$

By distributive law,

$$\left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k\right)a + \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k\right)b = \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k+1}.$$

Now, we can clarify that by adjusting indices:

$$\sum_{k=0}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k+1} = \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-k+1}b^k.$$

We set the first sum as:

$$\begin{aligned} & \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-k+1}b^k \\ = \; & \binom{n}{0} a^{n+1} + \sum_{k=1}^{n+1} \binom{n}{k} a^{n-k+1}b^k - \binom{n}{n+1} b^{n+1} + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-k+1}b^k. \end{aligned}$$

Using the fact that[67]

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k},$$

and that

$$\binom{n}{n+1} = 0,$$

we have:

$$\begin{aligned} & \binom{n}{0} a^{n+1} + \sum_{k=1}^{n+1} \binom{n}{k} a^{n-k+1}b^k - \binom{n}{n+1} b^{n+1} + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-k+1}b^k \\ = \; & \binom{n+1}{0} a^{n+1-0}b^0 + \sum_{k=1}^{n+1} \binom{n+1}{k} a^{(n+1)-k}b^k \\ = \; & \sum_{k=0}^{n+1} \binom{n+1}{k} a^{(n+1)-k}b^k. \end{aligned}$$

[67] I won't bother to prove it here, for now.

□

Definition. Let A be a ring and $a \in A$. We say that a is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{N}$. We say that a is **unipotent** if $1 - a$ is nilpotent.

Proposition. Let A be a ring with unity, $a \in A$ and $n \in \mathbb{N}$. Then,

1. $1 - a^n = (1 - a)(1 + a + a^2 + \cdots + a^{n-1}) = (1 + a + a^2 + \cdots + a^{n-1})(1 - a)$.
2. $a^n + 1 = (1 + a)(1 - a + a^2 + \cdots + (-1)^{n-1}a^{n-1})$, for odd n.
3. $1 - a^{2n} = (1 - a^n)(1 + a^n)$.

Proof. *Ad* 1. Let $n = 1$. Then, $1 - a^1 = 1 - a = (1 - a)1 = (1 - a)a^0 = (1 - a)(a^{1-1})$. Assume statement is true for n. Then, $1-a^{n+1} = 1-1a+1a-a^na = (1-a)+(1-a^n)a$. From that we have $(1 - a) + (1 - a^n)a = (1 - a) + (1 - a)(1 + a + \cdots + a^{n-1})a = (1 - a)1 + (1 - a)(a + a^2 + \cdots + a^n) = (1 + a)(1 + a + a^2 + \cdots + a^n)$. Similarly we can prove the second case.

Ad 2. We can see that $(1 + a)(1 - a + a^2 + \cdots + (-1)^{n-1}a^{n-1}) = 1 - a + a^2 + \cdots + (-1)^{n-1}a^{n-1} + a - a^2 + \cdots + (-1)^{n-1}a^n - a + a^2 + \cdots + (-1)^n(-1)^{n-1}a^n$. All elements cancel out except 1 and $(-1)^{n-1}a^n$. As n is odd, $n - 1$ is even, so we have only $1 + a^n$.

Ad 3. We have $(1-a^n)(1+a^n) = (1-a^n)1+(1-a^n)a^n = 1-a^n+a^2-a^{2n} = 1-a^{2n}$.

□

Proposition. Let A be a ring with unity. If a is nilpotent, then $a + 1$ and $a - 1$ are both invertible.

Proof. As a is nilpotent, then $a^n = 0$. Therefore, $1 - a^n = 1$. From the previous proposition that is equivalent to $(1-a)(1+a+\cdots+a^{n-1}) = (1+a+\cdots+a^{n-1})(1-a) = 1$. Using the fact that $(1 - a) = -(a - 1)$, we have $(a - 1)(-(1 + a + \cdots + a^{n-1})) = (-(1 + a + \cdots + a^{n-1}))(a - 1) = 1$. Thus, $(a - 1)^{-1} = -(1 + a + \cdots + a^{n-1})$.

From the previous proposition, for odd n, and from $a^n = 0$, we have $a^n + 1 = 1$. Then, $a^n+1 = (1+a)(1-a+a^2+\cdots+(-1)^{n-1}a^{n-1}) = (1-a+a^2+\cdots+(-1)^{n-1}a^{n-1})(1+a) = 1$, so $(a + 1)^{-1} = (1 - a + a^2 + \cdots + (-1)^{n-1}a^{n-1})$. If n is even, then, $a^{2k} = 0$. That is equivalent to $-a^{2k} = 0$ and $1 - a^{2k} = 1$. From the previous proposition, $(1 - a^{2k}) = (1 - a^k)(1 + a^k)$. If k is odd, then $(1 + a^k)$ can be factored to give $(1 + a)$, as in previous case. If k is even, then we can break it again into $(1 - a^{\frac{k}{2}})(1 - a^{\frac{k}{2}})$, until we get that k is odd. So, we get $1 = (a + 1)f(a) = f(a)(a + 1)$ (due to distributive law), where $f(a)$ is some expression dependant on a. Therefore, $a + 1$ and $a - 1$ are invertible.

□

Proposition. Let A be a commutative ring. Then:

1. Any product xa of a nilpotent element $a \in A$ by any element $x \in A$ is nilpotent.
2. Let $a^n = 0$, for some $n \in \mathbb{N}$. Then, let $m \in \mathbb{N}$ such that $m \geq n$. Then, $a^m = 0$.
3. Sum of two nilpotent elements is nilpotent.

Proof. *Ad* 1. Let $x, a \in A$ and $a^n = 0$, for some $n \in \mathbb{N}$. Then, as A is commutative, $(xa)^n = x^n a^n = x^n 0 = 0$. Therefore, xa is nilpotent.

Ad 2. As $a^n = 0$, then $a^m = a^{n+(m-n)}$. As $m \geq n$, then $m - n \in \mathbb{N}$ and we have $a^m = a^n a^{m-n} = 0a^{m-n} = 0$.

Ad 3. Let $a, b \in A$, where $a^m = 0$ and $b^n = 0$, for some $m, n \in \mathbb{N}$. Then,

$$\begin{aligned}(a+b)^{n+m} &= \sum_{k=0}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k \\ &= \sum_{k=0}^{n} \binom{n+m}{k} a^{n+m-k} b^k + \sum_{k=n+1}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k.\end{aligned}$$

In the first sum, $k \leq n$, meaning $n - k \in \mathbb{N}$. Similarly, in the second sum $k \geq n+1$, i.e. $k - (n+1) \in \mathbb{N}$. Let us denote $n - k = x$ and $k - (n+1) = y$. Then the sum above becomes:

$$\begin{aligned}&\sum_{k=0}^{n} \binom{n+m}{k} a^{m+x} b^k + \sum_{k=n+1}^{n+m} \binom{n+m}{k} a^{n+m-k} b^{y+(n+1)} \\ = &\sum_{k=0}^{n} \binom{n+m}{k} a^m a^x b^k + \sum_{k=n+1}^{n+m} \binom{n+m}{k} a^{n+m-k} b^n b^{y+1}.\end{aligned}$$

The first sum contains $a^m = 0$ and the second sum contains $b^n = 0$. Therefore all two sums equal zero, so $(a+b)^{m+n} = 0 + 0 = 0$ and $a + b$ is nilpotent, as $m + n \in \mathbb{N}$.

□

Proposition. Let A be a commutative ring with unity and $a, b \in A$ such that a and b are unipotent. Then, ab is unipotent.

Proof. As a and b are unipotent, then $1 - a$ and $1 - b$ are nilpotent, i.e. there exist $m, n \in \mathbb{N}$ such that $(1-a)^m = 0$ and $(1-b)^n = 0$. We need to show that $1 - ab$ is nilpotent (as then ab will be unipotent). We have that $1-ab = 1-ab = 1-a+a-ab = (1-a)+a(1-b)$. As $1-b$ is nilpotent, by previous proposition, $a(1-b)$ is also nilpotent. As $(1-a)$ and $a(1-b)$ are nilpotent, then their sum is also nilpotent. Therefore, $1-ab$ is nilpotent and ab is unipotent.

□

Proposition. Let A be a ring with unity. Then, if $a \in A$ is unipotent, it is invertible.

Proof. Let $a \in A$ be unipotent. Then, $1 - a$ is nilpotent. By first proposition, $1 - a - 1 = -a$ is invertible, i.e. there exists $a^{-1} \in A$ such that $(-a)a^{-1} = 1$. But, then $a(-a^{-1}) = (-a^{-1})a = 1$ and a is also invertible.

□

Definition. If A is a ring with unity, we define the set:

$$A^* = \{a \in A : \ (\exists a^{-1} \in A)(aa^{-1} = a^{-1}a = 1)\},$$

with multiplication from A as a respective operation.

Proposition. Let A be a ring with unity. Then, A^* is a group. If A is commutative then A^* is Abelian.

Proof. First, obviously $1 \in A^*$ and $A^* \subseteq A$ so A^* inherits associativity (and commutativity). If $a, b \in A^*$ then there exist $a^{-1}, b^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$ and $bb^{-1} = b^{-1}b = 1$. But, then also $a^{-1}, b^{-1} \in A^*$, so each element has its inverse. Now we only need to check whether A^* is closed with respect to multiplication. In A, we have $(ab)(b^{-1}a^{-1}) = aa^{-1} = 1$. Also, $(b^{-1}a^{-1})(ab) = b^{-1}b = 1$. From that we have that $(b^{-1}a^{-1}) = (ab)^{-1}$, therefore $(ab) \in A$ has its inverse $(ab)^{-1} = b^{-1}a^{-1} \in A$. Then it must be that $ab \in A^*$. Therefore A^* is a group (Abelian if A is commutative, which is inherited by subset relation).

□

Remark. This can, of course, be done in group theory for monoids. That is, if M is a (commutative) monoid, then the set

$$M^* = \{m \in M : \ (\exists m^{-1} \in M)(mm^{-1} = m^{-1}m = 1)\}.$$

is a (commutative) group. The proof is exactly the same as above.

Proposition. Let A and B be commutative rings with unity. If $A \cong B$, then $A^* \cong B^*$.

Proof. As $A \cong B$, then there exists an isomorphism $f : A \to B$. Then we can take restriction $g : A^* \to B^*$ with $g(x) = f(x)$. We will show that g is a bijection. As

f is well-defined then so is g. Then, $g(a) = g(b)$ is equivalent to $f(a) = f(b)$. But, as f is an injection, then $a = b$, so g is an injection. Now, if we take $y \in B^*$, we need to find $x \in A^*$ such that $g(x) = y$. But, as f is surjective, for each $y \in B^{ast}$ there exists $x \in A^*$ such that $f(x) = y$, i.e. $g(x) = y$. So, g is bijective. Now, $g(ab) = f(ab) = f(a)f(b) = g(a)g(b)$, so g is an isomorphism from A^* to B^*.

□

Proposition. Let A and B be commutative rings with unity. Then,

$$A^* \times B^* = (A \times B)^* .$$

Let $(a, b) \in A^* \times B^*$. Then $a \in A^*$ and $b \in B^*$, so there exist $a^{-1} \in A^*$ and $b^{-1} \in B^*$ such that $aa^{-1} = a^{-1}a = 1$ and $bb^{-1} = b^{-1}b = 1$. Then, $(a^{-1}, b^{-1}) \in A^* \times B^*$. We have $(a, b)(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (1, 1) = (a^{-1}a, b^{-1}b) = (a^{-1}, b^{-1})(a, b) = (1, 1)$, so $(a^{-1}, b^{-1}) = (a, b)^{-1}$, i.e. (a, b) has an inverse $(a, b)^{-1}$, and as $(a, b) \in A \times B$, then also $(a, b) \in (A \times B)^*$ and we have $A^* \times B^* \subseteq (A \times B)^*$. Now, let $(a, b) \in (A \times B)^*$. Then there exists $(a, b)^{-1}$ such that $(a, b)(a, b)^{-1} = (a, b)^{-1}(a, b) = (1, 1)$. But, as $(a, b)^{-1} \in (A \times B)^*$, then $(a, b)^{-1} = (c, d)$, where $(c, d) \in (A \times B)^*$. So, $(a, b)(c, d) = (c, d)(a, b) = (1, 1)$. From definition of direct product we have $(ac, bd) = (ca, db) = (1, 1)$. From definition of ordered pair that is equivalent to $ac = ca = 1$ and $bd = db = 1$, meaning $c = a^{-1}$ and $d = b^{-1}$, so $a \in A^{ast}$ and $b \in B^*$. In other words, $(a, b) \in A^* \times B^*$.

□

Ideals and homomorphisms

Definition. Let A be a ring and $B \subseteq A$ with $B \neq \emptyset$. Then, if B is closed with respect to addition, multiplication and negatives, we say that B is a **subring** of A and write $B \leq A$.

Proposition. Let A be a ring and $B \leq A$, $B \neq \emptyset$. Then, B is a ring.

Proof. As $B \subseteq A$, we have that B, with addition, is a subgroup of A (as it is closed with respect to addition and negatives). Therefore, A with addition is a group. Distributive laws hold for all elements in A and so they hold for all elements in $B \subseteq A$. As B is closed with respect to multiplication and as A is associative (for multiplication), then B is also associative (for multiplication). Therefore, B is a ring.

□

Proposition. Let A be a ring and $B \subseteq A$. Then, B is closed with respect to subtraction if and only if it is closed with respect to addition and negatives.

Proof. *Necessity.* Let B be closed with respect to subtraction. Let $a \in B$. Then, for all $b \in B$, we have $b - a \in B$. But, $b - a = b + (-a) \in B$. That also implies that $a + (-a) \in B$. As $a + (-a) = 0 \in A$, then $0 \in B$. That implies that for all $a \in B$, we have $0 - a = 0 + (-a) = -a \in B$. Therefore, B is closed with respect to negatives. Then, as $-a \in B$, for all $a \in B$, we have $a - (-b) = a + (-(-b)) = a + b \in B$, for all $b \in B$. So, B is closed with respect to addition. *Sufficiency.* Let B be closed with respect to addition and negatives. Then, $a + b \in B$ for all $a, b \in B$ and $-a \in B$ for all $a \in B$. Let $a, b \in B$. Then $-b \in B$. We have $a + (-b) = a - b \in B$. So, B is closed with respect to subtraction.

□

Definition. Let A be a ring and $B \subseteq A$. We say that B **absorbs products** in A if $ab \in B$ and $ba \in B$ for all $a \in A$ and $b \in B$. We say that $B \subseteq A$ is an **ideal** of A if B is closed with respect to addition and negatives[68] and if B absorbs products in A. Then, we write $B \trianglelefteq A$.

Proposition. Let A be a ring and $B \trianglelefteq A$. Then, $B \leq A$.

Proof. By definition, B is closed with respect to addition and negatives. Now, if $a, b \in B$, then also $b \in A$. So, $ab \in B$. Same thing for $ba \in B$. Thus, $B \leq A$.

[68] Or simply subtraction due to previous proposition.

□

Definition. Let A be a commutative ring, $a \in A$ and $\langle a \rangle = \{xa : \ x \in A\}$. We say that $\langle a \rangle$ is a **principal ideal generated by** a.

Proposition. Let A be a commutative ring and $a \in A$. Then, $\langle a \rangle \trianglelefteq A$.

Proof. We must show that $\langle a \rangle$ is closed with respect to subtraction and that it absorbs products in A. Let $xa, ya \in \langle a \rangle$. Then, by distributive law, $xa + ya = (x+y)a$. Now, as $x + y \in A$, then $(x + y)a \in \langle a \rangle$ and also $xa + ya \in \langle a \rangle$. If $xa \in \langle a \rangle$, then $-xa = (-x)a$. As $(-x) \in A$, then $(-x)a \in \langle a \rangle$ and $-xa \in \langle a \rangle$. If $xa \in \langle a \rangle$ and $b \in A$, then $b(xa) = (bx)a$, due to associativity. As $bx \in A$, then $(bx)a \in \langle a \rangle$, where we have $b(xa) \in \langle a \rangle$. Also, as A is commutative, $(xa)b = b(xa)$. As $(xa)b \in \langle a \rangle$, then also $b(xa) \in \langle a \rangle$. Therefore, $\langle a \rangle \trianglelefteq A$.

□

Definition. A **homomorphism** from ring A to a ring B is a function $f : A \to B$ such that for all $x_1, x_2 \in A$:

$$\begin{aligned} f(x_1 + x_2) &= f(x_1) + f(x_2), \\ f(x_1 x_2) &= f(x_1) f(x_2). \end{aligned}$$

Definition. Let $f : A \to B$ be a homomorphism from A to B. Then, **kernel** of f is $\ker(f) = \{x \in A : \ f(x) = 0\}$.

Definition. We say that a bijective homomorphism from A to B is an **isomorphism** from A to B and we write $A \cong B$.

Proposition. Let $f : A \to B$ be a homomorphism from A to B. Then, $\ker(f) \trianglelefteq A$.

Proof. Let $x, y \in \ker(f)$. Then, $f(x) = f(y) = 0$. Let $x + y = s$ for some $s \in A$. But, then, $f(x+y) = f(s)$ and, as f is a homomorphism, $f(x) + f(y) = f(s)$. But, as $x, y \in \ker(f)$, we have $f(x) + f(y) = 0 + 0 = f(s)$, i.e. $f(s) = 0$, so $s \in \ker(f)$. That means $x + y \in \ker(f)$. Let $x \in \ker(f)$. Then, $f(x) = 0$ implies $f(x) + (-f(x)) = 0 + (-f(x))$. From that we have $0 = -f(x)$. A result from group theory gives us $-f(x) = f(-x) = 0$, so $-x \in \ker(f)$. If $x \in \ker(f)$ and $a \in A$, then $f(xa) = f(x)f(a) = 0 \cdot f(a) = 0$, so $xa \in \ker(f)$. Also, $f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$ and $ax \in \ker(f)$. Therefore, $\ker(f) \trianglelefteq A$.

□

Problem. Prove the following:

1. $A = \{x + y\sqrt{3} : \ x, y \in \mathbb{Z}\} \leq \mathbb{R}$;
2. $B = \{x + 2^{\frac{1}{3}}y + 2^{\frac{2}{3}}z : \ x, y, z \in \mathbb{Z}\} \leq \mathbb{R}$;
3. $C = \{x2^y : \ x, y \in \mathbb{Z}\} \leq \mathbb{R}$;
4. Let $\mathcal{C}(\mathbb{R})$ be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$ which are continuous on $\mathbb{R}$ and $\mathcal{D}(\mathbb{R})$ set of functions from $\mathbb{R}$ to $\mathbb{R}$ which are differentiable on $\mathbb{R}$. Then, $\mathcal{C}(\mathbb{R}) \leq \mathcal{F}(\mathbb{R})$ and $\mathcal{D}(\mathbb{R}) \leq \mathcal{F}(\mathbb{R})$;
5. Let $\mathcal{U}(\mathbb{R})$ be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$ which are continuous on the interval $[0, 1]$. Then, $\mathcal{C}(\mathbb{R}) \leq \mathcal{U}(\mathbb{R}) \leq \mathcal{F}(\mathbb{R})$.

Solution.

1. $A = \{x + y\sqrt{3} : \ x, y \in \mathbb{Z}\} \leq \mathbb{R}$. Obviously $A \subseteq \mathbb{R}$. Let $a, b \in A$. Then, $a = x_1 + y_1\sqrt{3}$ and $b = x_2 + y_2\sqrt{3}$, for some $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. We have $a + b = (x_1+x_2)+(y_1+y_2)\sqrt{3}$, so $a+b \in A$. Then, $-a = -x_1-y_1\sqrt{3} = (-x_1)+(-y_1)\sqrt{3}$, so $-a \in A$. Finally, $ab = (x_1x_2+3y_1y_2)+(y_1x_2+x_1y_2)\sqrt{3} \in A$, so $A \leq \mathbb{R}$. Notice that A is not an ideal of $\mathbb{R}$, as, e.g. $\frac{1}{2}x + \frac{1}{2}y\sqrt{3} \notin A$ (as $\frac{x}{2}$ and $\frac{y}{2}$ are in $\mathbb{Z}$ only for even numbers).

2. $B = \{x + 2^{\frac{1}{3}}y + 2^{\frac{2}{3}}z : \ x, y, z \in \mathbb{Z}\} \leq \mathbb{R}$. We have $B \subseteq \mathbb{R}$. Take $a, b \in B$. Then, $a = x_1 + 2^{\frac{1}{3}}y_1 + 2^{\frac{2}{3}}z_1$ and $b = x_2 + 2^{\frac{1}{3}}y_2 + 2^{\frac{2}{3}}z_2$, for some $x_i, y_i, z_i \in \mathbb{Z}$, where $i \in \{1, 2\}$. We have $a + b = (x_1 + x_2) + 2^{\frac{1}{3}}(y_1 + y_2) + 2^{\frac{2}{3}}(z_1 + z_2) \in B$. Then, $-a = (-x_1)+2^{\frac{1}{3}}(-y_1)+2^{\frac{2}{3}}(-z_1) \in B$. Finally, $ab = (x_1+2^{\frac{1}{3}}y_1+2^{\frac{2}{3}}z_1)(x_2+2^{\frac{1}{3}}y_2+2^{\frac{2}{3}}z_2) = (x_1x_2+y_1z_2+z_1y_2)+2^{\frac{1}{3}}(x_1y_2+x_2y_1+2z_1z_2)+2^{\frac{2}{3}}(y_1y_2+z_1x_2+z_2x_1) \in B$, so $B \leq \mathbb{R}$. Also, B is not an ideal of $\mathbb{R}$ as multiplying it with, e.g. $\sqrt{3}$ would not give an element of B.

3. $C = \{x2^y : \ x, y \in \mathbb{Z}\} \leq \mathbb{R}$. We have $C \subseteq \mathbb{R}$. Then, $a, b \in C$ imply $a = x_1 2^{y_1}$ and $b = x_2 2^{y_2}$. We have $a+b = 2^m\,(2^{y_1-m}x_1 + 2^{y_2-m}x_2) \in C$, where $m = \min(y_1, y_2)$. Then, $-a = (-x_1)2^{y_1} \in C$ and $ab = (x_1x_2)2^{y_1+y_2} \in C$, so $C \leq \mathbb{R}$. Also, C is not an ideal of $\mathbb{R}$ as multiplying it with $\frac{1}{2}$ would not give $x \in \mathbb{Z}$, necessarily.

4. *Let $\mathcal{C}(\mathbb{R})$ be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$ which are continuous on $\mathbb{R}$ and $\mathcal{D}(\mathbb{R})$ set of functions from $\mathbb{R}$ to $\mathbb{R}$ which are differentiable on $\mathbb{R}$. Then, $\mathcal{C}(\mathbb{R}) \leq \mathcal{F}(\mathbb{R})$ and $\mathcal{D}(\mathbb{R}) \leq \mathcal{F}(\mathbb{R})$.* As sum and negative, and also a product, of continuous functions is a continuous function, obviously $\mathcal{C}(\mathbb{R}) \leq \mathcal{F}(\mathbb{R})$. The same thing goes for differentiable functions. Also, $\mathcal{C}(\mathbb{R})$ is not an ideal of $\mathcal{F}(\mathbb{R})$ as multiplying it with a discontinuous function would yield a discontinuous function.

5. *Let* $\mathcal{U}(\mathbb{R})$ *be the set of all functions from* $\mathbb{R}$ *to* $\mathbb{R}$ *which are continuous on the interval* $[0,1]$. *Then,* $\mathcal{C}(\mathbb{R}) \leq \mathcal{U}(\mathbb{R}) \leq \mathcal{F}(\mathbb{R})$. Due to the same reasoning as in previous problem, we have $\mathcal{U}(\mathbb{R}) \leq \mathcal{F}(\mathbb{R})$. Let $f \in \mathcal{C}(\mathbb{R})$. Then, f is continuous on $\mathbb{R}$, but so is on $[0,1]$, so $f \in \mathcal{U}(\mathbb{R})$. That implies $\mathcal{C}(\mathbb{R}) \subseteq \mathcal{U}(\mathbb{R})$. But, as $\mathcal{C}(\mathbb{R})$ is a ring (as a subring of $\mathcal{F}(\mathbb{R})$), then so is a subring of $\mathcal{U}(\mathbb{R})$.

Problem. Which of the following are ideals of $\mathbb{Z} \times \mathbb{Z}$: (1) $A = \{(n,n) : \ n \in \mathbb{Z}\}$, (2) $B = \{(5n,0)\} : \ n \in \mathbb{Z}\}$, (3) $C = \{(n,m) : \ 2|n+m\}$, (4) $D = \{(2n,3m) : \ n,m \in \mathbb{Z}\}$?

Solution. (1) If we take $(m,m),(n,n) \in A$, then $(m,m)-(n,n) = (m-n,m-n) \in A$. Then, $(m,m)(n,n) = (mn,mn) \in A$. If we take $(x,y) \in \mathbb{Z}$, then $(m,m)(x,y) = (mx,my)$ is generally not in A, as, e.g., $(2,2) \in A$ and $(3,5) \in \mathbb{Z} \times \mathbb{Z}$, but $(2,2)(3,5) = (6,10) \notin A$, so A is not an ideal of $\mathbb{Z} \times \mathbb{Z}$. (2) Let $(5m,0),(5n,0) \in B$. Then, $(5m,0) - (5m,0) = (5m-5m, 0-0) = (5 \cdot 0, 0) \in B$. Then, $(5m,0)(5n,0) = (5(5mn),0) \in B$. Also, if $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ then $(5m,0)(x,y) = (5(mx),0) \in B$. Therefore, B is an ideal of $\mathbb{Z} \times \mathbb{Z}$. (3) Let $(n,m),(p,q) \in C$. Then, $(n,m)-(p,q) = (n-p,m-q)$. If $n+m = 2k$ and $p+q = 2l$, then $n = 2k-m$ and $p = 2l-q$. So $n-p = 2(k-l)+(q-m)$. Then, $(n-p)+(m-q) = 2(k-l)+(q-m)+(m-1) = 2(k-l)$. Therefore, $(n-p,m-q) \in C$. Also, $(n,m)(p,q) = (np,mq)$ and $np+mq = (2k-m)(2l-q)+mq = 4kl-2kq-2lm+mq+mq = 2(2kl-kq-lm+mq)$. Therefore, $(n,m)(p,q) \in C$. If $(x,y) \in \mathbb{Z}$, then e.g. $(3,5)(2,1) = (6,5)$, but $6+5 = 11$ and $(6,5) \notin C$. Thus, C is not an ideal of $\mathbb{Z} \times \mathbb{Z}$. (4) Let $(2n,3m),(2p,3q) \in D$. Then, $(2n,3m)-(2p,3q) = (2(n-p),3(m-q)) \in D$. Also, $(2n,3m)(2p,2q) = (2(2np),3(3mq)) \in D$. If $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ then $(2n,3m)(x,y) = (2(nx),3(my)) \in D$. Therefore, D is an ideal of $\mathbb{Z} \times \mathbb{Z}$.

Problem. List all the ideals of $\mathbb{Z}_{12}$.

Solution. We have $\{0,2,4,6,8,10\}$, $\{0,3,6,9\}$, $\{0,4,8\}$, $\{0,6\}$ and $\{0\}$. Notice that in $\{0,3,6,9\}$, 9 is unity. Similarly in $\{0,4,8\}$, 4 is unity. So, in $\{0,6\}$, 6 is obviously unity. Yet, there is no unity in $\{0,2,4,6,8,10\}$.

Problem. Prove that if $A \leq \mathbb{Z}_n$, then $A \trianglelefteq \mathbb{Z}_n$.

Solution. Let $A \leq Z_n$. Then if $a \in A$ and $b \in \mathbb{Z}_n$, we have $ab = \underbrace{a+a+\cdot+a}_{b \text{ times}}$. As A is closed with respect to addition, $ab \in A$. Same thing for $ba \in A$.

Problem. Prove that each of the following is an ideal of $\mathcal{F}(\mathbb{R})$: (1) The set A of all f such that $f(x) = 0$ for every $x \in \mathbb{Q}$. (b) The set B of all f such that $f(0) = 0$.

Solution. (a) If $f,g \in A$, then $[f-g](x) = f(x) - g(x) = 0 - 0 = 0$, for all $x \in \mathbb{Q}$,

so $f - g \in A$. If $g \in \mathcal{F}(\mathbb{R})$, then $[fg](x) = f(x)g(x) = 0 \cdot g(x) = 0$, for all $x \in \mathbb{Q}$, so $fg \in A$. (b) If $f, g \in B$, then $[f - g](0) = f(0) - g(0) = 0 - 0 = 0$, so $f - g \in B$. If $g \in \mathcal{F}(\mathbb{R})$, then $[fg](0) = f(0)g(0) = 0 \cdot g(0) = 0$, so $fg \in B$.

Problem. Give an example of a subring of $\mathbb{Z}_3 \times \mathbb{Z}_3$ which is not an ideal.

Solution. We have $A = \{(0,0), (1,1), (2,2)\}$ which is obviously a subring of $\mathbb{Z}_3 \times \mathbb{Z}_3$. But, if we take $(1,2) \in \mathbb{Z}_3 \times \mathbb{Z}_3$, then $(1,1)(1,2) = (1,2) \notin A$, so A is not an ideal of $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Definition. Let A be an integral domain and $B \leq A$. If B is an integral domain, we say that B is a **subdomain** of A.

Proposition. Let A be an integral domain and $B \leq A$. If $1 \in B$, then B is a subdomain of A.

Proof. As A is an integral domain, then $ab = ac$ implies $b = c$, for all $a, b, c \in A$. Take $a, b, c \in B$ where $a \neq 0$. Then, as also $a, b, c \in A$, $ab = ac$ implies $b = c$. Integral domain is defined as a commutative ring with unity, so it also must be that $1 \in B$.

□

Proposition. Every subring containing the unity of a field is an integral domain.

Proof. Let F be a field and $A \leq F$ and $1 \in A$. As F is commutative, so is A. Let $a, b, c \in A$, $a \neq 0$ and $ab = ac$. As also $a \in F$, then there exists $a^{-1} \in F$ such that $aa^{-1} = a^{-1}a = 1$. Then, $a^{-1}ab = a^{-1}ac$ implies $b = c$. Therefore, as $1 \in A$, we have that A is a commutative ring with unity. As also $ab = ac$ implies $b = c$, then A is an integral domain.

□

Definition. Let F be a field and $A \leq F$. If A is a field, we say that A is a **subfield** of F.

Proposition. Let F be a field and $B \leq F$. If B is closed with respect to multiplicative inverses, then B is a field.

Proof. As $B \leq F$, we have that B is a ring. As F is commutative, then so is B. Assume B is closed with respect to inverses. Then, for all $a \in B$ there exists $a^{-1} \in B$ such that $aa^{-1} = a^{-1}a = 1$. As $a \in B$ and $a^{-1} \in B$, then $aa^{-1} \in B$ (as it is closed with

respect to multiplication). Therefore, also $aa^{-1} = 1 \in B$. So, B is a commutative ring with unity, and as every element has an inverse, it is also a field.

□

Problem. Find subrings of $\mathbb{Z}_1 8$ which illustrate each of the following: (a) A is a ring with unity, $B \leq A$, but B is not a ring with unity; (b) A and B are rings with unity, $B \leq A$, but the unity of B is not the same as the unity of A.

Solution. (a) We have $A = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$, where unity is 10 and $B = \{0, 6, 12\}$, where $A \leq B$, but it has no unity. (b) $A = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$ and $B \leq A$, where $B = \{0, 9\}$. Unity is $9 \in B$, but $10 \in A$.

Proposition. Let A be a ring, $f : A \to A$ a homomorphism, and $B = \{x \in A : f(x) = x\}$. Then, $B \leq A$.

Proof. Obviously $B \subseteq A$. Let $x, y \in B$. Then, $f(x) = x$ and $f(y) = y$. We have $x - y = f(x) - f(y) = f(x - y) \in B$, so $x - y \in B$. Then, $xy = f(x)f(y) = f(xy) \in B$, so $xy \in B$ and by that $B \leq A$.

□

Definition. Let A be a ring. Center of ring A is the set:

$$Z(A) = \{a \in A : \ (\forall x \in A)(xa = ax)\}.$$

Proposition. Let A be a ring. Then, $Z(A) \leq A$.

Proof. First, $Z(A) \subseteq A$. Then, if $a, b \in Z(A)$, we have $ax = xa$ and $bx = xb$, for all $x \in A$. Then, $ax - bx = xa - bx$. But, as $bx = xb$, we have $ax - bx = xa - xb$. By distributive laws, that is equivalent to $(a - b)x = x(a - b)$, so $a - b \in Z(A)$. Also, $abx = axb$, as $bx = xb$, for all $x \in A$. Then, $axb = xab$, as $ax = xa$, for all $x \in A$. So, as $(ab)x = x(ab)$, we have $ab \in Z(A)$. Therefore, $Z(A) \leq A$.

□

Proposition. Let A be a ring and $J_1, J_2 \trianglelefteq A$. Then, $J_1 \cap J_2 \trianglelefteq A$.

Proof. We see that $J_1 \cap J_2 \subseteq A$. Take $x, y \in J_1 \cap J_2$. Then, $x, y \in J_1$ and $x, y \in J_2$. As J_1 and J_2 are ideals, then $x - y \in J_1$ and $x - y \in J_2$, so $x - y \in J_1 \cap J_2$. Also, $xy \in J_1$ and $xy \in J_2$, therefore $xy \in J_1 \cap J_2$. If $a \in A$, then $xa, ax \in J_1$ and $xa, ax \in J_2$, i.e. $xa, ax \in J_1 \cap J_2$, so $J_1 \cap J_2 \trianglelefteq A$.

□

Proposition. Let A be a ring. If $J \trianglelefteq A$ and $1 \in J$ then $J = A$.

Proof. First, we have $J \subseteq A$, because $J \trianglelefteq A$. If we take $a \in A$, then $ax \in J$, for all $x \in J$. But, as $1 \in J$, then also $a1 \in J$. Therefore, $a \in J$ and we have $A \subseteq J$. That implies $J = A$.

□

Proposition. Let A be a ring. If $J \trianglelefteq A$ and there exists $a \in J$ such that $aa^{-1} = a^{-1}a = 1$, for some $a^{-1} \in J$, then $J = A$.

Proof. As, for some $a \in J$ there exists $a^{-1} \in J$ such that $aa^{-1} = 1$, then, due to $J \leq A$, we have $aa^{-1} \in J$, i.e. $1 \in J$. By previous proposition, if $1 \in J$, then $J = A$.

□

Proposition. Let F be a field. If $J \trianglelefteq F$, then $J = F$ or $J = \{0\}$.

Proof. As all $a \in F$ are invertible, i.e. there exists $a^{-1} \in F$, such that $aa^{-1} = 1$. So, if we have $a \in J$, then, as $J \trianglelefteq F$, we have $ba \in J$, for all $b \in F$. But, we also have $a^{-1} \in F$, so $a^{-1}a \in J$, i.e. $1 \in J$. By a previous proposition we have that $J = F$. The only other ideal is $J = \{0\}$, if J contains only the zero, i.e. the neutral element with respect to addition.

□

Proposition. Let A and B be rings, and $f : A \to B$ a homomorphism. Then,

1. $f(0) = 0$ and $f(-a) = -f(a)$ for all $a \in A$.
2. $f(A) \leq B$.
3. $\ker(f) \trianglelefteq A$.
4. Let $1 \in A$. If $\text{ran}(f)$ is an integral domain, then $f(1) \in \{0, 1\}$. If $f(1) = 0$, then $f(x) = 0$ for every $x \in A$. If $f(1) = 1$, the image of every invertible element of A is an invertible element of $\text{ran}(f)$.
5. Any homomorphic image of a commutative ring is a commutative ring. Any homomorphic image of a field is a field.
6. If the domain A of the homomorphism f is a field, and if the range of f has more than one element, then f is injective.

Proof. *Ad* 1. Altough results follow immediately from group theory, we will redo the proof in additive notation. First, let $0_A \in A$ be a zero in A and $0_B \in B$ zero in B. Then, $0_A + 0_A = 0_A$. But, as f is a well-defined function, $f(0_A + 0_A) = f(0_A)$. As f is a homomorphism, $f(0_A) + f(0_A) = f(0_A)$. As B is a ring, there exists $-f(0_A)$ (only a notation for negative, i.e. additive inverse, of $f(0_A) \in B$) such that $f(0_A) = f(0_A) + (-f(0_A))$. But, $f(0_A) + (-f(0_A)) = 0_B$, so $f(0_A) = 0_B$. That's why it is unambiguous if we denote both zeros in A and in B with 0. Then, take $a \in A$. We have $a + (-a) = 0$. As f is a well-defined function, then $f(a + (-a)) = f(0)$. As f is a homomorphism, and $f(0) = 0$, we have $f(a) + f(-a) = 0$. Then, as B is a ring and closed with respect to negatives, there exists $-f(a) \in B$ such that $f(a) + (-f(a)) = 0$. Therefore, $f(a) + f(-a) + (-f(a)) = -f(a)$. But, that is equivalent to $f(-a) = -f(a)$. Therefore, f copies negatives to negatives.

Ad 2. As $f(A) = \{b \in B : \ (\exists a \in A)(f(a) = b)\}$, then, $f(A) \subseteq B$. Assume $b_1, b_2 \in f(A)$. Then, there exist $a_1, a_2 \in A$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$. First, $b_1 - b_2 = b_1 + (-b_2) = f(a_1) + (-f(a_2)) = f(a_1) + f(-a_2) = f(a_1 + (-a_2)) \in f(A)$, so $b_1 - b_2 \in f(A)$. Then, $b_1 b_2 = f(a_1) f(a_2) = f(a_1 a_2) \in f(A)$, so $b_1 b_2 \in f(A)$. Therefore, $f(A) \leq B$.

Ad 3. As $\ker(f) = \{a \in A : \ f(a) = 0\}$, we have $\ker(f) \subseteq A$. But, assume $x, y \in \ker(f)$. As A is a ring, there exists $a \in A$ such that $x - y = a$ (it is closed with respect to subtraction). Then, as f is a well-defined function, $f(x - y) = f(a)$. But, $f(a) = f(x - y) = f(x + (-y)) = f(x) + f(-y) = f(x) + (-f(y)) = 0 + (-0) = 0$. Thus, $f(x - y) = 0$ and we have $x - y \in \ker(f)$. Also, as A is a ring, there exists $a' \in A$ such that $xy = a'$ (it is closed with respect to products). As f is a well-defined function, $f(xy) = f(a')$. But, $f(a') = f(xy) = f(x)f(y) = 0 \cdot 0 = 0$, so $xy \in \ker(f)$. Also, if $x \in \ker(f)$ and $a \in A$, then we have $xa = a'$, for some $a' \in A$. As f is a well-defined function, $f(a') = f(xa) = f(x)f(a) = 0 \cdot f(a) = 0$, so $xa \in \ker(f)$. Thus, $\ker(f) \trianglelefteq A$.

Ad 4. Let $\operatorname{ran}(f)$ be an integral domain, i.e. for all $f(a), f(b), f(c) \in \operatorname{ran}(f)$, $f(a) \neq 0$, we have $f(a)f(b) = f(a)f(c)$ implies $f(b) = f(c)$. As $1 \in A$, then $f(1) \in \operatorname{ran}(f)$. But, as f is a homomorphism, we have $f(1) = f(1 \cdot 1) = f(1)f(1)$. Then, taking the negative of $f(1)$, we get $0 = f(1)^2 - f(1)$. That is, by distributive law, equivalent to $0 = f(1)(f(1) - 1)$ (notice that 1 here refers to unity in $\operatorname{ran}(f)$; maybe we should have denoted it as $1_{\operatorname{ran}(f)}$). As B is an integral domain, that implies that $f(1) = 0$ or $f(1) - 1 = 0$, i.e. $f(1) = 1$. Thus, $f(1) \in \{0, 1\}$. Assume $f(1) = 0$. As $a \cdot 1 = a$, for all $a \in A$, then, $f(a) = f(a \cdot 1) = f(a)f(1) = 0$. Therefore, $f(a) = 0$, for all $a \in A$. Now, let $f(1) = 1$. Assume that for some $a \in A$ there exists $a^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$. Then, $f(aa^{-1}) = f(a^{-1}a) = f(1)$. That gives us $f(a)f(a^{-1}) = f(a^{-1})f(a) = 1$, i.e. $f(a)[f(a)]^{-1} = [f(a)]^{-1}f(a) = 1$, i.e. $f(a)$ (if $f(a) \neq 0$) is invertible.

Ad 5. Let A be a commutative ring. Then, $ab = ba$, for all $a, b \in A$. Choose $f(a), f(b) \in \text{ran}\,(f)$. Then, $f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$, for all $f(a), f(b) \in \text{ran}\,(f)$, therefore $\text{ran}\,(f)$ is a commutative ring. Let A be a field. Then, A is commutative, $1 \in A$ and for all $a \in A$ there exists $a^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$. The property of unity is that $1 \cdot a = a \cdot 1 = a$, for all $a \in A$. If we take $f(a) \in \text{ran}\,(f)$, then $f(a) = f(a \cdot 1) = f(a)f(1)$. Therefore, $f(1) = 1_{\text{ran}(f)}$, and we can designate it as 1. If we take $f(a) \in \text{ran}\,(f)$, then $a \in A$, and there exists $a^{-1} \in A$ such that $a^{-1}a = aa^{-1} = 1$. But, as $a^{-1} \in A$, then $f(a^{-1}) \in \text{ran}\,(f)$. We have $f(aa^{-1}) = 1$, i.e. $f(a)f(a^{-1}) = 1$. Thus, $f(a^{-1}) = [f(a)]^{-1}$, and every $f(a) \in \text{ran}\,(f)$ (except zero, of course) is invertible. That means that $\text{ran}\,(f)$ is a field.

Ad 6. Assume A is a field and $|\text{ran}\,(f)| > 1$, i.e. there exists $f(a) \in \text{ran}\,(f)$ such that $f(a) \neq 0$. Also, there exists $1 \in \text{ran}\,(f)$. But, as A is a field, then $\text{ran}\,(f)$ is a field. If we take $f(a) = f(b)$, for some $f(a), f(b) \in \text{ran}\,(f)$, we have $f(a)[f(b)]^{-1} = f(b)[f(b)^{-1}]$. That gives us $f(ab^{-1}) = 1$. As $f(1) = 1$, then, $f(ab^{-1}) = f(1)$. That gives us $f(ab^{-1} - 1) = 0$. That means that $(ab^{-1} - 1) \in \ker\,(f)$. But, as $\ker\,(f) \trianglelefteq A$, and A is a field, then $\ker\,(f) = \{0\}$, or $\ker\,(f) = A$. If it were that $\ker\,(f) = A$, we would have that $f(a) = 0$, for all $a \in A$, meaning $\text{ran}\,(f) = 0$. That would be in contradiction with our assumption that $|\text{ran}\,(f)| > 1$. So, it must be $\ker\,(f) = \{0\}$. That implies $ab^{-1} - 1 = 0$, i.e. $ab^{-1} = 1$. Multiplying by b on the right gives us $a = b$. Thus, as $f(a) = f(b)$ implied $a = b$, we have that f is injective.

□

Proposition. Let $m, n \in \mathbb{Z}$. If $m \neq n$, then $m\mathbb{Z} \ncong n\mathbb{Z}$.

Proof. If we assume that there exists an isomorphism, it would have to carry zero to zero and inverse to inverse, i.e. it would have to satisfy following set of equations:

$$\begin{aligned} f(0) &= 0, \\ f(-mk) &= -f(mk), \\ f(mk_1 + mk_2) &= f(mk_1) + f(mk_2), \\ f(mk_1mk_2) &= f(mk_1)f(mk_2). \end{aligned}$$

We can assume that $f(mk) = ng(k)$, where $g : \mathbb{Z} \to \mathbb{Z}$ is a bijection carrying indices. From $f(mk_1 + mk_2) = f(mk_1) + f(mk_2)$, we then get $f(mk_1 + mk_2) = f(m(k_1 + k_2) = ng(k_1 + k_2)$. But also, $f(mk_1) + f(mk_2) = ng(k_1) + ng(k_2)$, so it must be that $g(k_1+k_2) = g(k_1)+g(k_2)$. We also have $f(mk_1mk_2) = f(m(mk_1k_2)) = ng(mk_1k_2)$. But, we know that $g(mk_1k_2) = g(\underbrace{k_1k_2 + \cdots + k_1k_2}_{m \text{ times}}) = mg(k_1k_2)$. Therefore, $f(mk_1mk_2) =$

$nmg(k_1k_2)$, but also $f(mk_1)f(mk_2) = ng(k_1)ng(k_2)$, so $mg(k_1k_2) = ng(k_1)g(k_2)$, i.e. $g(k_1k_2) = \frac{n}{m}g(k_1)g(k_2)$. Now, as $n \neq m$, then $\frac{n}{m} \neq 1$. But, that fact can be exploited, as $g(k) = g(k \cdot (1 \cdot 1)) = \frac{n}{m}g(k)g(1 \cdot 1) = \frac{n^2}{m^2}g(k)g(1)g(1)$. Now, $f(mk) = f(m(k \cdot 1)) = ng(k \cdot 1) = \frac{n^2}{m}g(k)g(1)$. Let $k \neq 0$, then, $g(k) \neq 0$ (it has to be $f(0) = 0$, so $f(m \cdot 0) = ng(0) = 0$). But, $f(mk) = ng(k)$, so we have $ng(k) = \frac{n^2}{m}g(k)g(1)$. That gives us, as $g(k) \neq 0$, that $g(1) = \frac{m}{n}$. But, $g(1) = g(1 \cdot 1) = \frac{n^2}{m^2}g(1)g(1)$. That means that, as $g(1) \neq 0$, that $g(1) = \frac{m^2}{n^2}$. But, $g(1) = \frac{m}{n}$, so we have $\frac{m^2}{n^2} = \frac{m}{n}$, i.e. $\frac{m}{n} = 1$, but that can only happen if $m = n$. This is a contradiction to our assumption that $m \neq n$, and then, f cannot be an isomorphism.

□

Definition. Let A be a ring and $J \trianglelefteq A$. Then, the **radical** of J is the set:

$$\operatorname{rad}(J) = \{a \in A : \ (\exists n \in \mathbb{Z})\,(a^n \in J)\}.$$

Proposition. Let A be a ring and $J \trianglelefteq A$. Let $a \in A$. Then, if $a^n \in J$, for some $n \in \mathbb{Z}$, then $a^m \in J$, for all $m \geq n$, $m \in \mathbb{Z}$.

Proof. Assume $m = n$. Then, there is nothing to prove as already $a^n \in J$. Assume $a^m \in J$ for some $m > n$. Then, as $a^m \in J$ and $a \in A$, we have $aa^m \in J$ (as $J \trianglelefteq A$), i.e. $a^{m+1} \in J$. Thus, by induction we have that $a^m \in J$, for all $m > n$.

□

Proposition. Let A be a commutative ring and $J \trianglelefteq A$. Then, $\operatorname{rad}(J) \trianglelefteq A$.

Proof. First, $\operatorname{rad}(J) \subseteq A$ is obvious from the definition of $\operatorname{rad}(J)$. Let $a, b \in \operatorname{rad}(J)$. Then there exist $m, n \in \mathbb{Z}$ such that $a^m, b^n \in J$. If we take $(a+b)^{n+m}$, by binomial formula (applicable as A is commutative) we have:

$$\begin{aligned}(a+b)^{n+m} &= \sum_{k=0}^{n+m} \binom{n+m}{k} a^{n+m-k}b^k \\ &= \sum_{k=0}^{n} \binom{n+m}{k} a^{n+m-k}b^k + \sum_{k=n+1}^{n+m} \binom{n+m}{k} a^{n+m-k}b^k.\end{aligned}$$

In the first sum we have a^{n+m-k} where $0 \leq k \leq n$. That implies $0 \geq -k \geq -n$. Therefore, $n + m - k \geq n + m - n = m$. By previous proposition we have that $a^{n+m-k} \in J$, as $n+m-k \geq m$. But, as $b^k \in A$, then $a^{n+m-k}b^k \in J$. In the second sum we have b^k, where $n+1 \leq k \leq n+m$. So, $k > n$ and we have, by a previous proposition,

that $b^k \in J$. As $a^{n+m-k} \in A$, we have $a^{n+m-k}b^k \in J$. As all members of the sums are in J, then their sum is also in J, as also $J \leq A$. That gives us that $(a+b)^{n+m} \in J$. From that we have that $a+b \in \mathrm{rad}\,(J)$. If $a \in \mathrm{rad}\,(J)$, then $-a^m = (-a)^m$ if m is odd and $-a^{m+1} = (-a)^{m+1}$ if m is even, so $-a \in \mathrm{rad}\,(J)$. Finally, if $a \in A$ and $b \in \mathrm{rad}\,(J)$, then $b^m \in J$. As A is commutative, we have $(ab)^m = a^m b^m$. As $b^m \in J$, and $a^m \in A$, then $(ab)^m \in J$. So, $ab \in \mathrm{rad}\,(J)$.

□

Proposition. Let A be a ring and $J, K \trianglelefteq A$. If $J \cap K = \{0\}$, then $jk = 0$, for every $j \in J$ and $k \in K$.

Proof. Let $j \in J$ and $k \in K$. As $k \in K \subseteq A$, then $jk \in J$. As $j \in J \subseteq A$, then $jk \in K$. From that we have $jk \in J \cap K$. As $J \cap K = \{0\}$, then it can only be that $jk = 0$.

□

Proposition. Let A be a commutative ring. For any $a \in A$, $I_a = \{ax + j + k : \ x \in A, \ j \in J, \ k \in K\} \trianglelefteq A$.

Proof. Let $a \in A$. Then, $ax_1 + j_1 + k_1, ax_2 + j_2 + k_2 \in I_a$. We have $(ax_1 + j_1 + k_1) - (ax_2 + j_2 + k_2) = a(x_1 - x_2) + (j_1 - j_2) + (k_1 - k_2)$. As $x_1 - x_2 \in A$, $j_1 - j_2 \in J$ and $k_1 - k_2 \in K$, then $(ax_1 + j_1 + k_1) - (ax_2 + j_2 + k_2) \in I_a$. Now, let $b \in A$. Then, $(ax_1 + j_1 + k_1)b = ax_1 b + j_1 b + k_1 b$. As $x_1 b \in A$, $j_1 b \in J$ and $k_1 b \in K$, we have that $(ax_1 + j_1 + k_1)b \in I_a$. As A is commutative then also $b(ax_1 + j_1 + k_1) \in I_a$, so $I_a \trianglelefteq A$.

□

Definition. Let A be a commutative ring and $a \in A$. Set

$$\mathrm{Ann}\,(a) = \{x \in A : \ ax = 0\}$$

is called the **annihilator** of a. Also, set

$$\mathrm{Ann}\,(A) = \{x \in A : \ (\forall a \in A)\,(ax = 0)\}$$

is called the **annihilating ideal** of A.

Proposition. Let A be a commutative ring. Then,

1. $\mathrm{Ann}\,(a) \trianglelefteq A$, for all $a \in A$.

2. $\mathrm{Ann}\,(A) \trianglelefteq A$.

Proof. *Ad* 1. Let $a \in A$. Obviously, $\mathrm{Ann}\,(a) \subseteq A$. Then, let $x, y \in \mathrm{Ann}\,(a)$. Then, $ax = ay = 0$. First, by distributive law $a(x - y) = ax - ay = 0 - 0 = 0$, so $x - y \in \mathrm{Ann}\,(a)$. By associativity of multiplication, $a(xy) = (ax)y = 0y = 0$, so $xy \in \mathrm{Ann}\,(a)$. Finally, if $b \in A$, then $a(xb) = (ax)b = 0$, so $xb \in \mathrm{Ann}\,(A)$. As A is commutative, then $a(bx) = 0$ and $bx \in \mathrm{Ann}\,(a)$. Thus, $\mathrm{Ann}\,(a) \trianglelefteq A$.

Ad 2. We have $\mathrm{Ann}\,(A) \subseteq A$. If $x, y \in \mathrm{Ann}\,(A)$, then $ax = ay = 0$, for all $a \in A$. So, by distributive law, $a(x - y) = ax - ay = 0 + 0 = 0$, for all $a \in A$ and we have $x - y \in \mathrm{Ann}\,(A)$. Also, by associativity, $a(xy) = (ax)y = 0 \cdot y = 0$, and $xy \in \mathrm{Ann}\,(A)$. Finally, if $b \in A$, then, by associativity, $a(xb) = (ax)b = 0 \cdot b = 0$ and $xb \in \mathrm{Ann}\,(A)$. As A is commutative, then also $bx \in \mathrm{Ann}\,(A)$. That implies $\mathrm{Ann}\,(A) \trianglelefteq A$.

□

Proposition. Let A be a ring and $1 \in A$. Then, $\mathrm{Ann}\,(A) = \{0\}$.

Proof. We can see that $0 \in \mathrm{Ann}\,(A)$ as $a \cdot 0 = 0$, for all $a \in A$. Now, assume $x \in \mathrm{Ann}\,(A)$, $x \neq 0$. Then, $ax = 0$, for all $a \in A$. But, as $1 \in A$, then also $1 \cdot x = 0$. Thus, we have $x = 0$, which is a contradiction. Therefore, $\mathrm{Ann}\,(A) = \{0\}$.

□

Proposition. Let A be a ring. Then, $\{0\} \trianglelefteq A$ and $A \trianglelefteq A$.

Proof. As $0 - 0 = 0$ and $0 \cdot 0$ we have $\{0\} \leq A$. Then, as $a \cdot 0 = 0 \cdot a = 0$, for all $a \in A$, we have $\{0\} \trianglelefteq A$. Then, as $A \leq A$ and $ax \in A$ for all $x \in A$ and $a \in A$, we have $A \trianglelefteq A$.

□

Proposition. Let A and B be rings and $f : A \to B$ a homomorphism from A to B. If $\ker(f) \subseteq J \trianglelefteq A$, then $f(J) \trianglelefteq f(A)$.

Proof. Assume $\ker(f) \subseteq J$. Obviously, $f(J) \subseteq f(A)$. Now, take $f(x), f(y) \in f(J)$ (note that we have $x, y \in J$). Then, $f(x)f(y) = f(xy)$. As $x, y \in J$ and $J \trianglelefteq A$, then $xy \in J$. So, $f(xy) \in f(J)$ and from that $f(x)f(y) \in f(J)$. Similarly, as $x^{-1} \in J$ then $f(x^{-1}) \in f(J)$. But, $f(x^{-1}) = [f(x)]^{-1} \in J$. Thus, $f(J) \leq f(A)$. But, if we take $f(a) \in f(A)$ and $f(j) \in J$, then $f(a)f(j) = f(aj)$. But, as $J \trianglelefteq A$ and $a \in A$ and $j \in J$, then $aj \in J$. Similarly we show that $f(j)f(a) \in f(J)$. From that we have $f(J) \trianglelefteq f(A)$.

□

Definition. Let A be a ring and $J \trianglelefteq A$. We say that J is a **maximal ideal** of A if, for all $K \trianglelefteq A$, $J \subset K \subseteq A$ implies $K = A$.

Proposition. Let A and B be rings with $f : A \to B$ a homomorphism. If $\operatorname{ran}(f)$ is a field, then $\ker(f)$ is a maximal ideal of A.

Proof. Assume $\ker(f) \subset J$, where $J \trianglelefteq A$. Then, by a previous proposition, $f(J) \trianglelefteq f(A) = \operatorname{ran}(f)$. As $\operatorname{ran}(f)$ is a field, then, by a previous proposition, $f(J) = \operatorname{ran}(f)$ or $f(J) = \{0\}$. Assume $f(J) = \{0\}$. If we take $j \in J$, then $f(j) \in f(J) = \{0\}$, so it must be $f(j) = 0$, i.e. $j \in \ker(f)$. Thus, $J \subseteq \ker(f)$, contrary to our assumption that $\ker(f) \subset J$ and it cannot be that $f(J) = \{0\}$. Assume $f(J) = \operatorname{ran}(f)$. We already know that $J \subseteq A$. Assume $J \subset A$. Then there exists $a \in A - J$ and we have $f(a) \in f(A - J) \subseteq \operatorname{ran}(f)$. But, $f(J) = \operatorname{ran}(f)$, so $f(a) \in f(J)$. But, as $f(J)$ contains only $f(j)$, where $j \in J$, then it must be that $a \in J$, contrary to our assumption that $a \notin J$ and $a \in A$. So it must be $J = A$. That means that $\ker(f)$ is a maximal ideal of A.

□

Remark. Notice that, from elementary arithmetic we know that $\mathbb{Z}$ is an integral domain. We will later prove it more rigorously (and the proof will be found in my works on number theory).

Proposition. There are no non-trivial[69] homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

Proof. Assume that $f : \mathbb{Z} \to \mathbb{Z}$ is a homomorphism. Every element in $\operatorname{dom}(f)$ must be used, and so does $1 \in \mathbb{Z}$. Note that $\mathbb{Z} = \langle 1 \rangle$. So, if $f(k) \in \operatorname{ran}(f)$, then, as $k \in \mathbb{Z}$, we have

$$k = \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}}.$$

So, the image of k is equal to:

$$f(k) = f(\underbrace{1 + 1 + \cdots + 1}_{k \text{ times}}) = \underbrace{f(1) + f(1) + \cdots + f(1)}_{k \text{ times}} = k \cdot f(1).$$

As each $f(k)$ can be represented as a multiple (in group theory power) of $f(1)$, it is obvious that $\operatorname{ran}(f) = \langle f(1) \rangle$. Assume $f(1) = k$, where $k \neq 1$. Then, $f(n) = f(1 \cdot n) = f(1)f(n) = kf(n)$. From $f(n) = kf(n) = f(n)k$ (as multiplication is commutative) we

[69] Trivial homomorphisms are $f(x) = 0$ and $f(x) = x$.

get that k, i.e. $f(1)$ is a unity in $\mathrm{ran}\,(f)$. As $\mathrm{ran}\,(f)$ is a subring of $\mathbb{Z}$, with inherited cancellation property, and unity, it is an integral domain. So, by a previous proposition, either $f(1) = 1$ or $f(1) = 0$. If it were that $f(1) = 1$, then $f(\langle 1\rangle) = \langle f(1)\rangle = \langle 1\rangle$. So, if we take $f(x) \in \mathrm{ran}\,(f) = \langle 1\rangle$, then $f(x) = k$, i.e. $f(x) = k \cdot 1$. But, also $x = x \cdot 1$, so $f(x) = f(x \cdot 1) = f(x)f(1) = x \cdot 1$. But, that means that $x \cdot 1 = k \cdot 1$. From that we have $x = k$, i.e. $f(x) = x$, for all $x \in \mathbb{Z}$. If $f(1) = 0$, then $f(\langle 1\rangle) = \langle f(1)\rangle = \langle 0\rangle = 0$. Thus, $f(x) = 0$, for all $x \in \mathbb{Z}$.

□

Proposition. Let A be a commutative ring and $\pi_a : A \to A$ with $\pi_a(x) = ax$, for all $a \in A$. Then,

1. π_a is an endomorphism of the additive group A.
2. Let $a \neq 0$. Then, π_a is injective if and only if a is not a divisor of zero.
3. Let $1 \in A$. Then, π_a is surjective if and only if a is invertible.

Proof. *Ad* 1. First we will check that π_a is well-defined. If we take $x \in A$, then, as $a \in A$ and $x \in A$, obviously $ax \in A$, so $f(x) = ax$. Then, if $x = y$, and we multiply that by a on the left, we get $ax = ay$, i.e. $f(x) = f(y)$. Therefore, f is indeed a well-defined function. Then, $\pi_a(x + y) = a(x + y) = ax + ay = \pi_a(x) + \pi_a(y)$, so π_a is a homomorphism, i.e. endomorphism, for the additive group A.

Ad 2. *Necessity.* Assume $\pi_a(x) = \pi_a(y)$ implies $x = y$. That is, $ax = ay$ implies $x = y$. From the former expression we have $ax - ay = 0$, i.e. $a(x - y) = 0$, which implies $x = y$, that is $x - y = 0$. Therefore, a cannot be a divisor of zero, as it would have to be $a \neq 0$ and $(x - y) \neq 0$. *Sufficiency.* Assume a is not a divisor of zero. Then, $ax = 0$ implies $a = 0$ or $x = 0$. Assume $\pi_a(x) = \pi_a(y)$, i.e. $ax = ay$. Then, $ax - ay = 0$ and $a(x - y) = 0$. As a is not a divisor of zero, we have either $a = 0$ or $x - y = 0$, i.e. $x = y$. It cannot be the former, so it is the latter and we are done.

Ad 3. *Necessity.* Assume π_a is surjective, that is, for all $y \in A$, there exists $x \in A$ such that $\pi_a(x) = y$. Then, we have $ax = y$. As also $1 \in A$, then we can take $y = 1$. We would then have that there exists $x \in A$ such that $\pi_a(x) = 1$, i.e. $ax = 1$. As A is commutative then $ax = xa$. So, $ax = xa = 1$ is equivalent to the fact that a is invertible. *Sufficiency.* Assume that there exists $a^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$. If we take $y \in A$, then we need to find $x \in A$ such that $\pi_a(x) = y$. That means that $ax = y$. As a is invertible, we can multiply that equation by a^{-1} on the left. So we get $x = a^{-1}y$. To conclude, for all $y \in A$ we have that $\pi_a(a^{-1}y) = y$ and π_a is surjective.

□

Proposition. Let $\mathcal{A} = \{\pi_a : \ a \in A\}$ be a set with two operations, $[\pi_a + \pi_b](x) = \pi_a(x) + \pi_b(x)$ and $\pi_a\pi_b = \pi_a \circ \pi_b$. Then, $\mathcal{A}$ is a ring.

Proof. *Additive group.* Associativity is inherited from A, as $\pi_a(x), \pi_b(x), \pi_c(x) \in A$, we have $[\pi_a+(\pi_b+\pi_c)](x) = \pi_a(x)+[\pi_b+\pi_c](x) = \pi_a(x)+(\pi_b(x)+\pi_c(x)) = (\pi_a(x)+\pi_b(x))+\pi_c(x) = [\pi_a+\pi_b](x)+\pi_c(x) = [(\pi_a+\pi_b)+\pi_c](x)$. Commutativity is also inherited from A. Neutral element is π_0 as $[\pi_0+\pi_a](x) = \pi_0(x)+\pi_a(x) = 0x+ax = 0+ax = ax = \pi_a(x)$. Commutativity fulfills $[\pi_0 + \pi_a](x) = [\pi_a + \pi_0](x)$. Finally, inverse element is $\pi_{-a}(x)$ as $[\pi_a + \pi_{-a}](x) = \pi_a(x) + \pi_{-a}(x) = ax + (-a)x = ax - ax = 0 = 0x = \pi_0(x)$. Due to commutativity it's also $[\pi_{-a} + \pi_a](x) = \pi_0(x)$. *Distributive laws.* We have $[\pi_a(\pi_b + \pi_c)](x) = [\pi_a \circ (\pi_b + \pi_c)](x) = \pi_a([\pi_b + \pi_c](x)) = a(\pi_b(x) + \pi_c(x)) = a\pi_b(x) + a\pi_c(x) = \pi_a(\pi_b(x)) + \pi_a(\pi_c(x)) = [\pi_a\pi_b](x) + [\pi_a\pi_c](x)$. Similarly, we can show the second distributive law. *Multiplicative group.* Associativity holds due to associativity of function composition. Therefore, $\mathcal{A}$ is a ring.

□

Proposition. If $\phi : A \to \mathcal{A}$ is given by $\phi(a) = \pi_a$, then ϕ is a homomorphism. Additionaly, if A has a unity or A has no divisors of zero, then ϕ is an isomorphism.

Proof. First, ϕ is well defined as for each $a \in A$ there exists $\pi_a \in \mathcal{A}$, by definition. Also if $a = b$, then, multiplying by $x \in A$ on the right, we have $ax = bx$, i.e. $\pi_a(x) = \pi_b(x)$, for all $x \in A$. Now, for all $a, b \in A$, $\phi(a + b) = \pi_{a+b} = (a + b)x = ax + bx = \pi_a + \pi b$. Also, $\phi(ab) = \pi_{ab} = (ab)x = a(bx) = \pi_a(bx) = \pi_a(\pi_b(x)) = \pi_a\pi_b$. If $\pi_a \in \mathcal{A}$, then we want to find $x \in A$ such that $\phi(x) = \pi_a$. But, as we have $\pi_a \in \mathcal{A}$, for all $a \in A$, then, there exists $a \in A$ such that $x = a$, i.e. $\phi(a) = \pi_a$. Therefore, ϕ is a surjective homomorphism. Now, assume A has no divisors of zero and $\phi(a) = \phi(b)$. That is equivalent to $\pi_a = \pi_b$, i.e. $\pi_a(x) - \pi_b(x) = 0$. That means that $ax - bx = 0$, for all $x \in A$. By distributive law, $(a - b)x = 0$. As A has no divisors of zero, then either $a - b = 0$ (and from that $a = b$ and we are done) or $x = 0$. But, as $(a - b)x = 0$ is for all $x \in A$, it is not necessary that $x = 0$. If it were that $x = 0$ for all $x \in A$, then it would also be $a = 0$ and $b = 0$. In both cases, ϕ is injective. Now, assume $1 \in A$. Then, there exists $\pi_1 \in \mathcal{A}$ such that $\pi_1(x) = 1x = x$. We can see that $\pi_1(\pi_a(x)) = \pi_1(ax) = 1(ax) = ax = \pi_a(x)$. Also $\pi_a(\pi_1(x)) = \pi_a(x)$. Thus, $\pi_1 \in \mathcal{A}$ is unity. Assume $|\ker(\phi)| > 1$. Then there exists $a \in \ker(\phi)$, $a \neq 0$, such that $\phi a = \pi_0$. That would mean that $\pi_a = \pi_0$, i.e. $ax = 0$, for all $x \in A$. But, as also $1 \in A$, then $a \cdot 1 = 0$, i.e. $a = 0$, which is a contradiction. Therefore, $\ker(\phi) = \{0\}$ and ϕ is injective. As it is also surjective, it is bijective, and as it is also a homomorphism, it is an isomorphism.

□

Quotient rings

We will just go through results from group theory, but in additive notation. If A is a ring and $J \trianglelefteq A$, then we define, for any $a \in A$, the right coset of J as the set $J + a = \{j + a : \ j \in J\}$. Then, all results from group theory hold, such as $a \in J + b$ if and only if $J + a = J + b$ if and only if $a - b \in J$. Also, $J + a = J$ if and only if $a \in J$. We will then designate $A/J = \{J + a : \ a \in A\}$.

Theorem. Let $J \trianglelefteq A$. If $J + a = J + c$ and $J + b = J + d$, for some $a, b, c, d \in A$, then:

1. $J + (a + b) = J + (c + d)$.
2. $J + (ab) = J + (cd)$.

Proof. *Ad* 1. As additive group A is an Abelian group, every subgroup of A is normal. Thus, additive J is a normal subgroup of additive group A, and by a previous theorem from group theory we have $J + (a + b) = J + (c + d)$. We will prove it once more to clear things up with additive notation and using the fact that additive A is Abelian (not the fact that additive J is normal; because of that, this proof will be more specific, i.e. less general). As $J + a = J + c$, then $a - c \in J$ and $b - d \in J$. Note that as A is Abelian, we have $a = a + c + (-c) = c + a + (-c) = c + a - c$. Let $j \in J$. Then, $j + (a + b) \in J$. We have $j + (a + b) = j + (c + a - c) + (d + b - d)$. As $a - c \in J$ and $b - d \in J$, there exist $j_1, j_2 \in J$ such that $a - c = j_1$ and $b - d = j_2$. Thus, $j + (a + b) = j + (c + j_1) + (d + j_2) = (j + j_1 + j_2) + (c + d)$. As $J \trianglelefteq A$, then $j + j_1 + j_2 \in J$ so there exists $j_3 \in J$ such that $j_3 = j + j_1 + j_2$ and we have that for all $j \in J$ there exists $j_3 \in J$ such that $j + (a + b) = j_3 + (c + d)$, meaning $J + (a + b) \subseteq J + (c + d)$. Again, let $j \in J$. Then $j + (c + d) \in J + (c + d)$. We have $j+(c+d) = j+(a+c-a)+(b+d-b)$. But, as $a-c \in J$, then there exists $j_1 \in J$ such that $a-c = j_1$. Then, $a-c-j_1 = 0$ and from that $-j_1 = c-a$. Similarly, as $b-d \in J$, there exists $j_2 \in J$ such that $b-d = j_2$. From that we get $b-d-j_2 = 0$, that is, $-j_2 = d-b$. Therefore, $j+(c+d) = j+(a-j_1)+(b-j_2) = (j-j_1-j_2)+(a+b)$. As $J \trianglelefteq A$, then $j - j_1 - j_2 \in J$ so there exists $j_3 \in J$ such that $j - j_1 - j_2 = j_3$. So, for all $j \in J$ there exists $j_3 \in J$ such that $j + (c + d) = j_3 + (a + b)$, meaning $J + (c + d) \subseteq J + (a + b)$. That result, combined with former result, gives us $J + (a + b) = J + (c + d)$.

Ad 2. Let $j \in J$. Then, $j + (ab) \in J + (ab)$. We have $j + (ab) = j + cb + ab - cb = j + cb + (a - c)b$. But, as $a - c \in J$, then also $(a - c)b \in J$, as $J \trianglelefteq A$. Therefore, there exists $j_1 \in J$ such that $j+(ab) = (j+j_1)+(cb)$. Now, $j+(ab) = (j+j_1)+cd+cb-cd = (j + j_1) + cd + c(b - d)$. As $b - d \in J$, then also $c(b - d) \in J$ due to $J \trianglelefteq A$. So, there exists $j_2 \in J$ such that $j + (ab) = (j + j_1 + j_2) + (cd)$. As for all $j \in J$ there exists $j_3 \in J$ (where $j_3 = j + j_1 + j_2$) such that $j + (ab) = j_3 + (cd)$, we

have $J + (ab) \subseteq J + (cd)$. Again, let $j \in J$. Then $j + (cd) \in J + (cd)$. We have $j + (cd) = j + cb + cd - cb = j + (cb) + c(d - b)$. As $b - d \in J$, then there exists $j_1 \in J$ such that $j_1 = b - d$. That gives us $-j_1 = d - b$. Then, as $-j_1 \in J$, we have $d - b \in J$. As $J \trianglelefteq A$, we have $c(d - b) \in J$, i.e. there exists $j_2 \in J$ such that $j_2 = c(d - b)$. We have $j + (c + d) = (j + j_2) + (cb) = (j + j_2) + ab + cb - ab = (j + j_2) + (ab) + (c - a)b$. As $a - c \in J$, then there exists $j_3 \in j$ such that $a - c = j_3$. Now, $-j_3 = c - a$ so $c - a \in J$, and, as $J \trianglelefteq A$, we have $(c - a)b \in J$, i.e. there exists $j_4 \in J$ such that $(c - a)b = j_4$. Finally, $j + (c + d) = (j + j_2 + j_4) + (ab)$. As $j + j_2 + j_4 \in J$, there exists $j_5 \in J$ such that, for all $j \in J$, we have $j + (cd) = j_5 + (ab)$. Thus, $J + (cd) \subseteq J + (ab)$ and, combining that with former subset relation, we have $J + (ab) = J + (cd)$.

□

Theorem. Let A be a ring and $J \trianglelefteq A$. Then, A/J (with coset addition and multiplication defined as above) is a ring.

Proof. The binary operations are well-defined (they are defined for all $J+a \in A/J$, and satisfy the property of uniqueness due to the theorem above). *Additive associativity.* For all $J+a, J+b, J+c \in A/J$, we have $[J+a]+([J+b]+[J+c]) = [J+a]+[J+(b+c)] = J+(a+(b+c)) = J+((a+b)+c) = [J+(a+b)]+[J+c] = ([J+a]+[J+b])+[J+c]$. *Zero.* We have $0 \in A$ and so $J + 0 = J \in A/J$. If $J + a \in A/J$, then $[J + a] + J = [J+a]+[J+0] = J+(a+0) = J+a$. Also, $J+[J+a] = [J+0]+[J+a] = J+(a+0) = J+a$. *Negatives.* If $a \in A$, then $-a \in A$. Then also $J + a \in A/J$ and $J + (-a) \in A/J$. We have $[J + a] + [J + (-a)] = J + (a + (-a)) = J + 0 = J$. Also, $[J + (-a)] + [J + a] = J+(-a+a) = J+0 = J$. Therefore, $-(J+a) = J+(-a)$. *Commutativity.* Let $a, b \in A$. Then, $J+a, J+b \in A/J$ and $[J+a]+[J+b] = J+(a+b) = J+(b+a) = [J+b]+[J+a]$. *Distributivity.* Let $a, b, c \in J$. Then, $[J + a]([J + b] + [J + c]) = [J + a] \cdot [J + (b + c)] = J + (a(b+c)) = J + (ab+ac) = [J + (ab)] + [J + (ac)] = [J + a] \cdot [J + b] + [J + a] \cdot [J + c]$. Also, $([J + a] + [J + b])[J + c] = [J + (a + b)] \cdot [J + c] = J + ((a + b)c) = J + (ac + bc) = [J + (ac)] + [J + (bc)] = [J + a] \cdot [J + c] + [J + b] \cdot [J + c]$. *Multiplicative associativity.* For all $J + a, J + b, J + c \in A/J$, we have $[J + a]([J + b] \cdot [J + c]) = [J + a] \cdot [J + (bc)] = J + (a(bc)) = J + ((ab)c) = [J + (ab)] \cdot [J + c] = ([J + a] \cdot [J + b])[J + c]$.

□

Proposition. Let A be a ring and $J \trianglelefteq A$. Then,

1. If $1 \in A$, then A/J is a ring with unity.
2. If A is commutative, then so is A/J.
3. If A is a field, then so is A/J.

Proof. *Ad* 1. As A is a ring, then by the previous theorem, so is A/J. Now, as $1 \in A$, we have $J+1 \in A/J$. Then, for $a \in A$, $[J+a]\cdot[J+1] = J+(a\cdot 1) = J+a$. Also, $[J+1]\cdot[J+a] = J+(1\cdot a) = J+a$. *Ad* 2. If $ab = ba$, for all $a, b \in A$, then $[J+a]\cdot[J+b] = J+(ab) = J+(ba) = [J+b]\cdot[J+a]$. *Ad* 3. If for every $a \in A$, there exists $a^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$, then, as $a, a^{-1} \in A$, also $J+a, J+(a^{-1}) \in A/J$. We have $[J+a]\cdot[J+(a^{-1})] = J+(aa^{-1}) = J+1$. Also, $[J+(a^{-1})]\cdot[J+a] = J+(a^{-1}a) = J+1$. Therefore, $J+(a^{-1}) = (J+a)^{-1}$. If A has a unity then so does A/J. If A is commutative, then so is A/J. If A has all elements invertible, then so does A/J. In other words, if A is a field, then A/J is a field.

□

Theorem. Let A be a ring and $J \trianglelefteq A$. Then, there exists a homomorphism $f : A \underset{J}{\longrightarrow} A/J$ such that $\operatorname{ran}(f) = A/J$.

Proof. Let $f(x) = J+x$. This function is well-defined, as if $x \in A$, then there exists $J+x \in A/J$ and we have $f(x) = J+x$. Now, if $x = y$, then obviously $J+x = J+y$, i.e. $f(x) = f(y)$. Furthermore, $f(x+y) = J+(x+y) = (J+x)+(J+y) = f(x)+f(y)$ and $f(xy) = J+(xy) = (J+x)(J+y) = f(x)f(y)$. Therefore, f is a homomorphism from A to A/J. It is also surjective, as if we take $J+x \in A/J$, then, $x \in A$, so we have $f(x) = J+x$. Then, also:

$$\ker(f) = \{x \in A :\ f(x) = J\} = \{x \in A :\ J+x = J\} = \{x \in A :\ x \in J\} = J.$$

□

Theorem (FHT for rings). Let A be a ring and $f : A \underset{J}{\longrightarrow} B$ a homomorphism such that $\operatorname{ran}(f) = B$. Then, $A/J \cong B$.

Proof. We have that $\ker(f) \trianglelefteq A$, i.e. $J \trianglelefteq A$, thus A/J is a well-defined group. Let $\phi : A/J \to B$ be a mapping defined with $\phi(J+x) = f(x)$. If we take $J+x \in A/J$, then $x \in A$ and $f(x)$ is well defined by assumption. Also, $J+x = J+y$ implies $x-y \in J$. But, $J = \ker(f)$, so $x-y \in \ker(f)$, i.e. $f(x-y) = 0$. As f is a homomorphism, $f(x)-f(y) = 0$ and we have $f(x) = f(y)$. Therefore, ϕ is well-defined. Now, if $f(x) = f(y)$, we have $f(x)-f(y) = 0$ and, as f is a homomorphism, $f(x-y) = 0$. That means that $x-y \in \ker(f) = J$ which is equivalent to $J+x = J+y$. Thus, ϕ is injective. If we take $y \in B$, then, as $B = \operatorname{ran}(f)$, there exists $x \in A$ such that $f(x) = y$. Therefore, we have $f(x) \in B$, but, as $x \in A$, then $J+x \in A/J$, so $\phi(J+x) = f(x) = y$ and ϕ is surjective. Finally, $\phi((J+x)+(J+y)) = \phi(J+(x+y)) = f(x+y) = f(x)+f(y) = \phi(J+x)+\phi(J+y)$. Similarly, $\phi((J+x)(J+y)) = \phi(J+(xy)) =$

$f(xy) = f(x)f(y) = \phi(J+x)\phi(J+y)$. Thus, ϕ is an isomorphism from A/J to B and we have $A/J \cong B$.

□

Proposition. Let A and B be rings and $J \trianglelefteq A$. If $A/J \cong B$, then there exists a homomorphism $f : A \underset{J}{\longrightarrow} B$ such that $\text{ran}\,(f) = B$.

Proof. From a previous theorem we have that there exists a homomorphism $h : A \underset{J}{\longrightarrow} A/J$ with $h(x) = J + x$. But, as $A/J \cong B$, there exists an isomorphism $g : A/J \longrightarrow B$. If we take $g \circ h : A \to B$, we will prove that $f = g \circ h$ is a homomorphism with $\ker(f) = J$. As g and h are well-defined, so is their composition. Now, $f(x+y) = g(h(x+y)) = g(J+(x+y)) = g((J+x)+(J+y)) = g(J+x)+g(J+y) = g(h(x)) + g(h(y)) = f(x) + f(y)$. Similarly, $f(xy) = g(h(xy)) = g(J + (xy)) = g((J + x)(J + y)) = g(J + x)g(J + y) = g(h(x))g(h(y)) = f(x)f(y)$. Therefore, f is a homomorphism from A to B. But, $\ker(f) = \{x \in A : \ g(h(x)) = e\} = \{x \in A : g(J + x) = e\}$. Then, $J + x \in \ker(g)$. But, as $\ker(g) = \{J\}$, then $J + x \in \{J\}$ so it must be $J + x = J$ i.e. $x \in J$. So, $\ker(f) = \{x \in A : \ x \in J\} = J$.

□

Lemma. Let A be a commutative ring with unity, $J \trianglelefteq A$, $a \in A$ and $K = \{ax - y : (x \in A) \wedge (y \in J)\}$. Then, $K \trianglelefteq A$.

Proof. By definition of K, we have $K \subseteq A$. Then, if we take $ax_1 - y_1, ax_2 - y_2$, we have $(ax_1 - y_1) - (ax_2 - y_2) = ax_1 - y_1 - ax_2 + y_2 = a(x_1 - x_2) - (y_1 - y_2)$ and $(ax_1 - y_1)(ax_2 - y_2) = a^2x_1x_2 - ax_1y_2 - ax_2y_1 + y_1y_2 = a(ax_1x_2 - x_1y_1 - x - 2y_1) - (y_1y_2)$. Thus, as K is closed with respect to subtraction and multiplication, $K \leq A$. Finally, if $ax - y \in K$ and $b \in A$, we have $b(ax - y) = bax - by$. But, as A is commutative, we have $axb - yb = a(xb) - (yb) \in K$ and that means $K \trianglelefteq A$.

□

Theorem. Let A be a commutative ring with unity and $J \trianglelefteq A$. Then, J is a maximal ideal of A if and only if A/J is a field.

Proof. *Necessity.* Let J be a maximal ideal of A and $J + a \in A/J$. We want to prove that A/J is a field, i.e. if $J + a \neq J$ (in field all elements except zero are invertible), there exists $J + x \in A/J$ such that $(J + a)(J + x) = (J + x)(J + a) = J + 1$. Therefore, assume that $J + a \neq J$, i.e. that is it not true that $J + a = J$ (which is equivalent to $a \in J$). That means that it is not true that $a \in J$, i.e. it is true that $a \notin J$. Assume the inverse $J + x$ of $J + a$ does not exist. Then it follows that it cannot be

that $(J+a)(J+x) = J+1$. That expression is equivalent to $J+(ax) = J+1$. After applying $J+(-1)$ on that equality, we get $(J+(ax))+(J+(-1)) = J$ (and reverse). That is equivalent to $J+(ax-1) = J$. So, as $(J+a)(J+x) = J+1$ is equivalent to $J+(ax-1) = J$, i.e. $ax-1 \in J$, and we assumed that $(J+a)(J+x) = J+1$ is impossible, then it must be that $ax-1 \notin J$. Now, let K be defined as in a previous lemma. Then we have $K \trianglelefteq A$. If we take $j \in J$, then, as $j = a0-(-j)$, we have $j = a0-(-j) \in K$, so $J \subseteq K$. But, our condition is that $a \notin J$ and $a = a \cdot 1 + 0$ (as $0 \in J$, taken for y and $1 \in A$, taken for x). Therefore, $a \in K$. So, there exists $a \in K - J$ and that means that $J \subset K \trianglelefteq A$. But, as J is, by assumption maximal ideal, by definition it must be that $K = A$. Therefore, as $1 \in A$, we have $1 \in K$. Then, there exist $x \in A$ and $y \in J$ such that $ax - y = 1$. That is equivalent to $ax - 1 = y$, so it must be that $ax - 1 \in J$, for some $x \in A$. This is contrary to our assumption and it must be that $J + a \neq J$ is invertible. Therefore, A/J is a field.

Sufficiency. Let A/J be a field. Then, at least $1 \in A$ and $1 \neq 0$, so $|A/J| > 1$. From that we have $|A| : |J| > 1$, i.e. $|A| > |J|$. So, we can assume that there exists $K \trianglelefteq A$ such that $J \subset K \subseteq A$. Then, $K \neq \{0\}$. As $J \trianglelefteq A$, $J \subset K \trianglelefteq A$, then $J \trianglelefteq K$, so K/J is a well-defined quotient ring. If we take $J + k \in K/J$, then, as $k \in K \subseteq A$, we have that $J + k \in A/J$, i.e. $K/J \subseteq A/J$. It is evident that, as there exists $k \in K$ (from $K \neq \{0\}$) such that $k \neq 0$. But then as $J + k \in K/J \subseteq A/J$, we have $(J+k)^{-1} = J + (k^{-1}) \in A/J$ and $k^{-1} \in A$. As $K \trianglelefteq A$, we have $kk^{-1} \in K$, i.e. $1 \in K$. That implies that, if $a \in A$, then $a1 \in K$, so $A \subseteq K$ and we have $A = K$, i.e. J is a maximal ideal.

□

Problem. Prove the following:

1. $\mathcal{F}(\mathbb{R})/\{f \in \mathcal{F}(\mathbb{R}) : \ f(0) = f(1) = 0\} \cong \mathbb{R} \times \mathbb{R}$;
2. $\mathcal{F}(\mathbb{R})/\{f \in \mathcal{F}(\mathbb{R}) : \ (\forall x \in \mathbb{Q})(f(x) = 0)\} \cong \mathcal{F}(\mathbb{Q}, \mathbb{R})$.

Solution. *Ad* 1. Let $J = \{f \in \mathcal{F}(\mathbb{R}) : \ f(0) = f(1) = 0\}$. Then, $J \subseteq \mathcal{F}(\mathbb{R})$, by definition. If $f, g \in J$, then, $[f-g](0) = f(0) - g(0) = 0 - 0 = 0$. Also, $[f-g](1) = f(1) - g(1) = 0 - 0 = 0$. Therefore, $f - g \in J$. Then, $[fg](0) = f(0)g(0) = 0 \cdot 0 = 0$ and $[fg](1) = f(1)g(1) = 0 \cdot 0 = 0$. Finally, if $f \in \mathcal{F}(\mathbb{R})$ and $g \in J$, then $[fg](0) = f(0)g(0) = f(0) \cdot 0 = 0$ and $[fg](1) = f(1)g(1) = f(1) \cdot 0 = 0$ (function multiplication is commutative so the same thing is true for gf), so $fg \in J$ and $gf \in J$. Therefore, $J \trianglelefteq \mathcal{F}(\mathbb{R})$. Actually all this was unnecessary as FHT will prove it for us, but hey, it was a more or less fun excercise. Let $\phi : \mathcal{F}(\mathbb{R}) \to \mathbb{R} \times \mathbb{R}$ be a mapping defined with $\phi(f) = (f(0), f(1))$. Then, ϕ is well defined, as every f is a function from $\mathbb{R}$ to $\mathbb{R}$, so it is defined in 0 and in 1. Now, if $f = g$, then $f(x) = g(x)$ for all $x \in \mathbb{R}$. Therefore, $f(0) = g(0)$ and $f(1) = g(1)$, or by definition of ordered pair,

$(f(0), f(1)) = (g(0), g(1))$, i.e. $\phi(f) = \phi(g)$. Now, $\phi(f+g) = ([f+g](0), [f+g](1)) = (f(0)+g(0), f(1)+g(1)) = (f(0), f(1)) + (g(0), g(1)) = \phi(f) + \phi(g)$. Also, $\phi(fg) = ([fg](0), [fg](1)) = (f(0)g(0), f(1)g(1)) = (f(0), f(1))(g(0), g(1)) = \phi(f)\phi(g)$. Now, if we take $(a, b) \in \mathbb{R} \times \mathbb{R}$, then there exists $f \in \mathbb{R} \to \mathbb{R}$ such that $f(0) = a$ and $f(1) = b$ (as $a, b \in \mathbb{R}$). Thus, ϕ is a surjective homomorphism. Also, $\ker(\phi) = \{f : \ \phi(f) = (0,0)\} = \{f : \ (f(0), f(1)) = (0,0)\} = J$. By fundamental homomorphism theorem $\mathcal{F}(\mathbb{R})/J \cong \mathbb{R} \times \mathbb{R}$.

Ad 2. Let $\phi(f) : \mathcal{F}(\mathbb{R}) \to \mathcal{F}(\mathbb{Q}, \mathbb{R})$ be defined with $\phi(f) = f \circ r$, where $r : \mathbb{Q} \to \mathbb{R}$ with $r(x) = f(x)$. We see that r is well defined as, if we take $x \in \mathbb{Q} \subset \mathbb{R}$, then there exists $f(x) \in \mathbb{R}$. Then, composition $f \circ r$ is well-defined as $\mathrm{cod}(r) = \mathrm{dom}(f)$. Then, if $f, g \in \mathcal{F}(\mathbb{R})$ and $f = g$, we have $f(x) = g(x)$. It is obvious, then, that $f(r(x)) = g(r(x))$, i.e. $\phi(f) = \phi(g)$. Now, $\phi(f+g) = [f+g] \circ r$. We see that $[f+g](r(x)) = f(r(x)) + g(r(x))$, so $[f+g] \circ r = f \circ r + g \circ r = \phi(f) + \phi(g)$. Similarly, $\phi(f+g) = [fg] \circ r$ implies $[fg](r(x)) = f(r(x))g(r(x)) = \phi(f)\phi(g)$. If $h \in \mathcal{F}(\mathbb{Q}, \mathbb{R})$, then there exists $h' \in \mathcal{F}(\mathbb{R})$ such that $h(x) = h'(x)$ (as all $x \in \mathbb{Q} \subset \mathbb{R}$). So, $\phi(h') = h \circ r$ (think about it). Therefore, ϕ is a surjective homomorphism. Finally, $\ker(\phi) = \{f \in \mathcal{F}(\mathbb{R}) : \ \phi(f) = 0\} = \{f \in \mathcal{F}(\mathbb{R}) : \ f(r(x)) = 0\}$. As $f(r(x)) = 0$, then, as $r : \mathbb{Q} \to \mathbb{R}$, we have that $f(y) = 0$, for all $y \in \mathbb{Q}$. Therefore, $\ker(\phi) = \{f \in \mathcal{F}(\mathbb{R}) : (\forall x \in \mathbb{Q})(f(x) = 0)\}$. By FHT, $\mathcal{F}(\mathbb{R})/\{f \in \mathcal{F}(\mathbb{R}) : \ (\forall x \in \mathbb{Q})(f(x) = 0)\} \cong \mathcal{F}(\mathbb{Q}, \mathbb{R})$.

Remark. Let A be a ring. Notice that as additive A is Abelian group, we have $n(x+y) = nx + ny$ (same as $(xy)^n = x^n y^n$ for Abelian groups in multiplicative notation), for all $n \in \mathbb{Z}$ and $x, y \in a$.

Problem. Suppose $2x = 0$ for every $x \in A$, where A is a commutative ring. Prove that $(x+y)^2 = x^2 + y^2$ for all $x, y \in A$. Conclude that the function $h(x) = x^2$ is a homomorphism from A to A. If $J = \{x \in A : \ x^2 = 0\}$ and $B = \{x^2 : \ x \in A\}$, explain why $J \trianglelefteq A$, $B \leq A$ and $A/J \cong B$.

Solution. First, $(x+y)^2 = (x+y)(x+y) = x(x+y) + y(x+y) = x^2 + xy + yx + y^2 = x^2 + 2xy + y^2 = x^2 + y^2$. Then, for all $x \in A$, there exists $x^2 \in A$. If $x = y$, then $x^2 = xy$, i.e. $x^2 = y^2$. Then, $h(x+y) = (x+y)^2 = x^2 + y^2 = h(x) + h(y)$ and $h(xy) = (xy)^2 = x^2 y^2 = h(x)h(y)$. We have $\ker(h) = \{x : \ h(x) = 0\}$, i.e. $\ker(h) = \{x : \ x^2 = 0\} = J$. But, h needs to be surjective and it is obvious that $B = \mathrm{ran}(f)$. So, by FHT $A/J \cong B$.

Problem. Suppose $6x = 0$ for every $x \in A$, where A is a commutative ring. Prove that the function $h(x) = 3x$ is a homomorphism from A to A. If $J = \{x : \ 3x = 0\}$ and $B = \{3x : \ x \in A\}$, explain why $J \trianglelefteq A$, $B \leq A$ and $A/J \cong B$.

Solution. For all $x \in A$ we have $3x \in A$. If $x = y$, then $x + x + x = y + y + y$, i.e. $3x = 3y$. Then, $h(x+y) = 3(x+y) = (x+y)+(x+y)+(x+y) = 3x+3y = h(x)+h(y)$ and $h(xy) = 3xy = 3x + 0 = 3xy + 6xy = 3x(y + 2y) = 3x3y = h(x)h(y)$. We have $\text{ran}\,(f) = \{3x : \ x \in A\} = B$ and $\ker(f) = \{x : \ h(x) = 0\} = \{x : \ 3x = 0\} = J$. So, by FHT, $A/J \cong B$.

Problem. If a is an **idempotent** element of commutative ring A (that is, $a^2 = a$), prove that the function $\pi_a(x) = ax$ is a homomorphism from A into A. Show that $\ker(\pi_a) = \text{Ann}\,(a)$. Show that $\text{ran}\,(\pi_a) = \langle a \rangle$. Conclude that $A/\text{Ann}\,(a) \cong \langle a \rangle$.

Solution. For all $x \in A$, $ax \in A$, as $a \in A$. If $x = y$, then, after multiplying by a on the left we have $ax = ay$, i.e. $\pi_a(x) = \pi_a(y)$, so π_a is well-defined. Then, $\pi_a(x + y) = a(x + y) = ax + ay = \pi_a(x) + \pi_a(y)$ and $\pi_a(xy) = a(xy) = a^2xy = axay = \pi_a(x)\pi_a(y)$. Then, $\text{ran}\,(\pi_a) = \{ax : \ x \in A\} = \langle a \rangle$ (principal ideal of A generated by a) and $\ker(f) = \{x \in A : \ ax = 0\} = \text{Ann}\,(a)$. So, by FHT, $A/\text{Ann}\,(a) \cong \langle a \rangle$.

Problem. Let A be a commutative ring. For each $a \in A$, let π_a be the function given by $\pi_a(x) = ax$. Define the following addition and multiplication on $\overline{A} = \{\pi_a : \ a \in A\}$: $\pi_a + \pi_b = \pi_{a+b}$ and $\pi_a\pi_b = \pi_{ab}$ (assume that $\overline{A}$ is a ring). Show that the function $\phi(a) = \pi_a$ is a homomorphism from A onto $\overline{A}$. Show that $A/\text{Ann}\,(A) \cong \overline{A}$.

Solution. For all $a \in A$, π_a is well defined, as shown in the previous problem, so there exists $\pi_a \in A$, for all $a \in A$. Also, uniqueness holds as $a = b$ implies $ax = bx$, i.e. $\pi_a(x) = \pi_b(x)$, for all $x \in A$. Then, $\phi(a + b) = \pi_{a+b} = \pi_a + \pi_b = \phi(a) + \phi(b)$ and $\phi(ab) = \pi_{ab} = \pi_a\pi_b = \phi(a)\phi(b)$. We have $\text{ran}\,(\phi) = \{\pi_a : \ a \in A\} = \overline{A}$ and $\ker(\phi) = \{a \in A : \ \pi_a = \pi_0\}$. But, that means that $\pi_a(x) = \pi_0(x)$, i.e. $ax = 0$, for all $x \in A$. So, $\ker(f) = \{a \in A : \ (\forall x \in A)(ax = 0)\} = \text{Ann}\,(A)$ (as a and x here are interchangeable; the statement is true for all a and for all x). Thus, $A/\text{Ann}\,(A) \cong \overline{A}$.

Proposition. Let A be a ring and $J \trianglelefteq A$. Then,

1. Every element of A/J has a square root iff for every $x \in A$, there is some $y \in A$ such that $x - y^2 \in J$.
2. Every element of A/J is its own negative iff $x + x \in J$ for every $x \in A$.
3. A/J is a boolean ring iff $x^2 - x \in J$ for every $x \in A$.
4. If A is commutative and $J = \{a \in A : \ (\exists n \in \mathbb{N})(a^n = 0)\}$, then $J \trianglelefteq A$ and A/J has no nilpotent elements except zero ($J \in A/J$).
5. Every element of A/J is nilpotent iff for every $x \in A$, there exists $n \in \mathbb{Z}^+$ such that $x^n \in J$.

6. A/J has a unity element iff there exists an element $a \in A$ such that $ax - x \in J$ and $xa - x \in J$, for every $x \in A$.

Proof. *Ad* 1. *Necessity.* Assume that for all $J + x \in A/J$ there exists $J + y \in A/J$ such that $J + x = (J + y)^2$. That implies $J + x = J + y^2$, i.e. $x - y^2 \in J$. *Sufficiency.* Assume that for every $x \in A$ there exists $y \in A$ such that $x - y^2 \in J$. That is equivalent to $J + x = J + y^2$ which is equivalent to $J + x = (J + y)^2$, i.e. for every $J + x \in A/J$ there exists $J + y \in A/J$ such that $J + x = (J + y)^2$. In other words, every element of A/J has a square root.

Ad 2. *Necessity.* Assume that for all $J + x \in A/J$ we have $J + x = -(J + x)$. That is equivalent to $J + x = J + (-x)$, i.e. $x + x \in J$, for all $x \in A$. *Sufficiency.* Assume $x + x \in J$, for every $x \in A$. Then, $J + x = J + (-x)$, i.e. $J + x = -(J + x)$, so every element of A/J is its own negative.

Ad 3. *Necessity.* Assume A/J is a boolean ring. That means that every element is idempotent, i.e. $(J + x)^2 = J + x$, for all $J + x \in A/J$. That is equivalent to $J + (x^2) = J + x$, i.e. $x^2 - x \in J$. *Sufficiency.* Assume $x^2 - x \in J$ for all $x \in A$. Then, $J + (x^2) = J + x$, i.e. $(J + x)^2 = J + x$. That is, every element of A/J is idempotent.

Ad 4. Let $J = \{a \in A : (\exists n \in \mathbb{N})(a^n = 0)\}$. We see that $J \subseteq A$. Now, take $a, b \in J$. We have, by a previous proposition that $a + b$ is nilpotent in commutative rings, so $a + b \in J$. If we take $a \in J$, then there exists $n \in \mathbb{N}$ such that $a^n = 0$. So, if we take $(-a)^{2n} = ((-a)^2)^n = (a^2)^n = (a^n)^2 = 0^2 = 0$, we have that $-a$ is nilpotent and have $-a \in J$. Then, by a previous proposition, if $x \in A$ and $a \in J$, then, as A is commutative, xa is nilpotent and $xa \in J$. So is true for ax (due to commutativity) and we have $ax \in J$. Thus, $J \trianglelefteq A$. Assume there exists $J + a \in A/J$ such that $(J + a)^n = J$, for some $n \in \mathbb{Z}^+$ and $J + a \neq J$. That means that $J + a^n = J$, i.e. $a^n \in J$. But, then there must exist $m \in \mathbb{Z}^+$ such that $(a^n)^m = 0$ and that is equivalent to $a^{nm} = 0$. But, that also means that $a \in J$, so $J + a = J$ which is a contradiction. Therefore, there are no nilpotent elements in A/J except J.

Ad 5. *Necessity.* Assume that for all $J + x \in A/J$ (thus $x \in A$) there exists $n \in \mathbb{Z}^+$ such that $(J + x)^n = J$. That is equivalent to $J + (x^n) = J$, i.e. $x^n \in J$. *Sufficiency.* Assume that for all $x \in A$ there exists $n \in \mathbb{Z}^+$ such that $x^n \in J$. That is equivalent to $J + x^n = J$ and again to $(J + x)^n = J$. Thus, $J + x$ is nilpotent.

Ad 6. *Necessity.* Assume $J + 1 \in A/J$ (and by that $1 \in A$). Then, for all $x \in A/J$, $(J + 1)(J + x) = J + x$ and $(J + x)(J + 1) = J + x$. That is equivalent to $J + (1x) = J + x$ and $J + (x1) = J + x$. Then, that is equivalent to $1x - x \in J$ and $x1 - x \in J$. *Sufficiency.* Assume that for all $x \in A$ exists $a \in A$ such that $ax - x \in J$ and $xa - x \in J$. That is equivalent to $J + (ax) = J + x$ and $J + (xa) = J + x$. That is equivalent to $(J + a)(J + x) = J + x$ and $(J + x)(J + a) = J + x$. Therefore, $J + a$ is a unity in A/J.

□

Definition. Let A be a ring and let $J \trianglelefteq A$. We say that J is a **prime ideal** of A and write $J \trianglelefteq_p A$ if $ab \in J$ implies $a \in J$ or $b \in J$, for all $a, b \in A$.

Theorem. Let A be a commutative ring with unity. Then, $J \trianglelefteq_p A$ if and only if A/J is an integral domain.

Proof. *Necessity.* By a previous proposition we have that A/J is a commutative ring with unity. Assume $J \trianglelefteq_p A$. Then, for all $a, b \in A$, if $ab \in J$, then $a \in J$ or $b \in J$. Now, let $J + a, J + b, J + c \in A/J$ and assume that $J + a \neq J$. Then, $(J + a)(J + b) = (J + a)(J + c)$ is equivalent to $J + (ab) = J + (ac)$ which is equivalent to $J + (ab) - (J + (ac)) = J$. That is, again, equivalent to $J + (ab - ac) = J$, i.e. $J + (a(b - c)) = J$, meaning $a(b - c) \in J$. As $a \in A$, $b - c \in A$, then, as $J \trianglelefteq_p A$, either $a \in J$ or $b - c \in J$. If $a \in J$, then $J + a = J$, which cannot be as we assumed $J + a \neq J$. So, we are only left with $b - c \in J$ which is equivalent to $J + b = J + c$. As $(J + a)(J + b) = (J + a)(J + c)$, where $J + a \neq J$ implies $J + b = J + c$, A/J is an integral domain.

Sufficiency. Assume that A/J is an integral domain. Take $a, b \in A$ such that $ab \in J$. Then, $J + (ab) = J$ and $J + a, J + b \in A/J$. As $J + (ab) = (J + a)(J + b)$ we have $(J + a)(J + b) = J$. As A/J is an integral domain, it has no divisors of zero (zero in A/J is J), so it must be $J + a = J$ or $J + b = J$, i.e. $a \in J$ or $b \in J$. Therefore, $J \trianglelefteq_p A$.

□

Corollary. Every maximal ideal of A is a prime ideal.

Proof. Suppose $J \trianglelefteq A$ is a maximal ideal of A. Then, by a previous theorem, A/J is a field. But, every field is an integral domain, so A/J is also an integral domain. By the previous theorem, $J \trianglelefteq_p A$.

□

Definition. Let A be a ring and $J \trianglelefteq A$. We say that J is a **primary ideal** of A if, for all $a, b \in A$ such that $ab \in J$, then either $a \in J$ or $b^n \in J$ for some $n \in \mathbb{Z}^+$.

Definition. Let A be a ring and $J \trianglelefteq A$. We say that J is a **semiprime ideal** if, for all $a \in A$ such that $a^n \in J$, for some $n \in \mathbb{Z}^+$, it follows that $a \in J$.

Proposition. Let A be a commutative ring with unity and $J \trianglelefteq A$. Then,

1. A/J is a field iff for every $a \in A$, $a \notin J$, there exists $b \in A - J$ such that $ab - 1 \in J$.

2. Element $J + a \in A/J$, $J + a \neq J$ is either invertible or a divisor of zero iff for every $a \in A - J$, there exists $x \in A - J$ such that either $ax \in J$ or $ax - 1 \in J$.

3. Every zero divisor in A/J is nilpotent iff J is a primary ideal.

Proof. *Ad* 1. *Necessity.* Assume A/J is a field. Then, for all $J+a \in A/J$, $J+a \neq J$, there exists $J + b \in A/J - \{J\}$ such that $(J + a)(J + b) = (J + b)(J + a) = J + 1$. That is equivalent to $J+(ab) = J+1$ and that is equivalent to $ab-1 \in J$. *Sufficiency.* Assume that for all $a \in A-J$ exists $b \in A-J$ (then $J+b \neq J$, i.e. $J+b \in A/J-\{J\}$) such that $ab - 1 \in J$. That is equivalent to $J + (ab) = J + 1$ and that is equivalent to $(J + a)(J + b) = J + 1$. As A is a commutative ring, then so is A/J and we have $(J + a)(J + b) = (J + b)(J + a) = 1$. Therefore, A/J is a field.

Ad 2. *Necessity.* Assume that $J + a \in A/J - \{J\}$ is invertible. Then, by result from above, there exists $x \in A$ such that $ax - 1 \in J$. If $J + a$ is a divisor of zero, then there exists $J + x \in A/J - \{J\}$ such that $(J + a)(J + x) = J$. That is equivalent to $J + (ax) = J$, i.e. $ax \in J$. *Sufficiency.* Assume that for all $a \in A - J$ there exists $x \in A - J$ such that $ax \in J$ or $ax - 1 \in J$. If $ax \in J$, then $J + (ax) = J$, i.e. $(J+a)(J+x) = J$. As J is zero in A/J and $J+x, J+a \neq J$, then $J+a$ (and $J+x$) is a divisor of zero. If $ax - 1 \in J$, then by a previous proposition a is invertible.

Ad 3. *Necessity.* Let $a, b \in A$ such that $ab \in J$. That means that $J + (ab) = J$, i.e $(J + a)(J + b) = J$. If $J + a$ is not a divisor of zero, then $J + a = J$ or $J + b = J$, i.e. $a \in J$ or $b \in J$ (same as $b^1 \in J$). If $J + a$ is a divisor of zero, then it is nilpotent by assumption and there exists $n \in \mathbb{Z}^+$ such that $(J + a)^n = J$, i.e. $J + (a^n) = J$. That means $a^n \in J$. Therefore, J is a primary ideal. *Sufficiency.* Assume that J is a primary ideal and that $J + a \in A/J$, $J + a \neq J$ is a divisor of zero. Then, there exists $J + b \in A/J$, $J + b \neq J$ such that $(J + a)(J + b) = J$, which is equivalent to $ab \in J$ (see above). As A is commutative, then so is A/J, so we have $ba \in J$ As J is a primary ideal then either $b \in J$ (impossible as that would mean $J + b = J$, contrary to our assumption), or there exists $n \in \mathbb{Z}^+$ such that $a^n \in J$. Then, $J + a^n = J$, i.e. $(J + a)^n = J$, meaning that $J + a$ is nilpotent.

□

Proposition. Let A be a ring and $J \trianglelefteq A$. Then, J is semiprime if and only if A/J has no nilpotent elements except zero.

Proof. *Necessity.* Assume that J is semiprime ideal of A and that there exists $J+a \in A/J - \{J\}$ and $n \in \mathbb{Z}^+$ such that $(J + a)^n = J$. That implies $J + (a^n) = J$, i.e. $a^n \in J$. But, as J is a semiprime ideal, then we have $a \in J$, i.e. $J + a = J$, which is a contradiction to assumption that $J + a \neq J$. Therefore, there are no nilpotent elements in A/J except zero (which is J). *Sufficiency.* Let A/J have no nilpotent elements except zero, i.e. for all $J + a \in A/J - \{J\}$ there does not exist $n \in \mathbb{Z}^+$ such

that $(J+a)^n = J$. Now, assume $a^m \in J$, for some $m \in \mathbb{Z}^+$. Then, $J + (a^m) = J$, i.e. $(J+a)^m = J$. But that would mean that $J + a$ is nilpotent, but the only nilpotent element is zero so it must be $m = 1$, i.e. $J + a = J$, which is equivalent to $a \in J$. Therefore, J is a semiprime ideal of A.

□

Proposition. An integral domain can have no nonzero nilpotent elements.

Proof. Let A be an integral domain and $a \in A$, $a \neq 0$. We want to prove that there does not exists $n \in \mathbb{Z}^+$ such that $a^n = 0$, i.e. that it cannot be that $a^n = 0$, for any n. We cannot have $a = 0$, as we assumed a is non-zero. We also cannot have $a^2 = 0$ as that is equivalent to $aa = 0$. As A is an integral domain, then it has no divisors of zero and it must be that $a = 0$ or $a = 0$, which is impossible. Now, assume that $a^n = 0$ is impossible. We will show that $a^{n+1} = 0$ is impossible. We have $a^{n+1} = aa^n = 0$. As A is an integral domain, it has no divisors of zero, so either $a = 0$ or $a^n = 0$. But both is impossible so it cannot be that $a^{n+1} = 0$.

□

Proposition. Every prime ideal in a commutative ring is semiprime.

Proof. Let A be a commutative ring and $J \trianglelefteq_p A$. Then, by a previous theorem, A/J is an integral domain and it has no nonzero nilpotent elements. By a previous proposition, as A/J has no nonzero nilpotent elements, J is semiprime.

□

Formal construction of integers modulo n

Remark. Let $n \in \mathbb{Z}$. Notice that $n\mathbb{Z} = \langle n \rangle$ and that, as $\langle n \rangle$ is Abelian and a subgroup of $\mathbb{Z}$ it is a normal subgroup of $\mathbb{Z}$.

Lemma. Let $n, m, k \in \mathbb{Z}$. Then, $n\mathbb{Z} + k = n\mathbb{Z} + (nm + k)$.

Proof. If we take $nx + k \in n\mathbb{Z} + k$, then we must find $y \in \mathbb{Z}$ such that $nx + k = ny + (nm + k)$. From that we have $nx = ny + nm$ and $nx - nm = ny$. That gives us $y = (x - m)$. So, $nx + k = n(x - m) + (nm + k)$. As $(x - m) \in \mathbb{Z}$, then $nx+k = n(x-m)+(nm+k) \in n\mathbb{Z}+(nm+k)$ giving us $n\mathbb{Z}+k \subseteq n\mathbb{Z}+(nm+k)$. If we take $nx+(nm+k) \in n\mathbb{Z}+(nm+k)$, we have $nx+(nm+k) = n(x+m)+k$ which is in $n\mathbb{Z}+k$. Therefore, $n\mathbb{Z}+(nm+k) \subseteq n\mathbb{Z}+k$ which finally gives us $n\mathbb{Z}+(nm+k) = n\mathbb{Z}+k$.

□

Proposition. Let $n \in \mathbb{Z}^+$. Then, $[\mathbb{Z} : n\mathbb{Z}] = n$.

Proof. As $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$ we can define a quotient group $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z} + k : \ k \in \mathbb{Z}\}$. Let $\mathcal{Z} = \{n\mathbb{Z} + k : \ k \in \{0, \ldots, n-1\}\}$. Let $k, l \in \mathbb{Z}$, $k \neq l$ and $0 \leq k, l < n$. Then there exist $n\mathbb{Z} + k, n\mathbb{Z} + l \in \mathcal{Z}$. Suppose $n\mathbb{Z} + k = n\mathbb{Z} + l$. Then, if we take $nx + k \in n\mathbb{Z} + k$, where $x \in \mathbb{Z}$, there exists $y \in \mathbb{Z}$ such that $nx + k = ny + l$. That gives us $n(x - y) = l - k$. From that we have $n|(l - k)$ and then $l \equiv k \pmod{n}$. But, as $0 \leq l, k < n$ it follows by a proposition that $l = k$. That is contrary to our assumption that $k \neq l$ and it has to be $n\mathbb{Z}+k \neq n\mathbb{Z}+l$ and from that we have $|\mathcal{Z}| = n$. Obviously $\mathcal{Z} \subseteq \mathbb{Z}/n\mathbb{Z}$. If we take $n\mathbb{Z} + k \in \mathbb{Z}/n\mathbb{Z}$, then we can use division with remainder theorem to obtain $q, r \in \mathbb{Z}$ such that $k = qn + r$, where $0 \leq r < |n| = n$. Then we have $n\mathbb{Z} + k = n\mathbb{Z} + (nq + r)$. From that, by a previous lemma, we have $n\mathbb{Z} + k = n\mathbb{Z} + r$, where $0 \leq r < n$. That means that $n\mathbb{Z} + r \in \mathcal{Z}$ and we have $\mathbb{Z}/n\mathbb{Z} \subseteq \mathcal{Z}$. That implies $\mathbb{Z}/n\mathbb{Z} = \mathcal{Z}$, but also $|\mathbb{Z}/n\mathbb{Z}| = |\mathcal{Z}| = n$. From that we have $[\mathbb{Z} : n\mathbb{Z}] = |\mathbb{Z}/n\mathbb{Z}| = n$.

□

Proposition. Let $n \in \mathbb{Z}^+$. Then, $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. Let $f : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ with $f([a]_n) = n\mathbb{Z} + a$. We can see that f is defined for all $[a]_n \in \mathbb{Z}_n$. Now, if $[a]_n = [b]_n$, we have $a \equiv b \pmod{n}$. From that we have $n|(a - b)$, i.e. there exists $q \in \mathbb{Z}$ such that $a - b = nq$, that is $a = nq + b$. So, $n\mathbb{Z} + a = n\mathbb{Z} + (nq + b) = n\mathbb{Z} + b$ (by a previous lemma). Therefore, f satisfies the property of uniqueness and is well-defined. *Injectivity.* Suppose $f([a]_n) = f([b]_n)$.

Then, $n\mathbb{Z}+a = n\mathbb{Z}+b$. That means that if we take $nx+a \in n\mathbb{Z}+a$, where $x \in \mathbb{Z}$, there exists $y \in \mathbb{Z}$ such that $ny+b = nx+a$. That gives us $n(y-x) = a-b$, which is equivalent to $n|(a-b)$, i.e. $a \equiv b \pmod{n}$. But, then $a \sim_n b$ and from that $[a]_n = [b]_n$. *Surjectivity.* If we take $n\mathbb{Z}+a \in \mathbb{Z}/n\mathbb{Z}$, we can see that, as $a \in \mathbb{Z}$, we can always find $[a]_n \in \mathbb{Z}_n$ so that $f([a]_n) = n\mathbb{Z}+a$. Finally, $f([a]_n + [b]_n) = f([a+b]_n) = n\mathbb{Z}+(a+b)$. By definition of coset addition, $n\mathbb{Z}+(a+b) = [n\mathbb{Z}+a]+[n\mathbb{Z}+b] = f([a]_n)+f([b]_n)$. Therefore, f is an isomorphism from Z_n to $\mathbb{Z}/n\mathbb{Z}$.

□

Lemma. Let $n \in \mathbb{Z}^*$ and $a, b \in \mathbb{Z}$. Then, $n\mathbb{Z}+a = n\mathbb{Z}+b$ if and only if $a \equiv b \pmod{n}$.

Proof. *Necessity.* Let $n\mathbb{Z}+a = n\mathbb{Z}+b$. Then, if we take $nx+a \in n\mathbb{Z}+a$, there exists $y \in \mathbb{Z}$ such that $ny+b = nx+a$. That is equivalent to $n(y-x) = a-b$ which implies $a \equiv b \pmod{n}$. *Sufficiency.* Let $a \equiv b \pmod{n}$. That means that there exists $q \in \mathbb{Z}$ such that $a-b = nq$, i.e. $a = nq+b$. Then, $n\mathbb{Z}+a = n\mathbb{Z}+(nq+b)$ and, by a previous lemma, $n\mathbb{Z}+(nq+b) = n\mathbb{Z}+b$.

□

Proposition. Let $a, b \in \mathbb{Z}$. Then, $(n\mathbb{Z}+a)\cdot(n\mathbb{Z}+b) = n\mathbb{Z}+(ab)$ is a well-defined binary operation on $\mathbb{Z}/n\mathbb{Z}$.

Proof. Assume $n\mathbb{Z}+a = n\mathbb{Z}+c$ and $n\mathbb{Z}+b = n\mathbb{Z}+d$. Then, by a previous lemma, $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. From a property of congruence we have $ab \equiv cd \pmod{n}$ and that implies, by a previous lemma, $n\mathbb{Z}+(ab) = n\mathbb{Z}+(cd)$. Therefore, binary operation satisfies property of uniqueness (and is well-defined as it is also defined for all $n\mathbb{Z}+a \in \mathbb{Z}/n\mathbb{Z}$, by definition).

□

Remark. From now on we will use notation $\overline{a} = n\mathbb{Z}+a$. E. g., from now on we have $\overline{a}+\overline{b} = \overline{a+b}$ and $\overline{a}\overline{b} = \overline{ab}$. Also, from a previous proposition we have $\overline{a} = \overline{b}$ if and only if $a \equiv b \pmod{n}$.

Proposition. Let $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$. Then, $(\mathbb{Z}/n\mathbb{Z})^*$ with multiplication as defined in the previous proposition is an Abelian group.

Proof. From a previous proposition we have that multiplication is well-defined on $\mathbb{Z}/n\mathbb{Z}$. It carries on uniqueness, but we have to check whether it is closed. Let $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^*$. Then, $\gcd(a,n) = 1$ and $\gcd(b,n) = 1$. It is obvious that $\gcd(ab,n) = 1$ (proof in my work on number theory). From that we have $\overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^*$. *Associativity.*

We have $\overline{a}\left(\overline{b}\overline{c}\right) = \overline{a}\overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab}\overline{c} = \left(\overline{a}\overline{b}\right)\overline{c}$. *Neutral element.* As $\gcd 1, n = 1$, then $\overline{1} \in (\mathbb{Z}/n\mathbb{Z})^*$. Furthermore, $\overline{1}\overline{a} = \overline{1 \cdot a} = \overline{a} = \overline{a \cdot 1} = \overline{a}\overline{1}$. *Inverse element.* From a proposition in my number theory script there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$. From that $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^*$ and $\overline{b}\overline{a} = \overline{a}\overline{b} = \overline{1}$. *Commutativity.* Let $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^*$. Then, $\overline{a}\overline{b} = \overline{ab} = \overline{ba} = \overline{b}\overline{a}$.

□

Proposition. Let $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ and $k \in \mathbb{Z}_0^+$. Then, $(\overline{a})^k = \overline{a^k}$.

Proof. Let $n = 1$. Then, $(\overline{a})^1 = \overline{a}$. Assume that $(\overline{a})^n = \overline{a^n}$. Then, $(\overline{a})^{n+1} = (\overline{a})^n(\overline{a})$. By assumption, we have $(\overline{a})^n(\overline{a}) = \overline{a^n}\overline{a}$. By definition, $\overline{a^n}\overline{a} = \overline{a^n a} = \overline{a^{n+1}}$.

□

Remark. It is obvious that $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$, where φ is Euler's totient function. From that we have $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$. Also, remember that, if G is a group and $a \in G$, then $a^{|G|} = e$. We shall remind ourselves of that through the following lemma, as it will be of great importance to prove next two great theorems.

Lemma. Let G be a group and $a \in G$. Then, $a^{|G|} = e$.

Proof. By a corollary of Lagrange's theorem, we have that $\operatorname{ord}(a)$ divides order of G. Therefore, $|G| = k\operatorname{ord}(a)$, for some $k \in \mathbb{N}$. Then,

$$a^{|G|} = a^{k\operatorname{ord}(a)} = \left(a^{\operatorname{ord}(a)}\right)^k = e^k = e.$$

□

Euler's theorem. Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ where $\gcd(a, m) = 1$. Then,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Proof. As $(\mathbb{Z}/m\mathbb{Z})^*$ contains all $\overline{a}$ such that $\gcd(a, m) = 1$, then, by definition of Euler's totient function, it follows that $|(\mathbb{Z}/m\mathbb{Z})^*| = \varphi(m)$. From a previous lemma, for all $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$, we have (remember that neutral element in $(\mathbb{Z}/m\mathbb{Z})^*$ is $\overline{1}$):

$$(\overline{a})^{\varphi(m)} = \overline{1}.$$

That implies, using a previous proposition:

$$(\overline{a})^{\varphi(m)} = \overline{a^{\varphi(m)}} = \overline{1}.$$

Finally, by a previous proposition, $\overline{a} = \overline{b}$ if and only if $a \equiv b \pmod{m}$, so from $\overline{a^{\varphi(m)}} = \overline{1}$ we get $a^{\varphi(m)} \equiv 1 \pmod{m}$.

□

Fermat's little theorem. For all $a \in \mathbb{Z}$, $m \in \mathbb{N}$ and $p \in P$, $a^{p-1} \equiv 1 \pmod{m}$.

Proof. It follows directly from Euler's theorem and from $\varphi(p) = p - 1$ that $a^{\varphi(p)} \equiv 1 \pmod{m}$, i.e. $a^{p-1} \equiv 1 \pmod{m}$.

□

Theorem. Let $m, n \in \mathbb{Z}^+$ such that $\gcd(m, n) = 1$. Then,

$$\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Proof. Let mapping $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be defined with $f(x) = (m\mathbb{Z}+x, n\mathbb{Z}+x)$. First, we will show that f is a well-defined function. If we take $x \in \mathbb{Z}$, then there exist $m\mathbb{Z} + x \in \mathbb{Z}/m\mathbb{Z}$ and $n\mathbb{Z} + x \in \mathbb{Z}/n\mathbb{Z}$. Then, there also exists $(m\mathbb{Z} + x, n\mathbb{Z} + y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and we have $f(x) = (m\mathbb{Z}+x, n\mathbb{Z}+y)$. Now, assume $x = y$. We then have that $m\mathbb{Z} + x = m\mathbb{Z} + y$ and $n\mathbb{Z} + x = n\mathbb{Z} + y$. From definition of ordered pair, that is equivalent to $(m\mathbb{Z} + x, n\mathbb{Z} + x) = (m\mathbb{Z} + y, n\mathbb{Z} + y)$, i.e. $f(x) = f(y)$. Therefore, f is well-defined. Now, using the fact that coset addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are well-defined, and using the definition of direct product of groups, we have:

$$\begin{aligned} f(x+y) &= (m\mathbb{Z} + (x+y), n\mathbb{Z} + (x+y)) \\ &= ((m\mathbb{Z} + x) + (m\mathbb{Z} + y), (n\mathbb{Z} + x) + (n\mathbb{Z} + y)) \\ &= (m\mathbb{Z} + x, n\mathbb{Z} + x) + (m\mathbb{Z} + y, n\mathbb{Z} + y) = f(x) + f(y). \end{aligned}$$

We also have that:

$$\begin{aligned} f(xy) &= (m\mathbb{Z} + (xy), n\mathbb{Z} + (xy)) \\ &= ((m\mathbb{Z} + x)(m\mathbb{Z} + y), (n\mathbb{Z} + x)(n\mathbb{Z} + y)) \\ &= (m\mathbb{Z} + x, n\mathbb{Z} + x)(m\mathbb{Z} + y, n\mathbb{Z} + y) = f(x)f(y). \end{aligned}$$

That implies that f is a homomorphism. Let us remind ourselves that zero in $\mathbb{Z}/m\mathbb{Z}$ is $m\mathbb{Z} + 0 = m\mathbb{Z}$, as $(m\mathbb{Z} + 0) + (m\mathbb{Z} + x) = m\mathbb{Z} + (0 + x) = m\mathbb{Z} + x$ (commutativity

provides the other condition). So, the zero in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is $(m\mathbb{Z}, n\mathbb{Z})$. Let us observe the kernel of f:

$$\ker(f) = \{x \in \mathbb{Z} : \ f(x) = (m\mathbb{Z}, n\mathbb{Z})\} = \{x \in \mathbb{Z} : \ (m\mathbb{Z} + x, n\mathbb{Z} + x) = (m\mathbb{Z}, n\mathbb{Z})\}.$$

Notice that if $m\mathbb{Z} + x = m\mathbb{Z}$, then $x \in m\mathbb{Z}$. Also, if $n\mathbb{Z} + x = n\mathbb{Z}$, then $x \in n\mathbb{Z}$. That actually means that if $x \in m\mathbb{Z}$ and $x \in n\mathbb{Z}$, then $x = mz_1$ and $x = nz_2$, for some $z_1, z_2 \in \mathbb{Z}$. In other words $m|x$ and $n|x$. That tells us that x is a common multiple of m and n. Therefore $x = k\text{lcm}(m, n)$, for some $k \in \mathbb{Z}$. So, we may write:

$$\begin{aligned} \ker(f) &= \{x \in \mathbb{Z} : \ (\exists k \in \mathbb{Z})(x = k\text{lcm}(m, n))\} \\ &= \{k\text{lcm}(m, n) \in \mathbb{Z} : \ k \in \mathbb{Z}\} = \text{lcm}(m, n)\,\mathbb{Z}. \end{aligned}$$

As $\gcd(m, n) = 1$, then $\text{lcm}(m, n) = mn$ and we have $\ker(f) = (mn)\mathbb{Z}$. To use FHT in the way we want, we need to prove that $\text{ran}(f) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. If we take $(m\mathbb{Z} + y, n\mathbb{Z} + y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, does there exist $x \in \mathbb{Z}$ such that $f(x) = (m\mathbb{Z}+y, n\mathbb{Z}+y)$? That is equivalent to $(m\mathbb{Z}+x, n\mathbb{Z}+x) = (m\mathbb{Z}+y, n\mathbb{Z}+y)$. Let us find the value of $x \in \mathbb{Z}$. From definition of ordered pair equality, we have $m\mathbb{Z}+x = m\mathbb{Z}+y$ and $n\mathbb{Z} + x = n\mathbb{Z} + y$. As $m \in \mathbb{Z}$, then $n\mathbb{Z} + m \in \mathbb{Z}/n\mathbb{Z}$. Also, as $n \in \mathbb{Z}$, then $m\mathbb{Z} + n \in \mathbb{Z}/m\mathbb{Z}$. As $\gcd(m, n) = 1$, $n\mathbb{Z} + m$ has an inverse $(n\mathbb{Z} + m)^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$. Similarly, $m\mathbb{Z} + n$ has an inverse $(m\mathbb{Z} + n)^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*$. Then there exist $m', n' \in \mathbb{Z}$ such that $(m\mathbb{Z} + n)^{-1} = m\mathbb{Z} + n'$ and $(n\mathbb{Z} + m)^{-1} = n\mathbb{Z} + m'$. As $m, m', n, n' \in \mathbb{Z}$ and $y \in \mathbb{Z}$, then $mm'y \in \mathbb{Z}$ and $nn'y \in \mathbb{Z}$ but also $mm'y + nn'y \in \mathbb{Z}$. So, there exist $n\mathbb{Z} + (mm'y + nn'y) \in \mathbb{Z}/n\mathbb{Z}$ and $m\mathbb{Z} + (mm'y + nn'y) \in \mathbb{Z}/m\mathbb{Z}$. Keep in mind that $n\mathbb{Z} + nt = n\mathbb{Z}$ (because $nt \in n\mathbb{Z}$), for all $t \in \mathbb{Z}$ and that $(n\mathbb{Z} + m)(n\mathbb{Z} + m') = (n\mathbb{Z} + m)(n\mathbb{Z} + m)^{-1} = n\mathbb{Z} + 1$. We have:

$$\begin{aligned} n\mathbb{Z} + (mm'y + nn'y) &= (n\mathbb{Z} + (mm')y) + (n\mathbb{Z} + n(n'y)) \\ &= (n\mathbb{Z} + (mm'))(n\mathbb{Z} + y) + n\mathbb{Z} \\ &= (n\mathbb{Z} + m)(n\mathbb{Z} + m')(n\mathbb{Z} + y) + n\mathbb{Z} \\ &= (n\mathbb{Z} + 1)(n\mathbb{Z} + y) + n\mathbb{Z} \\ &= (n\mathbb{Z} + y) + n\mathbb{Z} = n\mathbb{Z} + y. \end{aligned}$$

On the other hand,

$$\begin{aligned} m\mathbb{Z} + (mm'y + nn'y) &= (m\mathbb{Z} + m(m'y)) + (m\mathbb{Z} + (nn')y) \\ &= m\mathbb{Z} + (m\mathbb{Z} + (nn'))(m\mathbb{Z} + y) \\ &= m\mathbb{Z} + (m\mathbb{Z} + n)(m\mathbb{Z} + n')(m\mathbb{Z} + y) \\ &= m\mathbb{Z} + (m\mathbb{Z} + 1)(m\mathbb{Z} + y) \\ &= m\mathbb{Z} + (m\mathbb{Z} + y) = m\mathbb{Z} + y. \end{aligned}$$

We see that if we take $x = mm'y + nn'y$ (where n' and m' are obtained as inverses in $(\mathbb{Z}/m\mathbb{Z})^*$ and $(\mathbb{Z}/n\mathbb{Z})^*$, respectively) we have that $n\mathbb{Z}+x = n\mathbb{Z}+y$ and $m\mathbb{Z}+x = m\mathbb{Z}+y$, i.e. $(m\mathbb{Z} + x, n\mathbb{Z} + x) = (m\mathbb{Z} + y, n\mathbb{Z} + y)$ or more clearly $f(x) = (m\mathbb{Z} + y, n\mathbb{Z} + y)$. Therefore, f is surjective, i.e. $\operatorname{ran}(f) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then, by fundamental homomorphism theorem, we have $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

□

Corollary. Let $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$. Then,

$$(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*.$$

Proof. Follows directly from previous theorem and a proposition from previous chapter.

□

Corollary. Let $m, n \in \mathbb{Z}^+$ and $\gcd(m, n) = 1$. Then, $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. Due to the fact that $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, as follows from the previous corollary, then also:

$$|(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*|.$$

Furthermore, as $\gcd(m, n) = 1$, by the previous theorem we have:

$$\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

A previous proposition implies

$$(\mathbb{Z}/(mn)\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*.$$

Then it follows that

$$|(\mathbb{Z}/(mn)\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*|.$$

So, we have:

$$|(\mathbb{Z}/(mn)\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^*| \cdot |(\mathbb{Z}/n\mathbb{Z})^*|.$$

Finally, by a previous proposition,

$$\varphi(mn) = |(\mathbb{Z}/(mn)\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^*| \cdot |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(m)\varphi(n).$$

□

Corollary. Let $m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$ such that $\gcd(m_i, m_j) = 1$, for all $i \neq j$, $i, j \in \{1, \ldots, k\}$, for some $k \in \mathbb{Z}^+ - \{1\}$. Then,

$$\mathbb{Z}/m_1 m_2 \cdots m_k\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

Proof. In the theorem we have already proved the case when $k = 2$. For $k = 1$ it is trivial. Assume that the statement is true for some $k \in \mathbb{Z}$. Then, we need to prove that the assumption is true for $k + 1$. Using a proposition in direct product chapter which statest that if G, K and H are groups, then $G \cong K$ implies $G \times H \cong G \times K$, and by taking:

$$\begin{aligned} G &= \mathbb{Z}/m_1 m_2 \cdots m_k\mathbb{Z}, \\ K &= \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}, \\ H &= \mathbb{Z}/m_{k+1}\mathbb{Z}, \end{aligned}$$

we get (notice that $G \cong K$ is true because it is the statement of the assumption of induction):

$$\mathbb{Z}/m_1 \cdots m_k\mathbb{Z} \times \mathbb{Z}/m_{k+1}\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}) \times \mathbb{Z}/m_{k+1}\mathbb{Z}.$$

Due to associativity of group operation, the direct product is also associative and the brackets can be dropped on the right-hand side. Now, observing the left-hand side,

as $\gcd(m_{k+1}, m_i) = 1$, for all $i \in \{1, \ldots, k\}$, then $\gcd(m_1 \cdots m_k, m_{k+1}) = 1$. So, by previous theorem we have:

$$\mathbb{Z}/m_1 m_2 \cdots m_k m_{k+1}\mathbb{Z} \cong \mathbb{Z}/m_1 \cdots m_k\mathbb{Z} \times \mathbb{Z}/m_{k+1}\mathbb{Z},$$

Now, due to the transitivity of isomorphism, from that, and the previous expression, we simply obtain:

$$\mathbb{Z}/m_1 m_2 \cdots m_k m_{k+1}\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}/m_{k+1}\mathbb{Z}.$$

□

Corollary. Let $m \in \mathbb{Z}^+$. Then, by fundamental theorem of arithmetic, $m = p_1^{t_1} \cdots p_k^{t^k}$, for some distinct primes $p_1, \ldots, p_k \in P$, integers $t_1, \ldots, t_k, k \in \mathbb{Z}^+$ and:

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\left(p_1^{t_1}\right)\mathbb{Z} \times \cdots \times \mathbb{Z}/\left(p_k^{t_k}\right)\mathbb{Z}.$$

Proof. Due to the fact that p_i are all distinct primes, which further implies that $\gcd(p_i^{t_i}, p_j^{t_j}) = 1$, the previos corollary can be directly applied and the expression easily obtained.

□

Remark. Basically, the previos theorem and it's corollaries are the **Chinese remainder theorem**. It actually states that if:

$$(a_1, \ldots, a_k) \in \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_k\mathbb{Z},$$

then there exists $x_0 \in \mathbb{Z}/m_1 \cdots m_k\mathbb{Z}$ such that $f(x_0) = (a_1, \ldots, a_k)$, where f is an isomorphism defined by $f(x) = (m_1\mathbb{Z} + x, \ldots, m_k\mathbb{Z} + x)$. So, we would have $a_i = m_i\mathbb{Z} + x_0$, i.e. $a_i - x_0 \in m_i\mathbb{Z}$, which is then equivalent to saying $x_0 \equiv a_i \pmod{m_i}$, for all $i \in \{1, \ldots, k\}$. In other words, x_0 is the solution (unique modulo $m_1 \cdots m_k$) to the system of congruences $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_k \pmod{m_k}$.

Proposition. Let $m, n \in \mathbb{N}$. If $m|n$, then $\mathbb{Z}/m\mathbb{Z}$ is a homomorphic image of $\mathbb{Z}/n\mathbb{Z}$.

Proof. Let $m|n$, i.e. $n = mq$, for some $q \in \mathbb{N}$. Let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ with $f(n\mathbb{Z} + x) = m\mathbb{Z} + x$. First, if $n\mathbb{Z} + x = n\mathbb{Z} + y$, then, $x \equiv y \pmod{n}$. But, $n = mq$, so $x \equiv y \pmod{m}q$. From that we have $x - y = mqq'$, where $q' \in \mathbb{Z}$. That is, $x - y = m(qq')$, so $m|x - y$ and $x \equiv y \pmod{m}$. Therefore, $m\mathbb{Z} + x = m\mathbb{Z} + y$,

i.e. $f(n\mathbb{Z}+x) = f(n\mathbb{Z}+y)$. Also, f is defined for all $n\mathbb{Z}+x$, as that implies $x \in \mathbb{Z}$ and that implies that $m\mathbb{Z}+x \in \mathbb{Z}/m\mathbb{Z}$. Now, $f((n\mathbb{Z}+x_1)+(n\mathbb{Z}+x_2)) = f(n\mathbb{Z}+(x_1+x_2)) = m\mathbb{Z}+(x_1+x_2) = (m\mathbb{Z}+x_1)+(m\mathbb{Z}+x_2) = f(n\mathbb{Z}+x_1)+f(n\mathbb{Z}+x_2)$. Also, $f((n\mathbb{Z}+x_1)(n\mathbb{Z}+x_2)) = f(n\mathbb{Z}+x_1x_2) = m\mathbb{Z}+x_1x_2 = (m\mathbb{Z}+x_1)(m\mathbb{Z}+x_2) = f(n\mathbb{Z}+x_1)f(n\mathbb{Z}+x_2)$, for all $x_1, x_2 \in \mathbb{Z}$. Therefore, f is a homomorphism from $\mathbb{Z}/n\mathbb{Z}$ onto $\mathbb{Z}/m\mathbb{Z}$.

□

Proposition. Let $m, n \in \mathbb{N}$. If $m|n$, then $n\mathbb{Z} \trianglelefteq m\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Proof. As $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, then $n\mathbb{Z} \subseteq \mathbb{Z}$. If $nk, nl \in n\mathbb{Z}$, then $nk-nl = n(k-l) \in n\mathbb{Z}$. Also $(nk)(nl) = n(knl) \in n\mathbb{Z}$. If $z \in \mathbb{Z}$, then $z(nk) = (nk)z = n(kz) \in n\mathbb{Z}$. Thus, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, but also $m\mathbb{Z} \trianglelefteq \mathbb{Z}$, due to same reasons. As $m|n$, then $n = mq$, for some $q \in \mathbb{Z}$. Thus, $n\mathbb{Z} = (mq)\mathbb{Z}$. If we take $nk \in n\mathbb{Z}$, then $nk = mqk = m(qk) \in m\mathbb{Z}$. Therefore, $n\mathbb{Z} \subseteq m\mathbb{Z}$. As both $n\mathbb{Z}$ and $m\mathbb{Z}$ are rings, then $n\mathbb{Z} \leq m\mathbb{Z}$. If we take $mk \in m\mathbb{Z}$ and $nl \in n\mathbb{Z}$, then, $(nl)(mk) = (mk)(nl) = n(lmk) \in n\mathbb{Z}$. Therefore, $n\mathbb{Z} \trianglelefteq m\mathbb{Z}$.

□

Remark. Note that, due to the third isomorphism theorem ($(G/H)/(K/H) \cong G/K$), we can prove that $\mathbb{Z}/m\mathbb{Z}$ is a homomorphic image of $\mathbb{Z}/n\mathbb{Z}$ from previous proposition. We have $(\mathbb{Z}/m\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. From corollary of FHT we have that there exists a homomorphism $f : \mathbb{Z}/m\mathbb{Z} \underset{m\mathbb{Z}/n\mathbb{Z}}{\longrightarrow} \mathbb{Z}/n\mathbb{Z}$.

Proposition. Let $n \in \mathbb{Z}^+ - 2\mathbb{Z}$. Then there exists an injective homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/2n\mathbb{Z}$.

Proof. We will define $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2n\mathbb{Z}$ with $f(n\mathbb{Z}+x) = 2n\mathbb{Z}+((n+1)x)$. First we will prove that f is a function. If we take $n\mathbb{Z}+x \in \mathbb{Z}/n\mathbb{Z}$, then we have that $x \in \mathbb{Z}$, but also $(n+1)x \in \mathbb{Z}$. So, there exists $2n\mathbb{Z}+((n+1)x) \in \mathbb{Z}/2n\mathbb{Z}$ and we have $f(n\mathbb{Z}+x) = 2n\mathbb{Z}+((n+1)x)$. Next, $n\mathbb{Z}+x = n\mathbb{Z}+y$ is equivalent to $x \equiv y \pmod{n}$, i.e. there exists $q \in \mathbb{Z}$ such that $x-y = nq$, that is $x = nq+y$. Now, for all $z \in \mathbb{Z}$ we have $2nz+(n+1)x \in n\mathbb{Z}+(n+1)x$. Then:

$$\begin{aligned} 2nz+(n+1)x &= 2nz+(n+1)(nq+y) \\ &= 2nz+n^2q+ny+nq+y \\ &= n(2z+nq+q)+ny+y \\ &= n(2z+q(n+1))+(n+1)y. \end{aligned}$$

Important observation here is that, as n is odd, then $n+1$ is even, i.e. there exists $s \in \mathbb{Z}$ such that $n+1 = 2s$. So,

$$2nz + (n+1)x = n(2z + 2qs) + (n+1)y = 2n(z + qs) + (n+1)y.$$

Take $z' = z + qs$. Obviously $z' \in \mathbb{Z}$ and we have that for all $z \in \mathbb{Z}$ there exists $z' \in \mathbb{Z}$ such that $2nz + (n+1)x = 2nz' + (n+1)y$, meaning $2n\mathbb{Z} + (n+1)x \subseteq 2n\mathbb{Z} + (n+1)y$. Now, for all $z \in \mathbb{Z}$ we have $2nz + (n+1)y \in n\mathbb{Z} + (n+1)x$. From $x - y = nq$ we get $y = x - nq$, i.e. $y = x + n(-q)$. Thus, we have:

$$\begin{aligned} 2nz + (n+1)y &= 2nz + (n+1)(x + n(-q)) \\ &= 2nz + n^2(-q) + nx + n(-q) + x \\ &= n(2z + n(-q) + (-q)) + nx + x \\ &= n(2z + (-q)(n+1)) + (n+1)x. \end{aligned}$$

That again implies, as $2|n+1$ that

$$2nz + (n+1)y = 2nz' + (n+1)x,$$

where $z' = z - q\frac{n+1}{2}$. Thus, we reach that $2n\mathbb{Z} + (n+1)y \subseteq 2n\mathbb{Z} + (n+1)x$. Combining this result with the former one, we get $2n\mathbb{Z} + (n+1)x = 2n\mathbb{Z} + (n+1)y$. Therefore, from $n\mathbb{Z} + x = n\mathbb{Z} + y$ we get $2n\mathbb{Z} + (n+1)x = 2n\mathbb{Z} + (n+1)y$, i.e. $n\mathbb{Z} + x = n\mathbb{Z} + y$ implies $f(n\mathbb{Z}+x) = f(n\mathbb{Z}+y)$. Therefore, f is well-defined. We will prove only injectivity now, as surjectivity obviously does not hold (see motivational example). Assume $f(n\mathbb{Z}+x) = f(n\mathbb{Z} + y)$. By definition of f that is equivalent to $2n\mathbb{Z} + (n+1)x = 2n\mathbb{Z} + (n+1)y$. That is in turn equivalent to $(n+1)x \equiv (n+1)y \pmod{2n}$. As n is odd, $n+1$ is even, i.e. $n+1 = 2m$, for some $m \in \mathbb{Z}$. We then have $2mx \equiv 2my \pmod{2n}$. Then there exists $q \in \mathbb{Z}$ such that $2mx - 2my = 2nq$. That gives us $mx - my = nq$, i.e. $m(x-y) = nq$. Notice that from $n+1 = 2m$ we have that $m|n+1$. If $m = 1$, then we have $x - y = nq$, i.e. $x \equiv y \pmod{n}$. For $m \neq 1$, assume that $\gcd(n, m) \neq 1$. Then there exists $g \in \mathbb{Z}$, $g \neq \pm 1$, such that $g|n$ and $g|m$, i.e. $n = n'g$ and $m = m'g$. Then, $n+1 = 2m$ implies $n'g + 1 = 2m'g$. From that we have $1 = g(2m' - n')$. But, then $g|1$ and it can only be that $g = \pm 1$, contrary to our assumption. Therefore, $|g| = \gcd(m, n) = 1$. Then, $m(x-y) = nq$ implies, by Euclid's lemma, that $n|(x-y)$, i.e. $x \equiv y \pmod{n}$ which is equivalent to $n\mathbb{Z} + x = n\mathbb{Z} + y$. As $f(n\mathbb{Z}+x) = f(n\mathbb{Z}+y)$ implied $n\mathbb{Z} + x = n\mathbb{Z} + y$, we conclude that f is injective. Finally we will show that f is a homomorphism. Somewhat trivial for addition, we have:

$$\begin{aligned} f\left((n\mathbb{Z}+x)+(n\mathbb{Z}+y)\right) &= f\left(n\mathbb{Z}+(x+y)\right) \\ &= 2n\mathbb{Z}+((n+1)(x+y)) = 2n\mathbb{Z}+((n+1)x+(n+1)y) \\ &= (2n\mathbb{Z}+(n+1)x)+(2n\mathbb{Z}+(n+1)y) \\ &= f\left(n\mathbb{Z}+x\right)+f\left(n\mathbb{Z}+y\right). \end{aligned}$$

To prove that f is homomorphism with regard to multiplication, we will need to use the fact[70] that, if n is odd, then $(n+1)^2 \equiv (n+1) \pmod{2}n$. We have:

$$f\left((n\mathbb{Z}+x)(n\mathbb{Z}+y)\right) = f\left(n\mathbb{Z}+(xy)\right) = 2n\mathbb{Z}+((n+1)(xy)).$$

As $(n+1) \in \mathbb{Z}$, and obviously $xy \in \mathbb{Z}$, we have:

$$2n\mathbb{Z}+((n+1)(xy)) = \left(2n\mathbb{Z}+(n+1)\right)\left(2n\mathbb{Z}+xy\right).$$

As $(n+1)^2 \equiv (n+1) \pmod{2}n$, for odd n, then $2n\mathbb{Z}+(n+1) = 2n\mathbb{Z}+((n+1)^2)$. Therefore,

$$\begin{aligned} f\left((n\mathbb{Z}+x)(n\mathbb{Z}+y)\right) &= \left(2n\mathbb{Z}+(n+1)\right)\left(2n\mathbb{Z}+xy\right) \\ &= \left(2n\mathbb{Z}+(n+1)^2\right)\left(2n\mathbb{Z}+xy\right) \\ &= 2n\mathbb{Z}+\left((n+1)^2(xy)\right) \\ &= 2n\mathbb{Z}+((n+1)x\cdot(n+1)y) \\ &= \left(2n\mathbb{Z}+((n+1)x)\right)\left(2n\mathbb{Z}+((n+1)y)\right) \\ &= f\left(n\mathbb{Z}+x\right)f\left(n\mathbb{Z}+y\right). \end{aligned}$$

Therefore, we have proved that f is an injective homomorphism.

□

Remark. Let $a_i \in \mathbb{Z}$, for $i \in \{0,\ldots,n\}$ and $x \in \mathbb{Z}$. Then, if $p = a_n x^n + \cdots + a_1 x + a_0 = 0$ and $f : \hom \mathbb{Z}\mathbb{Z}/m\mathbb{Z}m\mathbb{Z}$ is the projective homomorphism, i.e. defined with $f(x) = m\mathbb{Z}+x$, then $f(p) = f(0)$ implies $f(p) = 0$ (as $f(0) = 0$). Also, $f(p) = m\mathbb{Z}+(a_n x^n+\cdots+a_1 x+a_0) = [m\mathbb{Z}+(a_n x^n)]+\cdots+[m\mathbb{Z}+(a_1 x)]+[m\mathbb{Z}+a_0] = [m\mathbb{Z}+a_n]\cdot[m\mathbb{Z}+x]^n+\cdots+[m\mathbb{Z}+a_1]\cdot[m\mathbb{Z}+x]+[m\mathbb{Z}+a_0] = m\mathbb{Z}$. Therefore, if a polynomial equation is satisfied in $\mathbb{Z}$ it must be satisfied in $\mathbb{Z}/m\mathbb{Z}$. In a much better

[70] Proved in my works on number theory.

notation that can be written as $\overline{a_n} \cdot \overline{x}^n + \cdots + \overline{a_1} \cdot \overline{x} + \overline{a_0} = \overline{0}$ if there is no confusion around m. For an equation to have solutions in $\mathbb{Z}$ it is therefore necessary for it to have solutions in $\mathbb{Z}/m\mathbb{Z}$.

Problem. Prove that the equation $x^2 - 7y^2 - 24 = 0$ has no integer solutions.

Solution. Let us observe that equation in $\mathbb{Z}/7\mathbb{Z}$. We have $\overline{x^2} - \overline{7}\overline{y}^2 - \overline{24} = \overline{0}$. Reducing representatives modulo 7, and as $\overline{7} = \overline{0}$, we have $\overline{x}^2 - \overline{0} \cdot \overline{y}^2 - \overline{3} = \overline{0}$. Then, as $\overline{0} \cdot \overline{y}^2 = \overline{0 \cdot y^2} = \overline{0}$, and as $\overline{x^2} - \overline{0} = \overline{x^2 - 0} = \overline{x^2}$, we have $\overline{x}^2 - \overline{3} = \overline{0}$. We can add to that equation $\overline{3}$ and obtain $\overline{x}^2 = \overline{3}$. Now, obviously $\overline{0}^2 = \overline{0}$ and $\overline{1}^2 = \overline{1^2} = \overline{1} = \overline{36} = \overline{6}$ so they cannot be solutions. Neither can be $\overline{2}$ as $\overline{2}^2 = \overline{4} = \overline{25} = \overline{5}^2$. Furthermore, $\overline{3}^2 = \overline{9} = \overline{2} = \overline{16} = \overline{4}^2$. Thus, we have exhausted all elements of $\mathbb{Z}/7\mathbb{Z}$ and there are no solutions, so there cannot be any in $\mathbb{Z}$.

Remark. Notice this easy but useful fact. Let $m \in \mathbb{Z}^*$. Then, $\overline{a}^{2n} = \overline{m - a}^{2n}$, for all $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ and $n \in \mathbb{N}$. This is true because $\overline{-a} = \overline{m - a}$, i.e. $-\overline{a} = \overline{m - a}$. Therefore, multiplying that equality by itself even number of times gives us $(-1)^{2n}\overline{a}^{2n} = \overline{m - a}^{2n}$. Therefore, we will only need to check first $\left\lceil \frac{m}{2} \right\rceil + 1$ squares.

Problem. Prove that $x^2 + (x+1)^2 + (x+2)^2 = y^2$ has no integer solutions.

Solution. We have $x^2+(x+1)^2+(x+2)^2 = x^2+x^2+2x+1+x^2+4x+4 = 3x^2+6x+5$. So, we must prove that $3x^2 + 6x + 5 = y^2$ has no integer solutions. Luckily for us, $\overline{3} = \overline{6} = \overline{0}$ in $\mathbb{Z}/6\mathbb{Z}$, so we will apply exactly that homomorphism. We then have $\overline{3}\overline{x}^2 + \overline{6}\overline{x} + \overline{5} = \overline{y}^2$. Then, as $\overline{3} = \overline{6} = \overline{0}$ we have $\overline{5} = \overline{y}^2$. Now, we only need to check from $\overline{0}$ to $\overline{3}$. We have $\overline{0}^2 = \overline{6}^2 = \overline{0}$, $\overline{1}^2 = \overline{5}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}^2 = \overline{4}$ and $\overline{3}^2 = \overline{9} = \overline{3}$. As no square in $\mathbb{Z}/6\mathbb{Z}$ equals $\overline{5}$, then there are no solutions in $\mathbb{Z}/6\mathbb{Z}$ and also in $\mathbb{Z}$.

Problem. Let $n \in \mathbb{Z}$. Prove that $x^2 + 10y^2 = n$ has no integer solutions if the last digit of n is 2, 3, 7, or 8.

Solution. We will not only get the last digit of n in $\mathbb{Z}/10\mathbb{Z}$ but also remove $10y^2$ and get $\overline{x}^2 = \overline{n}$. All the squares of integers from 0 to 9 have 0 (0^2), 1 (1^2 or 9^2), 4 (8^2 or 2^2), 5 (5^2), 6 (4^2 and 6^2) or 9 (7^2 or 3^2) for their last digits. Therefore, if $n \in \{2, 3, 7, 8\}$ there cannot be a solution in $\mathbb{Z}/10\mathbb{Z}$ and also not in $\mathbb{Z}$.

Problem. Prove that the sequence $3, 8, 13, 18, 23, \ldots$ does not include the square of any integer.

Solution. We can see that the difference between two neighbour members is 5 and

that this is an arithmetic progression. Therefore, the formula is $a_n = 5n + 3$, for $n \in \mathbb{Z}_0^+$. So, we must show that $x^2 \neq 5n + 3$, for any $n \in \mathbb{Z}_0^+$. Let us assume that it exists. Then, $x^2 = 5n+3$. In $\mathbb{Z}/5\mathbb{Z}$ we have $\overline{x}^2 = \overline{3}$. We have $\overline{0}^2 = \overline{5}^2 = \overline{0}$, $\overline{1}^2 = \overline{4}^2 = \overline{1}$, $\overline{2}^2 = \overline{3}^2 = \overline{4}$. Therefore, there does not exist the square in $\mathbb{Z}/5\mathbb{Z}$ that equals $\overline{3}$ and so it cannot exist in $\mathbb{Z}$. Thus, the sequence above does not include the square of any integer.

Problem. Prove that the sequence $2, 10, 18, 26, \ldots$ does not include the cube of any integer.

Solution. We have the arithmetic sequence $a_n = 8n + 2$, where $n \in \mathbb{Z}_0^+$. We observe $x^3 = 8n + 2$. In $\mathbb{Z}/4\mathbb{Z}$, we have $\overline{x}^3 = \overline{2}$. It cannot be $\overline{0}$, or $\overline{1}$. Now, $\overline{2}^3 = \overline{8} = \overline{0}$ and $\overline{3}^3 = \overline{27} = \overline{3}$. Therefore, there do not exist integers such that $x^3 = 8n + 2$.

Problem. Prove that the sequence $3, 11, 19, 27, ...$ does not include the sum of two squares of integers.

Solution. We have $a_n = 8n + 3$, for $n \in \mathbb{Z}_0^+$. Then, let $x, y \in \mathbb{Z}$. Assume $x^2 + y^2 = 3n + 8$. Let us observe this in $\mathbb{Z}/4\mathbb{Z}$. We have $\overline{x}^2 + \overline{y}^2 = \overline{3}$. We will observe ordered pairs $(\overline{x}, \overline{y})$. Obviously it cannot be for $x, y \in \{0, 1\}$. Now, take $x = 2$. We have $\overline{4} + \overline{y}^2 = \overline{3}$, i.e. $\overline{y}^2 = \overline{3}$. It is obvious that it cannot be in $\mathbb{Z}/4\mathbb{Z}$ (which contains only squares $\overline{0}$ and $\overline{1}$). If $x = 3$, then, $\overline{1} + \overline{y}^2 = \overline{3}$. That is equivalent to $\overline{y}^2 = \overline{2}$. Thus we have exhausted all possibilities and conclude that there do not exist integers such that $x^2 + y^2 = 8n + 3$.

Problem. Prove that if n is a product of two consecutive integers, its units digit must be 0, 2 or 6.

Solution. We have $n = x(x + 1)$, i.e. $n = x^2 + x$. In $\mathbb{Z}/10\mathbb{Z}$ we observe that $\overline{0}^2 + \overline{0} = \overline{9}^2 + \overline{9} = \overline{4}^2 + \overline{4} = \overline{0} = \overline{5}^2 + \overline{5}$. Then, $\overline{1}^2 + \overline{1} = \overline{3}^2 + \overline{3} = \overline{6}^2 + \overline{6} = \overline{8}^2 + \overline{8} = \overline{2}$, $\overline{7}^2 + \overline{7} = \overline{6}$.

Problem. Prove that if n is the product of three consecutive integers, its units digit must be 0, 4 or 6.

Solution. We have $n = x(x + 1)(x + 2)$. In $\mathbb{Z}/10\mathbb{Z}$, $\overline{0 \cdot 1 \cdot 2} = \overline{3 \cdot 4 \cdot 5} = \overline{4 \cdot 5 \cdot 6} = \overline{5 \cdot 6 \cdot 7} = \overline{0}$, $\overline{1 \cdot 2 \cdot 3} = \overline{6 \cdot 7 \cdot 8} = \overline{6}$, $\overline{2 \cdot 3 \cdot 4} = \overline{7 \cdot 8 \cdot 9} = \overline{4}$. The following three contain 10 which is 0 modulo 10, so their product is zero. That exhausts all the cases.

Integral domains

Definition. Let A be a ring. If there exists $n \in \mathbb{Z}^+$ such that $n \cdot a = 0$, and if $m < n$, then $m \cdot a = 0$ implies $m = 0$, for all $m \in \mathbb{Z}_0^+$, then we say that n is the **additive order**[71] of a. If $1 \in A$, the additive order n of 1 is called **characteristic** of A (or we say that ring A has characteristic n) and we write $\operatorname{char}(A) = n$; if there is no $n \in \mathbb{Z}^+$ such that $n \cdot 1 = 0$ then A has characteristic 0 and we write $\operatorname{char}(A) = 0$.

Theorem. All the nonzero elements in an integral domain have the additive order equal to its characteristic.

Proof. Let A be an integral domain and $a \in A$, where $a \neq 0$. We have $a = a1$ and $1 \cdot n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$. Now, $n \cdot a = \underbrace{a1 + a1 + \cdots + a1}_{n \text{ times}}$. By distributive law, that is equivalent to $n \cdot a = a\left(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}\right) = a(n \cdot 1)$. Now, $n \cdot 1 \in A$, $a \in A$ and $n \cdot a \in A$. Assume the additive order of a is n. Then, $n \cdot a = 0$ and $0 = a(n \cdot 1)$. As A is an integral domain it has no divisors of zero. But, as $a \neq 0$, it must be that $n \cdot 1 = 0$. Therefore, the additive order of 1 divides additive order of a. Now, assume additive order of 1 is n. Then, $n \cdot 1 = 0$ and we have $(n \cdot 1)a = 0a = 0$, i.e $n \cdot a = 0$. Therefore, the additive order of a divides additive order of 1 (group theory). From that we have that additive order of a is the same as additive order of 1, i.e. characteristic of A.

□

Remark. From the previous theorem, we have that if A has characteristic n, then $(nk) \cdot a = 0$, for all $a \in A$ and $k \in \mathbb{Z}$.

Theorem. In an integral domain with nonzero characteristic, the characteristic is a prime number.

Proof. Assume $n = km$, for some $k, m \in \mathbb{Z}^+$ and that characteristic of integral domain A is n. Then, $n \cdot 1 = (km) \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{km \text{ times}} = \underbrace{k \cdot 1 + \cdots + k \cdot 1}_{m \text{ times}} = m \cdot (k \cdot 1)$. Then, $m \cdot (k \cdot 1) = 0$ implies that characteristic of $k \cdot 1$ is m. But, by a previous theorem, that means that $m = n$. Then, it must be that $k = 1$. Therefore, n is divisible only by 1 and itself, so it must be $n \in P$.

□

[71] This is analogous to the order of group elements in group theory, so all results here follow for additive groups.

Theorem. In any integral domain A of characteristic p, $(a+b)^p = a^p + b^p$, for all $a, b \in A$.

Proof. We know[72] that $p \equiv \binom{p}{n}$ for all $n \in \mathbb{Z}^+$, $n < p$. Thus, from binomial formula, $(a+b)^p$ contains $\binom{p}{n}$ as a coefficient (with $0 < n < p$) along every member except a^p and b^p (where actually we have $\binom{p}{p}$ and $\binom{p}{0}$). Therefore, all members become zero and only a^p and b^p remain, as $\binom{p}{p} = \binom{p}{0} = 1$.

□

Lemma. Let $n \in \mathbb{Z}^+ - \{1, 2\}$ and let $D = \{0, 1, d_1, \ldots, d_{n-2}\}$ be a finite integral domain. Then, $\pi_d : D \to D$ defined with $\pi_d(x) = dx$ is a bijection for all $d \in D - \{0\}$.

Proof. Let $d \in D - \{0\}$. First we will prove that f is well-defined. If we take $x \in D$, then, as D is closed with respect to multiplication, we have $dx \in D$ and then $\pi_d(x) = dx$. If $x = y$, then, multiplying by d on the left (or right, remember that an integral domain is commutative), we have $dx = dy$, i.e. $\pi_d(x) = \pi_d(y)$, so uniqueness is satisfied. Now, if $\pi_d(x) = \pi_d(y)$, i.e. $dx = dy$, then as $d \neq 0$ and as D is an integral domain, we have that $x = y$, so π_d is injective. The key observation is in the fact that D is finite. By a previous proposition, if $\mathrm{dom}\,(f)$ and $\mathrm{cod}\,(f)$ are finite and $|\mathrm{dom}\,(f)| = |\mathrm{cod}\,(f)|$, then function f is injective if and only if it is surjective. As $\mathrm{dom}\,(\pi_d) = D = \mathrm{cod}\,(\pi_d)$, which is finite, then also $|\mathrm{dom}\,(\pi_d)| = |D| = |\mathrm{cod}\,(\pi_d)|$. We have shown that π_d is an injective function, so it also must be surjective. In other words, $\pi_d : D \to D$ is bijective.

□

Theorem. Any finite integral domain is a field.

Proof. If $D = \{0, 1\}$, then $1 \in D - \{0\}$ is its own inverse and D is a field. Let $n \in \mathbb{Z}^+ - \{1, 2\}$. Let $D = \{0, 1, d_1, \ldots, d_{n-2}\}$ be an integral domain and $d \in D - \{0\}$. Then, by a previous lemma $\pi_d : D \to D$ is a bijection and it has an inverse π_d^{-1}. Let us observe the preimage:

$$\pi_d^{-1}(D) = \{x \in D : \ (\exists y \in D)(\pi_d(x) = y)\}.$$

As π_d is a bijection, so is $\pi_d^{-1}(D)$ and it must be $\mathrm{ran}\left(\pi_d^{-1}\right) = D$, i.e. $\pi_d^{-1}(D) = D$. As $1 \in D$, then there exists $x \in \pi_d^{-1}(D)$ such that $\pi_d(x) = 1$, i.e. $dx = 1$. In other words, d is invertible. Our choice of d was arbitrary, so every $d \in D - \{0\}$ is invertible and, from that, D is a field.

[72] Proof in my works on number theory.

□

Proposition[73]**.** Let D be a finite integral domain and $d \in D - \{0\}$. Then,

1. If $n \cdot d = 0$, where $n \in \mathbb{Z} - \{0\}$, then $\text{char}\,(D) \,|n$.
2. If $\text{char}\,(D) = 0$, $n \in \mathbb{Z} - \{0\}$, and $n \cdot a = 0$, then $a = 0$.

Proof. *Ad* 1. Let $n \in \mathbb{Z} - \{0\}$ and $n \cdot d = 0$. By division with remainder we have $n = q\text{char}\,(D) + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < |\text{char}\,(D)| = \text{char}\,(D)$. Then, $n \cdot d = (q\text{char}\,(D) + r) \cdot d = q(\text{char}\,(D) \cdot d) + r \cdot d = 0$. As $\text{char}\,(D) \cdot d = 0$, then we have $q(\text{char}\,(D) \cdot d) + r \cdot d = r \cdot d$ and from that $r \cdot d = 0$. But, as $r < \text{char}\,(D)$, it can only be that $r = 0$. So, $n = q\text{char}\,(D) + 0 = q\text{char}\,(D)$, i.e. $\text{char}\,(D) \,|n$.

Ad 2. Assume $n \in \mathbb{Z}^+$, $n \cdot a = 0$ and $a \neq 0$. We have $n \cdot a = n \cdot (1a) = (n \cdot 1)a = 0$. As D is an integral domain, it must be that either $a = 0$ or $n \cdot 1 = 0$. But, by our assumption $a \neq 0$, so it must be $n \cdot 1 = 0$. By definition of a characteristic, if $\text{char}\,(D) = 0$, there does not exist $n \in \mathbb{Z}^+$ such that $n \cdot 1 = 0$, so we have a contradiction and it must be that $a = 0$.

By definition, as $\text{char}\,(D) = 0$, there does not exist $n \in \mathbb{Z}^+$ such that $n \cdot a = 0$. So, the only other option is that $a = 0$. If $n < 0$, then we can always take $n \cdot a = (-n) \cdot (-a) = 0$, so we have the same reasoning.

□

Problem. Let D be a finite integral domain. Solve:

1. If $\text{char}\,(D) = 3$, and $5 \cdot a = 0$, for some $a \in D$, then $a = 0$.
2. If there is a nonzero element a in D such that $256 \cdot a = 0$, then $\text{char}\,(D) = 2$.
3. If there are distinct nonzero elements a and b in D such that $125 \cdot a = 125 \cdot b$, then $\text{char}\,(D) = 5$.
4. If there are nonzero elements a and b in D such that $(a + b)^2 = a^2 + b^2$, then $\text{char}\,(A) = 2$.
5. If there are nonzero elements a and b in D such that $10a = 0$ and $14b = 0$, then $\text{char}\,(A) = 2$.

Solution. Notice that in all exercises D is nontrivial, as we assume existence of nonzero elements.

1. *If* $\text{char}\,(D) = 3$*, and* $5 \cdot a = 0$*, for some* $a \in D$*, then* $a = 0$. Assume $a \neq 0$. By previous proposition, as $5 \cdot a = 0$, then $\text{char}\,(D) \,|5$. But $3 \nmid 5$, so it must be $a = 0$.

[73]Results follow from group theory, but I will prove them again, nontheless.

2. *If there is a nonzero element a in D such that $256 \cdot a = 0$, then* $\text{char}\,(D) = 2$. We have $a \neq 0$ and $256 \cdot a = 0$. Then, by previous proposition, $\text{char}\,(D) \,|256$, i.e. $\text{char}\,(D) \,|2^8$. But, we also know that $\text{char}\,(D) \in P$, so it can only be that $\text{char}\,(D) = 2$.

3. *If there are distinct nonzero elements a and b in D such that $125 \cdot a = 125 \cdot b$, then* $\text{char}\,(D) = 5$. We have $125 \cdot a = 125 \cdot b$ and $a \neq b$, $a \neq 0$ and $b \neq 0$. Then, $125 \cdot a - 125 \cdot b = 0$. From this we have $125 \cdot (1a) - 125 \cdot (1b) = 0$, i.e. $(125 \cdot 1)a - (125 \cdot 1)b = 0$. By, distributive law, as $(125 \cdot 1) \in A$, then $(125 \cdot 1)(a - b) = 0$. That is equivalent to $125 \cdot (1(a - b)) = 0$, that is $125 \cdot (a - b) = 0$. If it were that $a - b = 0$, then we would have $a = b$, but we assumed $a \neq b$. So, by previous proposition $\text{char}\,(D) \,|125$, i.e. $\text{char}\,(D) \,|5^3$. This implies, as $\text{char}\,(D) \in P$, that $\text{char}\,(D) = 5$.

4. *If there are nonzero elements a and b in D such that $(a + b)^2 = a^2 + b^2$, then* $\text{char}\,(D) = 2$. We have $(a + b)^2 = a^2 + b^2$. That is equivalent to $a^2 + 2ab + b^2 = a^2 + b^2$, i.e. $2ab = 0$. If it were that $ab = 0$, then we would have, as D is an integral domain and has no divisors of zero, that $a \neq 0$ or $b \neq 0$. But, by assumption $a \neq 0$ and $b \neq 0$. That means that $ab \neq 0$. So, as $2ab = 0$, and $ab \in D$, then, $\text{char}\,(A) \,|2$ and the only possibility, as $\text{char}\,(D) \in P$, is $\text{char}\,(D) = 2$.

5. *If there are nonzero elements a and b in D such that $10a = 0$ and $14b = 0$, then* $\text{char}\,(D) = 2$. We have $\text{char}\,(D) \,|10$ and $\text{char}\,(D) \,|14$. The only common divisor of 10 and 14 is 2, so it must be $\text{char}\,(D) = 2$.

Theorem. Let D be a finite integral domain. Then, $\text{char}\,(D)$ divides $|D|$.

Proof. Let $d \in D$, $d \neq 0$. Then, $\text{char}\,(D) \cdot d = 0$. As additive group D is an Abelian group, then the additive order of d divides $\text{char}\,(D)$. But, as $\text{char}\,(D) \in P$, it can only be that the additive order of d is 1 or $\text{char}\,(D)$. It cannot be 1 as then we would have $d = 0$, so additive order of d is $\text{char}\,(D)$. As additive order of d divides $|D|$, then $\text{char}\,(D)$ divides order of D.

□

Corollary. Let D be a finite integral domain with $|D| = p$, where $p \in P$. Then, $\text{char}\,(D) = p$.

Proof. From the previous theorem we have $\text{char}\,(D)$ divides order of $|D|$, so the only option is $\text{char}\,(D) = 1$ or $\text{char}\,(D) = p$. It cannot be that $\text{char}\,(D) = 1$ as that would imply $1 \cdot 1 = 0$, i.e. $1 = 0$, and we would have $D = \{0\}$, i.e. $|D| = 1$. So it must be that $\text{char}\,(D) = p$.

□

Corollary. Let D be a finite integral domain with $|D| = p^m$, where $p \in P$ and $m \in \mathbb{Z}^+$, then $\text{char}\,(D) = p$.

Proof. We have that $\text{char}\,(D)$ divides $|D|$ and $\text{char}\,(D) \in P$. That is satisfied only by p, so $\text{char}\,(D) = p$.

□

Remark. Let D be a finite integral domain. If $|D| = 81$, then by previous corollary it is obvious that $\text{char}\,(D) = 3$.

Proposition. Let D be a finite integral domain. If additive group D is cyclic, then $|D| \in P$.

Proof. If additive D (assume $|D| = m$, where $m \in \mathbb{Z}^+$) is cyclic, then there exists $d \in D$ such that if $a \in D$, we have $a = n \cdot d$, for some $n \in \mathbb{Z}^+$. We know that $m \cdot d = 0$. Therefore, $\text{char}\,(D)$ divides m and is equal to some $p \in P$. Then, as $\text{char}\,(D) \cdot d = 0$, it must be that additive order of d divides $\text{char}\,(D)$. So, we have $m|p$. Therefore, as $m|p$ and $p|m$ it must be that $m = p$, i.e. $|D| = p \in P$.

□

Proposition. Let A be a finite commutative ring with unity. Then, every $a \in A - \{0\}$ is either a divisor of zero or invertible.

Proof. If $A = \{0, 1\}$, then it is obvious that $1 \in A$ is invertible. Let $n \in \mathbb{Z}^+ - \{1, 2\}$ and $A = \{0, 1, a_1, \ldots, a_{n-2}\}$. Then, $|A| = n$. Let $a \in A - \{0\}$. Let $\pi_a : A \to A$ be defined with $\pi_a(x) = ax$. Then, π_a is a well-defined as $ax \in A$ for all $x \in A$ (due to A being closed with respect to multiplication) and as $x = y$ implies $ax = ay$ (due to uniqueness of binary operation of multiplication). We have that either π_a is injective or is not injective. If π_a is injective, then, as A is finite, it is also surjective, and by that, bijective. Therefore, $\text{ran}\,(f) = A$, so $1 \in \text{ran}\,(f)$ and, as π_a is surjective, there exists $x \in A$ such that $\pi_a(x) = 1$, i.e. $ax = 1$. As it is commutative, $xa = 1$, i.e. a is invertible. Assume π_a is not injective. Then, for some $x, y \in A$, we have that $ax = ay$ and $x \neq y$. From $ax = ay$ it follows that $ax - ay = 0$, i.e. $a(x - y) = 0$. But, as $x \neq y$, then $x - y \neq 0$. Therefore, as also $a \neq 0$, we have that $a \in A - \{0\}$ (and also $x - y \in A - \{0\}$) is a divisor of zero.

□

Lemma. Let A be a ring. If $a \in A - \{0\}$ is not a divisor of zero then a^m is not a divisor of zero and $a^m \neq 0$, for all $m \in \mathbb{Z}^+$.

Proof. If $m = 1$, then obviously $a^1 = a$ is not a divisor of zero and $a^1 = a \neq 0$. Assume a^m is not a divisor of zero and $a^m \neq 0$. We will prove that a^{m+1} is not a divisor of zero and $a^{m+1} \neq 0$. Let $b \in A$ such that $a^{m+1}b = 0$. That is equivalent to $a(a^m b) = 0$. As $a \neq 0$ and a is not a divisor of zero, then $a^m b = 0$. But, as a^m is not a divisor of zero and $a^m \neq 0$, by assumption, then $b = 0$. Therefore, $a^{m+1}b = 0$ implies $b = 0$ (or $a^{m+1} = 0$). Assume $a^{m+1} = 0$. Then, $aa^m = 0$. But, that is impossible as $a \neq 0$ and $a^m \neq 0$ and they are not divisors of zero. So, a^{m+1} is not a divisor of zero and $a^{m+1} \neq 0$.

□

Theorem. Let A be a finite commutative ring with unity. If $a \in A - \{0\}$ is not a divisor of zero, then there exists $m \in \mathbb{Z}^+$ such that $a^m = 1$.

Proof. Let $a \in A - \{0\}$ and $\pi_a : \mathbb{Z}^+ \to A$ be a mapping defined with $\pi_a(x) = a^x$. If $x \in \mathbb{Z}^+$ then $a^x \in A$. If $x = y$, then $x - y = 0$. As $a^0 = 1$, then $a^{x-y} = 1$. Multiplying by a^y gives us $a^x = a^y$. Obviously π_a is a well-defined function. But, ϕ_a cannot be an injection as $\mathbb{Z}^+$ is infinite and A is finite. Therefore, there exist $x, y \in \mathbb{Z}^+$ such that, $a^x = a^y$ and $x \neq y$. Assume $x < y$. Then, $a^x - a^y = 0$ is equivalent to $a^x(1 - a^{y-x}) = 0$. As a is not a divisor of zero, then also a^x is not a divisor of zero and $a^x \neq 0$, by a previous lemma. That implies that $1 - a^{y-x} = 0$. But, that is equivalent to $1 = a^{y-x}$. Taking $m = y - x$ proves the theorem.

□

Corollary. Let A be a finite commutative ring with unity. Then, if $a \in A - \{0\}$ is invertible, there exists $m \in \mathbb{Z}^+$ such that $a^m = a^{-1}$.

Proof. As a is invertible, there exists $a^{-1} \in A - \{0\}$ such that $aa^{-1} = 1$. Assume a is a divisor of zero. Then for some $b \in A$, where $b \neq 0$, we have $ab = 0$. But, as a^{-1} is invertible, we have $a^{-1}ab = a^{-1}0$, i.e. $b = 0$, which is a contradiction. Therefore, a is not a divisor of zero, and so is not a^{-1}. By a previous theorem, there exists $n \in \mathbb{Z}^+$ such that $a^n = 1$. Then, we have $a^{n-1} = a^{-1}$. If $n > 1$, then taking $m = n$ proves the corollary. If it were that $n = 1$, then we would have $a^0 = a^{-1}$, i.e. $a^{-1} = a = 1$. But, as $1^m = 1$, for all $m \in \mathbb{Z}^+$, we have $a^m = a^{-1}$, for all $m \in \mathbb{Z}^+$, so in this case, any positive integer will do for m.

□

Theorem. Let D be an integral domain. Then:

1. Relation $\sim$ defined on $D \times D - \{0\}$ as $(a,b) \sim (c,d)$ if and only if $ad = bc$, for all $a, b \in D$, is an equivalence relation.

2. Let $[a,b] = \{(c,d) \in D \times D - \{0\} : \ ad = bc\}$. Then, $D^* = \{[a,b] : \ (a,b) \in D \times D - \{0\}\}$ with $[a,b] + [c,d] = [ad + bc, bd]$ as addition and $[a,b] \cdot [c,d] = [ac, bd]$ as multiplication[74] is a field. Zero is $[0,1]$ and unity $[1,1]$.

3. Let $D' = \{[a,1] : \ a \in D\}$. Then, $D' \leq D^*$ and $D \cong D'$.

Proof. *Ad* 1. *Reflexivity.* We have $(a,b) \sim (a,b)$ because $ab = ba$ and D is commutative. *Symmetry.* Let $(a,b) \sim (c,d)$. Then, $ad = bc$, but as D is commutative, also $cb = da$, therefore $(c,d) \sim (a,b)$. *Transitivity.* Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then, $ad = bc$ and $cf = de$. Multiplying first equation by f gives us $adf = bcf$. Substituting cf for de gives us $adf = bde$. As D is commutative and associativity holds, that is equivalent to $(af)d = (be)d$. From $d \neq 0$ (because $(c,d) \in D \times D - \{0\}$), as D is an integral domain, then $af = be$, i.e. $(a,b) \sim (e,f)$. Thus, $\sim$ is an equivalence relation.

Ad 2. As $\sim$ is an equivalence relation, then it is obvious that $[a,b] = \{(c,d) \in D \times D - \{0\} : \ (a,b) \sim (c,d)\} = \{(c,d) \in D \times D - \{0\} : \ ad = bc\}$ are its equivalence classes. Let $D^* = \{[a,b] : \ (a,b) \in D \times D - \{0\}\}$. We will show simultaneously that $(D^*, +)$ and $(D^*, \cdot)$ are Abelian groups. *Associativity.* We have $[a,b]([c,d] \cdot [e,f]) = [a,b]([cf + de, df]) = [(df)a + b(cf + de), b(df)] = [adf + bcf + bde, bdf] = [(bd)e + f(ad + bc), (bd)f] = [ad + bc, bd] \cdot [e,f] = ([a,b] \cdot [c,d]) \cdot [e,f]$. Similarly, $[a,b] \cdot ([c,d] \cdot [e,f]) = [a,b] \cdot [ce, df] = [a(ce), b(df)] = [(ac)e, (bd)f] = [ac, bd] \cdot [e,f] = ([a,b] \cdot [c,d]) \cdot [e,f]$. *Neutral elements.* Zero is $[0,1]$ as $[0,1] + [a,b] = [1a + 0b, 1b] = [a,b]$ and $[a,b] + [0,1] = [a1 + 0b, b1] = [a,b]$. Unity is $[1,1]$ because $[1,1] \cdot [a,b] = [a,b] \cdot [1,1] = [a1, b1] = [a,b]$. *Inverse elements.* Inverse of $[a,b]$ in $(D^*, +)$ is $[-a,b]$ (that is, $-[a,b] = [-a,b]$) because $[a,b] + [-a,b] = [ab - ab, b^2] = [0, b^2]$. But, $[0,b^2] \sim [0,1]$ because $01 = b^2 0$, i.e. $0 = 0$. Inverse of $[a,b]$ in $(D^*, \cdot)$ is $[b,a]$ because $[a,b] \cdot [b,a] = [ab, ba]$. It is obvious that $[ab, ba] \sim [1,1]$ because $ab1 = ba1$, i.e. $ab = ab$. *Commutativity.* Both groups are commutative as $[a,b] + [c,d] = [ad + bc, bd] = [cb + ad, db] = [c,d] + [a,b]$ and $[a,b] \cdot [c,d] = [ac, bd] = [ca, db] = [c,d] \cdot [a,b]$. *Distributive law.* We have $[a,b] \cdot ([c,d] + [e,f]) = [a,b] \cdot [cf + de, df] = [a(cf + de), b(df)] = [acf + ade, bdf]$. From the other side, $[a,b] \cdot [c,d] + [a,b] \cdot [e,f] = [ac, bd] + [ae, bf] = [acbf + aebd, b^2 df] = [b(acf) + b(ade), b(bdf)]$. We know that $[acf + ade, bdf] \sim [b(acf + ade), b(bdf)]$ because $(acf + ade) \cdot b(bdf) = (bdf) \cdot b(acf + ade)$, i.e. $(acf + ade)(bdf) = (acf + ade)(bdf)$. Second distributive law holds because of commutativity. Therefore, as $(D^*, +)$ and $(D^*, \cdot)$ are

[74] Notice that the $+$ sign on the left-hand side of definition of addition denotes addition in D^* and on the right-hand side we use addition and multiplication from D; similarly, in the second definition, $\cdot$ on the left-hand side denotes multiplication in D^* and on the right-hand side multiplication in D.

Abelian groups, and multiplication is distributive over addition, then $(D^*, +, \cdot)$ is a field.

Ad 3. If $[a,1] \in D'$, then $(a,1) \in D \times D - \{0\}$, so $[a,1] \in D^*$ and $D' \subseteq D^*$. Let $[a,1],[b,1] \in D'$. Then, $[a,1] - [b,1] = [a,1] + [-b,1] = [a + (-b),1] \in D'$ and $[a,1] \cdot [b,1] = [ab,1] \in D'$, so $D' \leq D^*$, i.e. D' is a subring of D^*. Let $\phi : D \to D'$ be a mapping defined with $\phi(x) = [x,1]$. Then, if we take $x \in D$, there exists $[x,1] \in D'$ and $\phi(x) = [x,1]$. Also, if $x = y$, i.e. $x1 = y1$, then $(x,1) \sim (y,1)$ and $[x,1] = [y,1]$, that is, $\phi(x) = \phi(y)$. Therefore, ϕ is well-defined. Now, if we take $[x,1] \in D'$, obviously there exists $x \in D$ such that $\phi(x) = [x,1]$. If $\phi(x) = \phi(y)$, that is, $[x,1] = [y,1]$, then $(x,1) \sim (y,1)$, i.e. $x1 = 1y$ and $x = y$. Therefore, ϕ is bijective. Let $x, y \in D$. Then, $\phi(x + y) = [x + y, 1] = [x1 + 1y, 1 \cdot 1] = [x,1] + [y,1] = \phi(x) + \phi(y)$ and $\phi(xy) = [xy,1] = [xy, 1 \cdot 1] = [x,1] \cdot [y,1] = \phi(x) \cdot \phi(y)$. In conclusion, $D \cong D'$.

□

Proposition. Let D be an integral domain, $d \in D$ and $p \in P$. Then,

1. If $\operatorname{char}(D) = p$ and $m \in \mathbb{Z}^+$ such that $m \cdot d = 0$, where $p \nmid m$, then $d = 0$.
2. If $p \cdot d = 0$ and $d \neq 0$, then $\operatorname{char}(D) = p$.
3. If $d \neq 0$, $p^m \cdot d = 0$, for some $m \in \mathbb{Z}^+$, then $\operatorname{char}(D) = p$.

Proof. *Ad* 1. Assume $d \neq 0$. Then, by a previous proposition $\operatorname{char}(D) \mid m$, i.e. $p|m$, which is a contradiction to assumption that $p \nmid m$, so it must be that $d = 0$.

Ad 2. Let $d \neq 0$, $p \cdot d = 0$. Assume $\operatorname{char}(D) = q$, where $q \in P$ (as characteristic is a prime number). Then we have $q \cdot d = 0$, but also $q \cdot d - p \cdot d = 0$, i.e. $(q - p)d = 0$. As $d \neq 0$, by assumption, and as D is an integral domain, then $(q - p) = 0$, i.e. $q = p$, which means $\operatorname{char}(D) = p$.

Ad 3. Let $d \neq 0$, $p^m \cdot d = 0$. We have $p \cdot (p^{m-1} \cdot d) = 0$. Obviously $p^{m-1} \in \mathbb{Z}^+$ because $m \in \mathbb{Z}^+$. Therefore, $p^{m-1} \cdot d \in D$, that is to say, there exists $a \in D$ such that $p^{m-1} \cdot d = a$. So, from $p \cdot (p^{m-1} \cdot d) = 0$, we have $p \cdot a = 0$, where $a \neq 0$. Thus, by previous problem, we have $\operatorname{char}(D) = p$.

□

Proposition. Let D be an integral domain. If $|D| = p$, then $D \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. As $|D| = p$ then additive D is cyclic and isomorphic to $\mathbb{Z}/p\mathbb{Z}$. We will show that the generator of additive D is its unity. From a previous theorem (corollary of the theorem, to be more precise), we have that $\operatorname{char}(D) = p$. Let us observe $D' = \{k \cdot 1 : \ k \in \{0, \ldots, p-1\} \subset \mathbb{Z}\}$. Obviously $|D'| \leq p$. Assume $|D'| < p$. Then there exist $k_1 \cdot 1, k_2 \cdot 1 \in D'$, with $k_1, k_2 \in \{0, \ldots, p-1\}$ such that $k_1 \cdot 1 = k_2 \cdot 1$ and

$k_1 \neq k_2$. That is equivalent to $k_1 \cdot 1 - k_2 \cdot 1 = 0$. That implies $(k_1 - k_2) \cdot 1 = 0$. But, as $0 \leq k_1, k_2 < p$, then $0 \leq |k_1 - k_2| < p$. Let $q = k_1 - k_2$. Assume $q \geq 0$. If $q \leq 0$ then we can take $k_2 \cdot 1 - k_1 \cdot 1 = 0$ (by adding negative of $k_1 \cdot 1$ instead of $k_2 \cdot 1$). We then have $q \cdot 1 = 0$. That implies that $q|\text{char}\,(D)$, i.e. $q|p$. But that means that either $q = 1$ or $q = p$. If $q = 1$, then $1 = 0$, making D trivial, i.e. $D = \{0\}$ and $|D| = 1$, and $1 \notin P$, which is a contradiction. Therefore, it must be that $q = p$, but $q < p$, so it is again a contradiction and we have that it must be $q = 0$ (it satisfies $0 \cdot 1 = 0$) which implies $k_1 = k_2$, again a contradiction. Therefore, order of D' cannot be less than p and it can only be that $|D'| = p$. From that we have $|D'| = |D|$. But, if we take $k \cdot 1 \in D'$, for any $k \in \mathbb{Z}$, then $k \cdot 1 \in D$, giving us $D' \subseteq D$. We have $|D'| = |D|$ and $D' \subseteq D$, so it must be $D = D'$. Generator of additive D' is obviously 1, and so generator of D is also 1 (its unity).

Now we can take $f : D \to \mathbb{Z}/p\mathbb{Z}$ with $f(n \cdot 1) = p\mathbb{Z} + n$. Let $x \in D$. As $D = D'$ then there exists $n \cdot 1 \in D'$ such that $x = n \cdot 1$. As $n \in \mathbb{Z}$ then there exists $p\mathbb{Z} + n \in \mathbb{Z}/p\mathbb{Z}$ making $f(x) = f(n \cdot 1) = p\mathbb{Z} + n$. If $n \cdot 1 = m \cdot 1$, then it must be that, due to the same reasoning as above, that $n = m$. So they are also congruent modulo p, i.e. $n - m = 0 \cdot p$, so $p\mathbb{Z} + n = p\mathbb{Z} + m$, i.e. $f(n \cdot 1) = f(m \cdot 1)$. Thus, f is well-defined. Now, if we take $p\mathbb{Z} + n \in \mathbb{Z}/p\mathbb{Z}$ it is obvious that $n \in \mathbb{Z}$. Now, by division with remainder theorem, there exist $q, r \in \mathbb{Z}$ such that $n = qp + r$, where $0 \leq r < |p| = p$. Also, $n = qp + r$ is equivalent to $n - r = qp$, i.e. $n \equiv r \pmod{p}$. That is equivalent to $p\mathbb{Z} + n = p\mathbb{Z} + r$. Therefore, as $r \in \{0, \ldots, p-1\}$, there exists $r \cdot 1 \in D'$ and, as $D' = D$, there exists $x \in D$ such that $x = r \cdot 1$. Thus, $f(x) = f(1 \cdot r) = p\mathbb{Z} + r = p\mathbb{Z} + n$ and f is surjective. If we take $f(n \cdot 1) = f(m \cdot 1)$, then $p\mathbb{Z} + n = p\mathbb{Z} + m$, giving us $n \equiv m \pmod{p}$. But, as $n \cdot 1, m \cdot 1 \in D'$, then $0 \leq n, m < p$. That, combined with $n \equiv m \pmod{p}$ implies $n = m$ and $n \cdot 1 = m \cdot 1$, making f injective and bijective. Now, $f(1 \cdot n + 1 \cdot m) = f(1 \cdot (n+m)) = p\mathbb{Z} + (n+m) = (p\mathbb{Z} + n) + (p\mathbb{Z} + m) = f(1 \cdot n) + f(1 \cdot m)$ and $f((1 \cdot n)(1 \cdot m)) = f(1 \cdot (nm)) = p\mathbb{Z} + (nm) = (p\mathbb{Z} + n)(p\mathbb{Z} + m) = f(1 \cdot n) f(1 \cdot m)$ and f is an isomorphism from D to $\mathbb{Z}/p\mathbb{Z}$, which means that $D \cong \mathbb{Z}/p\mathbb{Z}$.

□

Proposition. Let D be an integral domain with $\text{char}\,(D) = p$, for some $p \in P$, and let $m \in \mathbb{Z}^+$. Then:

1. $(a + b)^{p^m} = a^{p^m} + b^{p^m}$, for all $a, b \in D$.
2. $(a_1 + a_2 + \cdots + a_n)^{p^m} = a_1^{p^m} + a_2^{p^m} + \cdots + a_n^{p^m}$, where $n \in \mathbb{Z}^+$ and $a_1, a_2, \ldots, a_n \in D$.

Proof. *Ad* 1. Let $m = 1$. Then, $(a + b)^p = a^p + b^p$. Assume that $(a + b)^{p^m} = a^{p^m} + b^{p^m}$ for some $m \in \mathbb{Z}^+$. Then, $(a + b)^{p^{m+1}} = (a + b)^{p^m p} = \left((a + b)^{p^m}\right)^p = \left(a^{p^m} + b^{p^m}\right)^p = \left(a^{p^m}\right)^p + \left(b^{p^m}\right)^p = a^{p^{m+1}} + b^{p^{m+1}}$. Therefore, the equality is true for all $m \in \mathbb{Z}^+$.

Ad 2. Let $n = 1$. Then, $(a_1)^{p^m} = a_1^{p^m}$. Assume the statement is true for some $n \in \mathbb{Z}^+$. Then, $(a_1 + \cdots + a_n + a_{n+1})^{p^m}$ can be grouped to have two members, i.e. $((a_1 + \cdots + a_n) + a_{n+1})^{p^m}$. By previous problem, that equals $(a_1 + \cdots + a_n)^{p^m} + a_{n+1}^{p^m}$. By assumption, that is equal to $a_1^{p^m} + \cdots + a_n^{p^m} + a_{n+1}^{p^m}$. That way, we have proved the formula by induction on n.

□

Proposition. Let A and B be integral domains such that $A \subseteq B$ and let $p \in P$. Then, $\operatorname{char}(A) = p$ if and only if $\operatorname{char}(B) = p$.

Proof. *Necessity.* Assume $\operatorname{char}(A) = p$. Then, for all $a \in A - \{0\}$, we have that $p \cdot a = 0$. But, as $a \in B$, due to $A \subseteq B$, we have $p \cdot a = 0$. By previous problem, $\operatorname{char}(B) \mid p$, so it must be that $\operatorname{char}(B) = p$. *Sufficiency.* Let $\operatorname{char}(B) = p$. Take $a \in A - \{0\}$. Then, $a \in B$, so $p \cdot a = 0$. That means that $\operatorname{char}(A) \mid p$ and it must be $\operatorname{char}(A) = p$.

□

Proposition. Every finite field[75] has nonzero characteristic.

Proof. Let F be a field with $|F| = n$ and $\operatorname{char}(F) = 0$. Then, $n \cdot 1 = 0$, but, as $\operatorname{char}(F) = 0$, there cannot, by definition, exist $n \in \mathbb{Z}^+$ such that $n \cdot 1 = 0$. Therefore, it must be $\operatorname{char}(F) \neq 0$.

□

Definition. Let F be a finite field with $\operatorname{char}(F) = p$. The function $f : F \to F$ defined with $f(a) = a^p$ is called a **Froebenius automorphism**.

Lemma. Let D be an integral domain and $p \in P$. If $\operatorname{char}(D) = p$, then $f : D \to D$ defined with $f(d) = d^p$ is a homomorphism from D to D.

Proof. Let $\operatorname{char}(D) = p$, $f : D \to D$ with $f(d) = d^p$. If we take $d \in D$, then due to D being closed with respect to multiplication, $d^p \in D$, so $f(d) = d^p$. If $x = y$, then obviously $x^p = y^p$ (if we multiplied the former equality p times with itself), i.e. $f(x) = f(y)$. Thus, D is well-defined. So, $f(x + y) = (x + y)^p$. By a previous theorem, that is equivalent to $f(x + y) = x^p + y^p = f(x) + f(y)$. Finally, $f(xy) = (xy)^p = x^p y^p = f(x)f(y)$, thus f is a homomorphism from D to D.

□

[75] Due to a previous theorem, F is a finite field if and only if F is a finite integral domain.

Proposition. Froebenius automorphism is an automorphism.

Proof. Let F be a finite field. Then, by a previous proposition it has a nonzero characteristic, which must be, by a previous theorem a prime number. Thus, $\text{char}\,(F) = p$, for some $p \in P$. Then, as every field is also an integral domain, from the previous lemma it follows that $f : F \to F$ defined with $f(a) = a^p$ is a homomorphism from F to F.

Injectivity. We won't pay much attention to what $\ker(f)$ is, but how it relates to F. We know that $\ker(f) \trianglelefteq F$. So, assume f is not injective, i.e. $\ker(f) \neq \{0\}$. Then, there exists $a \in \ker(f)$ such that $a \neq 0$. But, all $a \in F - \{0\}$ are invertible, so there exists $a^{-1} \in F$ such that $aa^{-1} = 1$. As $\ker(f)$ is an ideal of F, for all $x \in F$ and $y \in \ker(f)$ we must have $xy \in \ker(f)$ and $yx \in \ker(f)$. Therefore, as $a \in \ker(f)$, and $a^{-1} \in F$, then aa^{-1} and $a^{-1}a$ are in $\ker(f)$. That is, $1 \in \ker(f)$. But, then, if $a \in F$, it also must be that $1 \cdot a \in \ker(f)$, i.e. $a \in \ker(f)$. Therefore, $F \subseteq \ker(f)$ which implies $F = \ker(f)$. That would mean that $f(x) = 0$ for all $x \in F$, but at least $f(1) = 1^p = 1$. Therefore, there does not exist $a \in \ker(f) - \{0\}$ and it must be that $\ker(f) = \{0\}$. So, if we take $f(x), f(y) \in \text{ran}\,(f)$, then, $f(x) = f(y)$ implies $f(x) - f(y) = 0$. But, as f is a homomorphism, that is equivalent to $f(x - y) = 0$. That means that $x - y \in \ker(f)$ and, as $\ker(f) = \{0\}$, it can only be that $x - y = 0$, i.e. $x = y$. Therefore, f is injective.
Surjectivity. As F is finite and $|F| = |\text{dom}\,(f)| = |\text{cod}\,(f)|$, and as F is an injective function, then F is also surjective. That means that f is a bijective homomorphism, i.e. an isomorphism. As it is an isomorphism from F to F it is an automorphism on F.

□

Corollary. Let $p \in P$. In a finite field of characteristic p, every element has a p-th root.

Proof. Let F be a finite field and $\text{char}\,(F) = p$. Let $y \in F$. We want to prove that there exists $x \in F$ such that $x^p = y$. Let us observe Froebenius automorphism on F (that we can as we're dealing with a finite field with characteristic p). We have $f : F \to F$ with $f(x) = x^p$ and we know that f is an automorphism (but also a surjection). Then, if we take $y \in F$, we have $y \in \text{ran}\,(f) = F$, and there exists $x \in F$ such that $f(x) = y$, i.e. $x^p = y$.

□

The integers

Definition. Let D be an integral domain and $<$ a relation on D such that for all $a, b, c \in D$:

1. $a < b$, $b < a$ or $a = b$;
2. $a < b$ and $b < c$ implies $a < c$;
3. $a < b$ implies $a + c < b + c$;
4. $0 < c$ and $a < b$ imply $ac < bc$.

Then, D with relation $<$, is called an **ordered integral domain**. Also, we say that $<$ is an **order relation** on D.

Remark. We will just note that $a \leq b$ means $a < b$ or $a = b$.

Definition. Let D be an ordered integral domain and $d \in D$. Then, if $d > 0$, we say that d is **positive**, and if $d < 0$ we say that d is **negative**.

Proposition. Let D be an ordered integral domain and $a, b \in D$. Then, $a < b$ if and only if $-b < -a$.

Proof. *Necessity.* Let $a < b$. Then we can add $-a$ on both sides to get $a - a < b - a$, i.e. $0 < b - a$. Then, we can add $-b$ on both sides and get $0 - b < b - a - b$, which is equivalent to $-b < -a$. *Sufficiency.* Let $-b < -a$. Then we add a and b on both sides and get $-b + a + b < -a + a + b$, i.e. $a < b$.

□

Remark. From the previous proposition we have that if a is positive, then $-a$ is negative, and if a is negative, then $-a$ is positive. That follows from $0 < a$ implies $-a < -0$, i.e. $-a < 0$, and from $a < 0$ implies $-0 < -a$, that is, $0 < -a$.

Proposition. The square of every non-zero element in an ordered integral domain is positive. Also, unity is always positive.

Proof. Let D be an ordered integral domain and $d \in D - \{0\}$. Assume $0 < d$. Then, multiplying that equality by d (that we can because $0 < d$) gives us $0d < dd$, which is equivalent to $0 < d^2$. Assume $d < 0$. Then, by previous proposition, $0 < -d$, and multiplying that by $-d$ (possible because $0 < -d$) gives us $-d0 < (-d)(-d)$, i.e. $0 < d^2$. So, $0 < d^2$, for all $d \in D - \{0\}$, but so it is true for $1 \in D - \{0\}$, i.e. $0 < 1^2$. But, $1^2 = 1$, so $0 < 1$.

□

Proposition. Let D be an ordered integral domain. Then, for every $n \in \mathbb{Z}$ we have $n \cdot 1 < (n+1) \cdot 1$.

Proof. From the previous proposition we have that $0 < 1$. As $n \cdot 1 \in D$, then adding it to both sides gives us $n \cdot 1 < 1 + n \cdot 1$. That is, $n \cdot 1 < 1 \cdot 1 + n \cdot 1$ which is equivalent[76] to $n \cdot 1 < (1+n) \cdot 1$.

□

Remark. Let D be an ordered integral domain. Then we denote the set of all positive elements in D as:

$$D^+ = \{d \in D : \ d > 0\}.$$

Definition. Let D be an ordered integral domain. If there exists $d \in D^+$ such that $d \leq x$, for all $x \in D^+$, we say that D has a **well-ordering property**. Also, an ordered integral domain with well-ordering property is called an **integral system**.

Proposition. In any integral system, there is no element between[77] zero and unity.

Proof. Let D be an integral system. Assume that there exists $x \in D$ such that $0 < x < 1$. Then the set $A = \{x \in D : \ 0 < x < 1\}$ is non-empty and, due to well-ordering of D, there exists $a \in A$ such that $a \leq x$ for all $x \in A$. But, also $0 < a < 1$, i.e. $0 < a$ and $a < 1$. As $0 < a$, we can multiply both equalities to get $0 < a^2$ and $a^2 < a$, i.e. $0 < a^2 < a$. But, $a^2 < a$ is a contradiction to well-ordering on D and A must be empty.

□

Proposition. Characteristic of an ordered integral domain is zero.

Proof. Assume that there exists $n \in \mathbb{Z}^+$ such that $n \cdot 1 = 0$. But, due to a previous proposition, we have $0 < 1 < 2 \cdot 1 < \ldots < n \cdot 1$, then, $0 < n \cdot 1$, so that is a contradiction and there cannot exist $n \in \mathbb{Z}^+$ such that $n \cdot 1 = 0$ and by definition, characteristic of an ordered integral domain is zero.

[76] Be careful to notice that in $1 \cdot 1$, first 1 is integer and second 1 is unity in D. We kind of use ambiguous notation, but I will either clarify them more in a finished version, or make it unambiguous by using 1_D to denote unity in D (and also 0_D to denote zero in D).

[77] No element greater than zero and less than unity, to be more precise.

□

Proposition. Every integral system is isomorphic to $\mathbb{Z}$.

Proof. Let D be an integral system. Let $D' = \{x \in D : (\exists n \in \mathbb{Z})(x = n \cdot 1)\}$. First, we will show that $D = D'$. If we take $x \in D'$, then obviously $x \in D$ and we have $D' \subseteq D$. Now, let us take $x \in D$. Assume that $x \neq n \cdot 1$, for any $n \in \mathbb{Z}$. Then, as by a previous proposition, for all $n \cdot 1, (n+1) \cdot 1 \in D'$ we have $n \cdot 1 < (n+1) \cdot 1$, then there must exist $m \in \mathbb{Z}$ such that $m \cdot 1 < x < (m+1) \cdot 1$, i.e. $m \cdot 1 < x$ and $x < (m+1) \cdot 1$. Latter inequality can be written as $x < m \cdot 1 + 1$. Now, adding $-m \cdot 1$ on both sides on both inequalities, gives us $m \cdot 1 - m \cdot 1 < x - m \cdot 1$ and $x - m \cdot 1 < m \cdot 1 + 1 - m \cdot 1$, respectively. But, those two inequalities are equivalent to $0 < x - m \cdot 1$ and $x - m \cdot 1 < 1$, i.e. $0 < x - m \cdot 1 < 1$. As $x - m \cdot 1 \in D$, and D has a well-ordering property, there cannot be an element between zero and unity. Therefore there does not exist $x \in D$ such that $x \notin D'$ and we have $D \subseteq D'$, combined with a previous result that is $D = D'$.

Now, an obvious isomorphism is $f : D \to \mathbb{Z}$ defined with $f(n \cdot 1) = n$. That function is well-defined due to reasoning above and because $n \cdot 1 = m \cdot 1$ implies $n \cdot 1 - m \cdot 1 = 0$ and $(n-m) \cdot 1 = 0$. As $\text{char}\,(D) = 0$ and $1 \neq 0$ in integral domain, then it must be $n - m = 0$, that is $n = m$. Thus, f satisfies property of uniqueness. If we take $n \in \mathbb{Z}$ then obviously $n \cdot 1 \in D$ due to D being closed with respect to addition (here successive addition, n times). Finally, if $f(n \cdot 1) = f(m \cdot 1)$, then $n = m$. But, that obviously implies $n \cdot 1 = m \cdot 1$ and f is a bijection. Now, $f(n \cdot 1 + m \cdot 1) = f((n+m) \cdot 1) = n + m = f(n \cdot 1) + f(m \cdot 1)$ and $f((n \cdot 1)(m \cdot 1)) = f((nm) \cdot 1) = nm = f(n \cdot 1) f(m \cdot 1)$ and f is an isomorphism from D to $\mathbb{Z}$.

□

Theorem. Let $S \subseteq \mathbb{Z}^+$. If:

1. $1 \in S$,
2. $s \in S$ implies $s + 1 \in S$, for all $s \in S$,

then, $S = \mathbb{Z}^+$.

Proof. Let $T = \mathbb{Z}^+ - S$. Assume $T \neq \emptyset$. Then, as $T \subseteq \mathbb{Z}^+$, and $\mathbb{Z}^+$ has a well-ordering property, there exists $m \in T$ such that $m \leq t$ for all $t \in T$. Also, as $1 \in S$, then $1 \notin T$ and $m \neq 1$, i.e. $1 < m$. From that we have $0 < m - 1$, so $m - 1 \in \mathbb{Z}^+$. Assume $m - 1 \notin S$. Then, it must be that $m - 1 \in T$ (as $T = \mathbb{Z}^+ - S$, i.e. it contains all elements of $\mathbb{Z}^+$ that are not in S). As $m - 1 \in T$ and $m \in T$, and also $m - 1 < m$, it is a contradiction to m being the least element. Therefore, $m - 1 \in S$. But, as $m - 1 \in S$, by assumption we also have $m - 1 + 1 \in S$, i.e. $m \in S$, which is a contradiction to $m \in T$ (i.e. $m \in \mathbb{Z}^+$ and $m \notin S$). Therefore, it must be that $T = \emptyset$ and from that we have $S = \mathbb{Z}^+$.

□

Theorem (principle of mathematical induction). Assume the following:

1. Statement S_1 is true.
2. For all $k \in \mathbb{Z}^+$, statement S_k is true implies statement S_{k+1} is true.

Then, statement S_n is true for all $n \in \mathbb{Z}^+$.

Proof. Let T be a set of all integers for which statement is true. Then, $1 \in T$. Also, if $t \in T$, then also $t + 1 \in T$, as truth of statement S_t implies truth of S_{t+1}. Then, by previous theorem $T = \mathbb{Z}^+$, i.e. statement S_n is true for all $n \in \mathbb{Z}^+$.

□

Problem. Let D be an ordered integral domain. Prove the following, for all a, b and c in D:

1. If $a \leq b$ and $b \leq c$, then $a \leq c$;
2. If $a \leq b$, then $a + c \leq b + c$;
3. If $a \leq b$ and $c \geq 0$, then $ac \leq bc$;
4. If $a < b$ and $c < 0$, then $bc < ac$;
5. If $a + c < b + c$, then $a < b$;
6. If $ac < bc$ and $c > 0$ then $a < b$;
7. If $a < b$ and $c < d$, then $a + c < b + d$.

Solution.

1. *If $a \leq b$ and $b \leq c$, then $a \leq c$.* Let $a \leq b$ and $b \leq c$. Then, $a < b$ or $a = b$ and $b < c$ or $b = c$. Assume $a < b$. If $b < c$ then, by definition, $a < c$. If $b = c$, then by substitution, $a < c$. Assume $a = b$. If $b < c$, then by substitution $a < c$. If $b = c$, then $a = c$. Therefore, if $a \leq b$ and $b \leq c$ then $a < c$ or $a = c$, i.e. $a \leq c$.
2. *If $a \leq b$, then $a + c \leq b + c$.* Let $a \leq b$. That means $a < b$ or $a = b$. Assume $a < b$. Then, by definition $a + c < b + c$. If $a = b$, then by adding c we get $a + c = b + c$. Therefore, if $a \leq b$, then $a + c < b + c$ or $a + c = b + c$, that is $a + c \leq b + c$.

3. *If $a \leq b$ and $c \geq 0$, then $ac \leq bc$.* Let $a \leq b$ and $0 \leq c$, i.e. $a < b$ or $a = b$ and $0 < c$ or $0 = c$. Assume $a < b$. If $0 < c$, by definition, $ac < bc$. If $c = 0$, then $a \cdot 0 = 0$ and $b \cdot 0 = 0$, so $a0 = b0$, i.e. $ac = bc$. Assume $a = b$. Then, multiplying by c gives us $ac = bc$. So, $a \leq b$ and $0 \leq c$ implies $ac < bc$ or $ac = bc$, which means $ac \leq bc$.

4. *If $a < b$ and $c < 0$, then $bc < ac$.* If $c < 0$, then $0 < -c$, by a previous proposition. That implies $a(-c) < b(-c)$, i.e. $-ac < -bc$. But, due to a previous proposition, that implies $bc < ac$.

5. *If $a + c < b + c$, then $a < b$.* Let $a + c < b + c$. Using $-c$ in the definition gives us $(a + c) - c < (b + c) - c$, which means $a + (c - c) < b + (c - c)$. That is equivalent to $a + 0 < b + 0$, i.e. $a < b$.

6. *If $ac < bc$ and $c > 0$ then $a < b$.* Let $ac < bc$ and $0 < c$. Assume $a \geq b$. Then, as $c > 0$ we have $ac \geq bc$. But, that is in contradiction with $ac < bc$. Therefore, it must be $a < b$.

7. *If $a < b$ and $c < d$, then $a + c < b + d$.* We have $a < b$ and $c < d$, i.e. $a - b < 0$ and $0 < d - c$, respectively. That implies $a - b < d - c$, and after adding $b + c$ we get $(a - b) + (b + c) < (d - c) + (b + c)$, which is due to associativity and commutativity equivalent to $a + c < b + d$.

Problem. Let D be an ordered integral domain. Prove the following, for all a, b and c in D:

1. $a^2 + b^2 \geq 2ab$;

2. $a^2 + b^2 \geq ab$ and $a^2 + b^2 \geq -ab$;

3. $a^2 + b^2 + c^2 \geq ab + bc + ac$;

4. $a^2 + b^2 > ab$, if $a^2 + b^2 \neq 0$;

5. $a + b < ab + 1$, if $a, b > 1$;

6. $ab + ac + bc + 1 < a + b + c + abc$, if $a, b, c > 1$.

Solution.

1. $a^2 + b^2 \geq 2ab$. The square of any non-zero element in D is positive. Assume $(a - b) \in D - \{0\}$. Then, $(a - b)^2 > 0$. That is equivalent to $a^2 - 2ab + b^2 > 0$. After adding $2ab$ on both sides, by definition, we have $a^2 - 2ab + b^2 + 2ab > 0 + 2ab$, that is, $a^2 + b^2 > 2ab$. Now, if $(a - b) = 0$, then $(a - b)^2 = 0(a - b)$, i.e. $(a - b)^2 = 0$. From that we have $a^2 - 2ab + b^2 = 0$, which is $a^2 + b^2 = 2ab$. Therefore, $a^2 + b^2 > 2ab$ or $a^2 + b^2 = 2ab$, so $a^2 + b^2 \geq 2ab$.

2. $a^2 + b^2 \geq ab$ *and* $a^2 + b^2 \geq -ab$. Assume $ab \geq 0$. Then, $ab + ab \geq ab$ and we have $2ab \geq ab$. Therefore, as $a^2 + b^2 \geq 2ab$ and $2ab \geq ab$, we have $a^2 + b^2 \geq ab$. Assume $ab < 0$. As $a^2 \geq 0$ and $b^2 \geq 0$, then $a^2 + b^2 \geq 0$, by a previous problem. If $a^2 + b^2 > 0$, then, as $0 > ab$, we have $a^2 + b^2 > ab$. If $a^2 + b^2 = 0$, then by substitution $a^2 + b^2 > ab$. So, $a^2 + b^2 \geq ab$. Assume $ab \geq 0$. Then, $0 \geq -ab$ and we have $ab \geq -ab$. Assume $ab > 0$. Then, $0 > -ab$ and we have $ab > -ab$. Therefore $ab \geq -ab$, so $a^2 + b^2 \geq ab$ and $ab \geq -ab$ gets us $a^2 + b^2 \geq -ab$.

3. $a^2 + b^2 + c^2 \geq ab + bc + ac$. We know that $a^2 + b^2 \geq 2ab$, $b^2 + c^2 \geq 2ab$ and $a^2 + c^2 \geq 2ac$. By previous problem, we can add those three inequalities to get $a^2 + b^2 + b^2 + c^2 + a^2 + c^2 \geq 2ab + 2bc + 2ac$, i.e. $2a^2 + 2b^2 + 2c^2 \geq 2ab + 2bc + 2ac$. By distributive law that is equivalent to $2(a^2 + b^2 + c^2) \geq 2(ab + bc + ac)$. That is, again equivalent to $2 \cdot (1(a^2 + b^2 + c^2)) \geq 2 \cdot (1(ab + bc + ac))$. Then, that is $(2 \cdot 1)(a^2 + b^2 + c^2) \geq (2 \cdot 1)(ab + bc + ac)$. As $2 \cdot 1 \in D$, and $0 < 1 < 2 \cdot 1$, then $2 \cdot 1 > 0$ implies that $a^2 + b^2 + c^2 \geq ab + bc + ac$.

4. $a^2 + b^2 > ab$, *if* $a^2 + b^2 \neq 0$. Proof by contraposition. Let $a^2 + b^2 \leq ab$. But, by a previous proposition, we have $a^2 + b^2 \geq ab$. So it can only be $a^2 + b^2 = ab$. Then, $(a - b)^2 \geq 0$ implies $a^2 - 2ab + b^2 \geq 0$. That is, $a^2 - 2a^2 - 2b^2 + b^2 \geq 0$, by substitution, i.e. $-a^2 - b^2 \geq 0$. From that we have $-(a^2 + b^2) \geq 0$. That can only be if $a^2 + b^2 = 0$.

5. $a + b < ab + 1$, *if* $a, b > 1$. From $a > 1$ and $b > 1$ we have $a - 1 > 0$ and $b - 1 > 0$. So, we can multiply $a - 1 > 0$ by $b - 1$ to get $(a - 1)(b - 1) > 0$. That is, $ab - a - b + 1 > 0$. From that we have $ab + 1 > a + b$.

6. $ab + ac + bc + 1 < a + b + c + abc$, *if* $a, b, c > 1$. From $a > 1$, $b > 1$ and $c > 1$ we have $a - 1 > 0$, $b - 1 > 0$ and $c - 1 > 0$. We can multiply $a - 1 > 0$ by $b - 1$ and then by $c - 1$ to get $(a - 1)(b - 1)(c - 1) > 0$. That is equivalent to $(ab - a - b + 1)(c - 1) > 0$, that is $abc - ab - ac + a - bc + b + c - 1 > 0$ That means $abc + a + b + c > ac + bc + ab + 1$.

Definition. Let D be an ordered integral domain. Then, for all $d \in D$ we define **absolute value of** d as:

$$|d| = \begin{cases} d, & d \geq 0, \\ -d, & d < 0. \end{cases}$$

Problem. Let D be an ordered integral domain and $a, b \in D$. Prove:

1. $|-a| = |a|$;

2. $a \leq |a|$;

3. $a \geq -|a|$;

4. If $b > 0$, $|a| \leq b$ iff $-b \leq a \leq b$;

5. $|a + b| \leq |a| + |b|$;

6. $|a - b| \leq |a| + |b|$;

7. $|ab| = |a| \cdot |b|$;

8. $|a| - |b| \leq |a - b|$;

9. $||a| - |b|| \leq |a - b|$.

Solution.

1. $| - a| = |a|$. Assume $a \geq 0$. Then, $-a \leq 0$, so $| - a| = -(-a) = a$. Also, as $a \geq 0$, by definition $|a| = a$. Therefore $a \geq 0$ implies $| - a| = |a|$. Assume $a < 0$. Then, $-a > 0$ so $| - a| = -a$. Also, as $a < 0$, then by definition $|a| = -a$ and we have $|a| = -a = | - a|$. In conclusion, $| - a| = |a|$.

2. $a \leq |a|$. Assume $a \geq 0$. Then $|a| = a$. Assume $a < 0$. Then, $|a| = -a$. But, as $a < 0$, then $0 < -a$, and we have $0 < |a|$ by substitution and $a < |a|$. In conclusion, we have $a = |a|$ or $a < |a|$ so $a \leq |a|$.

3. $a \geq -|a|$. Assume $a \geq 0$. Then, $|a| = a$, and, if we add $-(a + |a|)$ on both sides, we get $-|a| = -a$. But, we know that $a \geq 0$, and then $0 \geq -a$, so $a \geq -a$. By substituting $-|a|$ for $-a$ we get $a \geq -|a|$. If $a < 0$ then $|a| = -a$, and after adding $a - |a|$ on both sides, we have $a = -|a|$. Therefore, $a \geq -|a|$.

4. *If $b > 0$, $|a| \leq b$ iff $-b \leq a \leq b$.* Let $b > 0$. *Necessity.* Let $|a| \leq b$. Assume $a \geq 0$. Then, $|a| = a$ and we have $a \leq b$. But, also $b > 0$, and, as $a \geq 0$, then, if $a > 0$, we have $a + b > 0$. If $a = 0$, then $0 + b > 0$, i.e. $a + b > 0$. From that we have $a > -b$. We can loosen our claim by saying $a \geq -b$. Therefore, if $a \geq 0$ we have $-b \leq a$ and $a \leq b$, which means $-b \leq a \leq b$. If $a < 0$, then $|a| = -a$ and we have $-a \leq b$. That is equivalent to $-b \leq a$. Therefore, we have $-b \leq a$. But, as $a < 0$ and $0 < b$, we have $a < b$ and we can loosen that by saying $a \leq b$. Therefore, if $a < 0$ we again obtain $-b \leq a \leq b$. *Sufficiency.* Let $-b \leq a$ and $a \leq b$. Assume $a \geq 0$. Then, $|a| = a$ and we have $|a| \leq b$. Assume $a < 0$. Then we have $|a| = -a$. But, as $-b \leq a$ we have $-a \leq b$, from which we get $|a| \leq b$. Therefore, $|a| \leq b$.

5. $|a + b| \leq |a| + |b|$. Assume $a, b \geq 0$. Then, $a + b \geq 0$ and we have $|a + b| = a + b$. Also, as $a \geq 0$ we have $|a| = a$ and, as $b \geq 0$, we have $|b| = b$. So, $a + b = |a| + |b|$. Therefore, $|a + b| = |a| + |b|$. Assume $a \geq 0$ and $b < 0$. Assume $a \geq -b$. Then,

$a+b \geq 0$ and we have $|a+b| = a+b$. On the other hand, we have $|a| = a$ and $|b| = -b$. So, $|a| + |b| = a + (-b)$. As $b < 0$ we have $0 < -b$ so $b < -b$. After adding a on both sides we get $a+b < a-b$, i.e. $|a+b| < |a|+|b|$. Assume $a < -b$. Then, $a+b < 0$ and we have $|a+b| = -a-b$. Also, we have $|a|+|b| = a+(-b)$. But, as $a \geq 0$ and $0 \geq -a$, then $a \geq -a$, so we have $a - b \geq -a - b$, which means $|a| + |b| \geq |a+b|$, i.e. $|a+b| \leq |a| + |b|$. The same proof goes for $a < 0$ and $b \geq 0$, the difference is in notation. Assume $a, b < 0$. Then, $a + b < 0$ and we have $|a+b| = -(a+b) = -a-b$. We also have $|a| = -a$ and $|b| = -b$, so $|a| + |b| = -a - b$. And, from that we have $|a+b| = |a| + |b|$. In conclusion, we had $|a+b| = |a| + |b|$ or $|a+b| < |a| + |b|$ or $|a+b| \leq |a| + |b|$, which is actually $|a+b| \leq |a| + |b|$ by definition.

6. $|a-b| \leq |a| + |b|$. We have $|a + (-b)| \leq |a| + |-b|$, by previous problem. But, $|-b| = |b|$, so $|a + (-b)| \leq |a| + |b|$, i.e. $|a-b| \leq |a| + |b|$.

7. $|ab| = |a| \cdot |b|$. Assume $a, b \geq 0$. Then, $ab \geq 0$ and we have $|ab| = ab$. But, also $|a| = a$ and $|b| = b$, so, $|ab| = |a| \cdot |b|$. Assume $a \geq 0$ and $b < 0$. Then, $-b > 0$. If $a > 0$, then $-ab > 0$. Therefore, $ab < 0$, and we have $|ab| = -ab$. On the other hand, $|a| = a$ because $a \geq 0$, and $|b| = -b$ as $b < 0$. So, $|a| \cdot |b| = -ab$ and we have $|ab| = |a| \cdot |b|$. If $a = 0$, then $|0b| = |0| = 0$ and $|0| \cdot |b| = 0b = 0$ and that is $|ab| = |a| \cdot |b|$. Assume $a, b < 0$. Then, $-a > 0$ and $-b > 0$ so, $-a(-b) > 0$, i.e. $ab > 0$. From that we have $|ab| = ab$. Also, $|a| = -a$ and $|b| = -b$, so $|a| \cdot |b| = -a(-b) = ab$. Therefore, $|ab| = |a| \cdot |b|$ in this case, and in all cases (we only didn't check $a < 0$ and $b \geq 0$, but that is analogous to the $a \geq 0$ and $b < 0$ with a difference in notation).

8. $|a| - |b| \leq |a-b|$. Assume $a, b \geq 0$. Assume $a \geq b$. Then, $a - b \geq 0$ and we have $|a-b| = a-b$. Also, $|a| = a$ and $|b| = b$, so $|a| - |b| = a - b$. Thus, $|a-b| = |a| - |b|$. Assume $a < b$. Then, $a - b < 0$ and $|a-b| = -(a-b) = b-a$. But, $|a| = a$ and $|b| = b$, so $|a| - |b| = a - b$. We know that $a - b < 0$, so $0 < b - a$, i.e. $a - b < b - a$ and we have $|a| - |b| < |a-b|$. Assume $a \geq 0$ and $b < 0$. Then, $a \geq 0$ and $-b > 0$, so $a - b > 0$, i.e. $|a-b| = a-b$. Also, $|a| = a$ and $|b| = -b$ and we have $|a| - |b| = a + b$. We know that $b < 0$ and $0 < -b$ so $b < -b$ and, after adding a on both sides, $a + b < a - b$. Then, $|a| - |b| < |a-b|$. Assume $a < 0$ and $b \geq 0$. Then, $-a > 0$ and $b - a > 0$. From that we have $a - b < 0$ and $|a-b| = b-a$. Also, $|a| = -a$ and $|b| = b$, and $|a| - |b| = -a - b$. Now, as $-b < b$, we have $-a - b < b - a$, i.e. $|a| - |b| < |a-b|$. Assume $a, b \leq 0$. Then, $-b \geq 0$. Assume $a \geq b$. Then, $a - b \geq 0$ and we have $|a-b| = a-b$. Also, $|a| = -a$ and $|b| = -b$ and we have $|a| - |b| = -a + b$. As $a - b \geq 0$, then $0 \geq b - a$ and we have $a - b \geq b - a$, i.e. $|a-b| \geq |a| - |b|$, which is $|a| - |b| \leq |a-b|$. Assume $a < b$. Then, $a - b < 0$ and we have $|a-b| = b-a$. Also, $|a| = -a$ and $|b| = -b$ and

$|a| - |b| = -a + b$. In this case, $|a| - |b| = |a - b|$. That exhausts all possibilities, and in each case we have $|a| - |b| = |a - b|$ or $|a| - |b| < |a - b|$. By definition, that is $|a| - |b| \leq |a - b|$.

9. $||a| - |b|| \leq |a - b|$. Assume $|a| \geq |b|$. Then, $|a| - |b| \geq 0$ and we have $||a| - |b|| = |a| - |b|$ and by previous problem, $|a| - |b| \leq |a - b|$, so $||a| - |b|| \leq |a - b|$, by substitution. Assume $|a| < |b|$. Then, $|a| - |b| < 0$ and we have $||a| - |b|| = |b| - |a|$. But, by previous problem, $|b| - |a| \leq |b - a|$. But, also $|b| - |a| \leq |-(a - b)|$. By a previous problem, $|-(a - b)| = |a - b|$, so $|b| - |a| \leq |a - b|$. Thus, we have $|b| - |a| \leq |a - b|$, i.e. $||a| - |b|| \leq |a - b|$.

Problem. Let A be a ring, $a, b \in A$ and $m, n \in \mathbb{Z}^+$. If $1 \cdot a = a$ and $n \cdot a + a = (n+1) \cdot a$, prove:

1. $n \cdot (a + b) = n \cdot a + n \cdot b$;
2. $(n + m) \cdot a = n \cdot a + m \cdot a$;
3. $(n \cdot a)b = a(n \cdot b) = n \cdot (ab)$;
4. $m \cdot (n \cdot a) = (mn) \cdot a$;
5. $n \cdot a = (n \cdot 1_A)a$;
6. $(n \cdot a)(m \cdot b) = (nm) \cdot (ab)$.

Solution.

1. $n \cdot (a + b) = n \cdot a + n \cdot b$. Let $n = 1$. Then, by assumption, $1 \cdot (a + b) = a + b = 1 \cdot a + 1 \cdot b$. Then, if the formula is true for n, we have, for $n + 1$, by definition $(n + 1) \cdot (a + b) = n \cdot (a + b) + (a + b)$, and when using the assumption and basis, $n \cdot (a + b) + (a + b) = n \cdot a + n \cdot b + a + b = n \cdot a + a + n \cdot b + b = (n + 1) \cdot a + (n + 1) \cdot b$.

2. $(n + m) \cdot a = n \cdot a + m \cdot a$. Let $m = 1$. Then, by definition, $(n + 1) \cdot a = n \cdot a + a = n \cdot a + 1 \cdot a$. Assuming formula is true for m, we have $(n + (m + 1)) \cdot a = ((n + m) + 1) \cdot a = (n + m) \cdot a + a$. Using the assumption, we have $(n + m) \cdot a + a = n \cdot a + m \cdot a + a = n \cdot a + (m + 1) \cdot a$.

3. $(n \cdot a)b = a(n \cdot b) = n \cdot (ab)$. Let $n = 1$. Then, $(1 \cdot a)b = ab = a(1 \cdot b) = 1 \cdot (ab)$. If formulae are true for n, then $((n + 1) \cdot a)b = (n \cdot a + a)b = (n \cdot a)b + ab$. From this we have, using the assumption of induction, $(n \cdot a)b + ab = a(n \cdot b) + ab = a(n \cdot b + b) = a((n + 1) \cdot b)$. Also, $(n \cdot a)b + ab = n \cdot (ab) + ab = (n + 1) \cdot ab$, by definition.

4. $m \cdot (n \cdot a) = (mn) \cdot a$. Let $m = 1$. Then, $1 \cdot (n \cdot a) = n \cdot a = (n \cdot 1) \cdot a$. If formula is true for m, then for $m + 1$ we have $(m + 1) \cdot (n \cdot a) = m \cdot (n \cdot a) + n \cdot a$, by definition. Using the assumption we have $m \cdot (n \cdot a) + n \cdot a = (mn) \cdot a + n \cdot a$. By previous problem, that is $(mn) \cdot a + n \cdot a = (mn + n) \cdot a = ((m + 1)n) \cdot a$.

5. $n \cdot a = (n \cdot 1_A)a$. By using the third problem, we have $n \cdot a = (n \cdot a)1_A = n \cdot (a1_A) = n \cdot (1_A a) = (n \cdot 1_A)a$.

6. $(n \cdot a)(m \cdot b) = (nm) \cdot (ab)$. Let $m = 1$. Then, $(n \cdot a)(1 \cdot b) = (n \cdot a)b = n \cdot (ab) = (n \cdot 1) \cdot (ab)$. Assume formula is true for m. Then, for $m + 1$, we have $(n \cdot a)((m+1) \cdot b) = (n \cdot a)(m \cdot b + b)$, by definition. Furthermore, by distributive law, $(n \cdot a)(m \cdot b + b) = (n \cdot a)(m \cdot b) + (n \cdot a)b$. By using assumption of induction and formula from the third problem, we have $(nm) \cdot (ab) + n \cdot (ab)$. By the second problem, we have $(nm) \cdot (ab) + n \cdot (ab) = (nm + n) \cdot (ab) = (n(m + 1)) \cdot (ab)$.

Theorem. Let $K \subseteq \mathbb{Z}^+$. Let:

1. $1 \in K$.

2. For all $k \in K$, if $l \in K$, for all $l \in \mathbb{Z}^+ \cap \{1, \ldots, k\}$, then $k \in K$.

Then, $K = \mathbb{Z}^+$.

Proof. Let $k \in K$. Let $1 \in K$ and let K have a property that, if $l \in K$, for all $l < k$, then $k \in K$. Let $K' = \mathbb{Z}^+ - K$. Assume that $K' \neq \emptyset$. Then, by the well-ordering property it has a least element c. As $1 \in K$, then $1 \notin K'$ so we must have $c > 1$. Now, let us observe $c - d$, for all $d \in \{1, \ldots, c - 1\}$. Then, $0 < d < c$, so $c - d \in \mathbb{Z}^+$. Assume that $c - d \notin K$. If $c - d \notin K$, then $c - d \in K'$ and, as $c - d < c$, c cannot be the least element. Therefore, $c - d \notin K'$ so it must be that $c - d \in K$. Thus, if we take $l = c - d$ and $k = c$, we have that $l \in K$ for all $l < k$. Therefore, by second property, $k \in K$, i.e. $c \in K$. But, then it cannot be that $c \in K'$ and K' must be empty, implying $K' = \emptyset$, i.e. $\mathbb{Z}^+ = K$.

□

Theorem (principle of strong induction). If:

1. Statement S_1 is true.

2. If statement S_i is true for every $i < k$, for some $k \in \mathbb{Z}^+$, then statement S_k is true.

Then, S_n is true for all $n \in \mathbb{Z}^+$.

Proof. Let S_1 be true. Let K be the set of all integers for which the statement is true. Then, $1 \in K$. But, if statement is true for all $i < k$, where $k \in \mathbb{Z}^+$, then S_k is true. Therefore, if $i \in K$, for all $i < k$, then $k \in K$. So, by previous theorem, $\mathbb{Z}^+ = K$, that is S_n is true for all $n \in \mathbb{Z}^+$.

□

Theorem. Every ideal of $\mathbb{Z}$ is principal.

Proof. Let $J \trianglelefteq \mathbb{Z}$. We must show that for all $y \in J$ there exists $a \in J$ such that $y = xa$ for some $x \in J$. $J \cap \mathbb{Z}^+ = \emptyset$. Now, if there are no negative elements, at least $0 \in J$, i.e. $J = \{0\}$ so we can say $J = \langle 0 \rangle$. If there are negative elements in J, then it cannot be that $J \cap \mathbb{Z}^+ = \emptyset$, because if $x \in J$ and $x < 0$, then also $-x \in J$, as J is closed with respect to negatives and, as $-x \in \mathbb{Z}^+$ and $-x \in J$, we have $J \cap \mathbb{Z}^+ \neq \emptyset$. Therefore, by the well-ordering property, as $J \cap \mathbb{Z}^+ \subseteq \mathbb{Z}^+$ and $J \cap \mathbb{Z}^+$ is non-empty, there exists $a \in J \cap \mathbb{Z}^+$ such that $a < x$, for all $x \in J \cap \mathbb{Z}^+$. Take any $y \in J$. By division with remainder theorem, there exist $q, r \in \mathbb{Z}$ such that $y = aq + r$, where $0 \leq r < |a|$. Note that $|a| = a$, as $a \in \mathbb{Z}^+$. As $q \in \mathbb{Z}$ and $a \in J$, then as $J \trianglelefteq A$, we have $aq \in J$. Also, as $y \in J$ and $aq \in J$, then $y - aq \in J$. Therefore, $r \in J$. Assume, $0 < r$, so $r \in \mathbb{Z}^+$ and $r \in J \cap \mathbb{Z}^+$. But, we said that a is the least element and we have $r < a$, which is a contradiction. Therefore, it must be that $r = 0$ and we have $y = aq$. Therefore, $J = \langle a \rangle$.

□

Proposition. Let $m \in \mathbb{Z}$. Then, $m|1$ if and only if m is invertible.

Proof. *Necessity.* Assume $m|1$. That means that there exists $q \in \mathbb{Z}$ such that $1 = mq$. That is, of course, due to $\mathbb{Z}$ being commutative, equivalent to $1 = qm$. Denoting q as m^{-1} clarifies that m is invertible, as then $1 = mm^{-1} = m^{-1}m$. *Sufficiency.* Assume m is invertible. Then there exists $m^{-1} \in \mathbb{Z}$ such that $mm^{-1} = m^{-1}m = 1$. But, that implies that $m|1$.

□

Proposition. In $\mathbb{Z}$, the only invertible elements are 1 and -1.

Proof. Assume $m \in \mathbb{Z}$ is invertible, and that $m \neq \pm 1$. Then, by previous proposition, $m|1$, so there exists $q \in \mathbb{Z}$ such that $mq = 1$. Let us observe the nature of m and q. We know that $m, q \neq 0$ as then it would be $mq = 0$. We also know that either $m > 0$ and

$q > 0$ or $m < 0$ and $q < 0$, because $1 > 0$, i.e. $mq > 0$. In the first case, either $q = 1$ or $q > 1$. If $q = 1$, then $mq = m$. But, as $mq = 1$, then $m = 1$, which is a contradiction. If $q > 1$, then $mq > m$, but as $mq = 1$, we have $1 > m$. But, as $m > 0$ and $m \neq 0$, this is impossible. In the second case, if $m < 0$ and $q < 0$, then, as $q \neq 0$, it must be either $q = -1$ or $q < -1$. If $q = -1$, then $mq = -m$, i.e. $1 = -m$, so $m = -1$, which is a contradiction to assumption that $m \notin \{1, -1\}$. If $q < -1$, then, as $-m > 0$, we have $(-m)q < -1(-m)$, i.e. $-mq < -m$. As $mq = 1$, then $-mq = -1$ and we have $-1 < -m$, which is equivalent to $m > 1$, which is a contradiction to assumption that $m > 0$. Therefore, if m is invertible, then $m \in \{1, -1\}$.

□

Definition. If $r, s \in \mathbb{Z}$ such that $r|s$ and $s|r$, we say that r and s are **associates** in $\mathbb{Z}$.

Proposition. Let $r, s \in \mathbb{Z}$. If r and s are associates in $\mathbb{Z}$, then $r = \pm s$.

Proof. Let $r|s$ and $s|r$. Then there exist $q_1, q_2 \in \mathbb{Z}$ such that $s = q_1 r$ and $r = q_2 s$. Multiplying the first equality with q_2 gives us $sq_2 = q_1 r q_2$. That is equivalent to $r = q_1 r q_2$. As $\mathbb{Z}$ is an integral domain, that is equivalent to $1 = q_1 q_2$. As $\mathbb{Z}$ is commutative, then $1 = q_1 q_2 = q_2 q_1$, i.e. q_1 and q_2 are invertible. So, $q_1, q_w = \pm 1$. Therefore, $r = \pm s$ and $s = \pm r$.

□

Proposition. Let $m \in \mathbb{Z} - \{0\}$. Then $\langle m \rangle$ is a prime ideal of $\mathbb{Z}$ if and only if m is prime.

Proof. *Necessity.* Assume $\langle m \rangle$ is a prime ideal of $\mathbb{Z}$ and m is not a prime. Then, there exist $m_1, m_2 \in \mathbb{Z} - \{-1, 1\}$ such that $m = m_1 m_2$. Now, as $m_1 m_2 = m \in \langle m \rangle$ we have that $m_1 \in \langle m \rangle$ or $m_2 \in \langle m \rangle$. Assume $m_1 \in \langle m \rangle$. But, that means that there exists $k \in \mathbb{Z}$ such that $m_1 = km$, meaning $m|m_1$. So, from $m_1|m$ and $m|m_1$, we conclude that $m_1 = \pm m$. That would imply $m = \pm m m_2$, and as $\mathbb{Z}$ is an integral domain, $1 = \pm m_2$, which is a contradiction. Therefore, m is a prime number. *Sufficiency.* Let m be a prime number. Then, $\langle m \rangle = \{xm : x \in \mathbb{Z}\}$. Take $y_1 y_2 \in \langle m \rangle$. Then, there exists $k \in \mathbb{Z}$ such that $y_1 y_2 = mk$. Now, we have that $m|(y_1 y_2)$. Assume $m \nmid y_1$ and $m \nmid y_2$. Then, as m is a prime number, it's only divisors are ± 1 and $\pm m$. If it were $\gcd m, y_1 = m$, we would have $m|y_1$, a contradiction. So, $\gcd m, y_1 = 1$ and by Euclid's lemma $m|y_2$, which is a contradiction. Therefore, $m|y_1$ or $m|y_2$. Without loss of generality, assume $m|y_1$. Then, there exists $q \in \mathbb{Z}$ such that $y_1 = qm$. But, that means that $y_1 \in \langle m \rangle$. If we assumed $m|y_2$, we would, in the same way, get $y_2 \in \langle m \rangle$. Therefore, $y_1 y_2 \in \langle m \rangle$ implies $y_1 \in \langle m \rangle$ or $y_2 \in \langle m \rangle$, so $\langle m \rangle \trianglelefteq_p \mathbb{Z}$.

□

Proposition. Every prime ideal of $\mathbb{Z}$ is maximal.

Proof. Assume $J \trianglelefteq_p \mathbb{Z}$ and that there exists $K \trianglelefteq \mathbb{Z}$ such that $J \subset K$ and $K \neq \mathbb{Z}$. As $J, K \trianglelefteq \mathbb{Z}$, they are principal and prime, i.e. $J = \langle p_1 \rangle$ and $K = \langle p_2 \rangle$, for some $p_1, p_2 \in P$. As $J \subset K$, then $p_1 \in J$ implies $p_1 \in K$, so there exists $k \in \mathbb{Z}$ such that $p_1 = kp_2$. But, that would imply $p_2 | p_1$, which is possible only if $p_2 = p_1$ or $p_2 = 1$. But, $p_2 = p_1$ would imply $\langle p_1 \rangle = \langle p_2 \rangle$, i.e. $J = K$, which is a contradiction to $J \subset K$. Then, $p_2 = 1$ would imply $K = \langle p_2 \rangle = \langle 1 \rangle = \mathbb{Z}$, which is a contradiction to $K \neq \mathbb{Z}$. Therefore, J is maximal.

□

Proposition. Let $m \in \mathbb{Z}$. Then, $\langle m \rangle = m\mathbb{Z}$.

Proof. Let $x \in \langle m \rangle$. Then, there exists $k \in \mathbb{Z}$ such that $x = km$. But, $mk \in m\mathbb{Z}$, so $x \in m\mathbb{Z}$ and $\langle m \rangle \subseteq m\mathbb{Z}$. Now, if we take $x \in m\mathbb{Z}$, then there exists $k \in \mathbb{Z}$ such that $x = mk$. But, $mk \in \langle m \rangle$, so $m\mathbb{Z} \subseteq \langle m \rangle$ and from that we have $m\mathbb{Z} = \langle m \rangle$.

□

Proposition. Let $p \in P$. Then, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof. Let $p \in P$. Then, $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\langle p \rangle$, by a previous proposition. Also, by a previous proposition, as $p \in P$, $\langle p \rangle$ is a prime ideal. Therefore, by a previous proposition, it is a maximal ideal, and by a previous theorem, $\mathbb{Z}/\langle p \rangle$ is a field.

□

Proposition. Let $m, n \in \mathbb{Z}$. Then, $\langle m \rangle \cap \langle n \rangle = \langle \operatorname{lcm}(m, n) \rangle$.

Proof. Let $x \in \langle m \rangle \cap \langle n \rangle$. Then there exist $k_1, k_2 \in \mathbb{Z}$ such that $x = mk_1$ and $x = nk_2$. From that we have that $m|x$ and $n|x$, so x is a common multiple of m and n. Therefore, $x = k\operatorname{lcm}(m, n)$, for some $k \in \mathbb{Z}$ and $x \in \langle \operatorname{lcm}(m, n) \rangle$. That implies $\langle m \rangle \cap \langle n \rangle \subseteq \langle \operatorname{lcm}(m, n) \rangle$. Now, let $x \in \langle \operatorname{lcm}(m, n) \rangle$. Then there exists $k \in \mathbb{Z}$ such that $x = k\operatorname{lcm}(m, n)$. So, as $m|\operatorname{lcm}(m, n)$ and $n|\operatorname{lcm}(m, n)$, also $m|x$ and $n|x$, and there exist $k_1, k_2 \in \mathbb{Z}$ such that $x = mk_1$ and $x = nk_2$, which implies $x \in \langle m \rangle$ and $x \in \langle n \rangle$. That is, $x \in \langle m \rangle \cap \langle n \rangle$ and $\langle \operatorname{lcm}(m, n) \rangle \subseteq \langle m \rangle \cap \langle n \rangle$. Therefore, $\langle m \rangle \cap \langle n \rangle = \langle \operatorname{lcm}(m, n) \rangle$.

□

Proposition. Every homomorphic image of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, for some $n \in \mathbb{Z}$.

Proof. Let A be a homomorphic image of $\mathbb{Z}$. Then, there exists a homomorphism $f : \mathbb{Z} \to A$. By FHT, $A \cong \mathbb{Z}/\ker(f)$. But, $\ker(f) \trianglelefteq \mathbb{Z}$, and by a previous proposition, $\ker(f)$ is a principal ideal, i.e. there exists $n \in \mathbb{Z}$ such that $\ker(f) = \langle n \rangle$. But, then $A \cong \mathbb{Z}/\ker(f)$ is equivalent to $A \cong \mathbb{Z}/\langle n \rangle$, which is in turn eqivalent to $A \cong \mathbb{Z}/n\mathbb{Z}$.

□

Proposition. Let G be a group and $a, b \in G$. Then, $\{n \in \mathbb{Z} : \ ab^n = b^n a\} \trianglelefteq \mathbb{Z}$.

Proof. Let $S = \{n \in \mathbb{Z} : \ ab^n = b^n a\}$. By definition, $S \subseteq \mathbb{Z}$. Let $m, n \in S$. Then, $ab^m = b^m a$ and $ab^n = b^n a$. Multiplying first equality on the right by b^n gives us $ab^m b^n = b^m ab^n$. But, $ab^n = b^n a$, so $ab^{m+n} = b^m b^n a$, i.e. $ab^{m+n} = b^{m+n} a$, so $m + n \in S$. Now, multiplying first equality on the right by $b^{-m} \in G$ gives us $ab^m b^{-m} = b^m ab^{-m}$. We multiply that equality again on the left by b^{-m} and get $b^{-m}a = b^{-m}b^n ab^{-m}$, which is $b^{-m}a = ab^{-m}$, so $-m \in S$. Finally, if $k \in \mathbb{Z}^+$, we will prove that $ab^{mk} = b^{mk}a$. For $k = 1$, we have $ab^{m1} = ab^m = b^m a = b^{m1}a$, so $1 \in S$. Then, assume the statement holds for k, i.e. $ab^{mk} = b^{mk}a$. We will prove that it holds for $k + 1$. We have $ab^{m(k+1)} = ab^{mk+m} = ab^{mk}b^m$. By assumption of induction, $ab^{mk}b^m = b^{mk}ab^m = b^{mk}b^m a = b^{mk+m}a = b^{m(k+1)}a$. Therefore, the equality is true for all $k \in \mathbb{Z}^+$. If $k < 0$, then we can take $k = -k'$, so that $k' > 0$. We have $ab^{mk} = ab^{-mk'} = a(b^{-m})^{k'}$. But, as also $ab^{-m} = b^{-m}a$, as proved just a moment ago, then $a(b^{-m})^{k'} = (b^{-m})^{k'}a = b^{-mk'}a = b^{mk}a$. If $k = 0$, then $ab^0 = ae = ea = b^0 a$. Therefore, $ab^{mk} = b^{mk}a$ is true for all $k \in \mathbb{Z}$, so $mk \in S$. Now, as $n \in S \subseteq \mathbb{Z}$, it is also true that $ab^{mn} = b^{mn}a$ (which can be obtained in the same way as above). In conclusion, $S \trianglelefteq \mathbb{Z}$.

□

Proposition. Let G be a group, $H \leq G$ and $a \in G$. Then, $\{n \in \mathbb{Z} : \ a^n \in H\} \trianglelefteq \mathbb{Z}$.

Proof. Let $S = \{n \in \mathbb{Z} : \ a^n \in H\}$. By definition, $S \subseteq \mathbb{Z}$. Let $m, n \in \mathbb{Z}$. Then, $a^m, a^n \in H$. But, as $H \leq G$, we also have $a^m a^n \in H$, i.e. $a^{m+n} \in H$, and $a^{-m} \in H$. So, $m + n \in \mathbb{Z}$ and $-m \in \mathbb{Z}$. Let $k \in \mathbb{Z}$. Then, $a^{mk} = (a^m)^k$. But, $a^m \in H$ and so $(a^m)^k \in H$ and we have $k \in S$, for all $k \in \mathbb{Z}$ (and so also for n). Therefore, $S \trianglelefteq \mathbb{Z}$.

□

Proposition. Let $m, n \in \mathbb{Z}$. Then, $\langle m \rangle + \langle n \rangle = \langle \gcd(m, n) \rangle$.

Proof. Let $mk + nl \in \langle m \rangle + \langle n \rangle$ and $g = \gcd(m, n)$. Then, there exists $g' \in \mathbb{Z}$ such that $mk + nl = g'$. As $g|m$ and $g|n$, we have that there exist $m', n' \in \mathbb{Z}$ such that

$m = m'g$ and $n = n'g$. Therefore, $g' = mk + nl = m'gk + n'gl$, i.e. $g' = g(m'k + n'l)$. If we take $x = m'k + n'l$ then $g' = \gcd(m, n)x$, where $x \in \mathbb{Z}$. Therefore, $g' \in \langle \gcd(m, n) \rangle$ and $\langle m \rangle + \langle n \rangle \subseteq \langle \gcd(m, n) \rangle$. Take $k \gcd(m, n) \in \langle \gcd(m, n) \rangle$. By Bezout's lemma, there exist $x, y \in \mathbb{Z}$ such that $\gcd(m, n) = mx + ny$. Multiplying that equality by k we get $k \gcd(m, n) = m(xk) + n(yk)$. So, $m(xk) \in \langle m \rangle$ and $n(yk) \in \langle n \rangle$, therefore $m(xk) + n(yk) \in \langle m \rangle + \langle n \rangle$, and that is $k \gcd(m, n) \in \langle m \rangle + \langle n \rangle$, from which we get $\langle \gcd(m, n) \rangle \subseteq \langle m \rangle + \langle n \rangle$ and conclude that $\langle m \rangle + \langle n \rangle = \langle \gcd(m, n) \rangle$.

□

Notes on classification of integral domains

Definition. Let A be an integral domain and let $a, b \in A$. If there exists $q \in A$ such that $b = qa$, we say that a **divides** b and symbolize that by writing $a|b$.

Proposition. Let A be an integral domain. Then, for all $a \in A - \{0\}$:

1. $a \mid 0$;
2. $0 \nmid a$.

Proof. Let $a \in A - \{0\}$. *Ad* 1. We have $0 = a0$, so $a|0$. *Ad* 2. Assume $0 \mid a$. Then, there exists $q \in A$ such that $a = 0q$. But, that implies $a = 0$, which is a contradiction to $a \neq 0$. Therefore, $0 \nmid a$ for all $a \in A - \{0\}$.

□

Definition. Let A be an integral domain and $a \in A - \{0\}$. If $a|1$ then we say that a is a **unit**. We denote by A^* as the set of all units in A, that is:

$$A^* = \{a \in A - \{0\} : \ a|1\}.$$

Theorem. Every finite integral domain is a field.

Proof. Just notice that, if $A = \{0, 1\}$ is an integral doman, then A is a trivial field, every $a \in A - \{0\}$, which is only unity, has an inverse, and is commutative with respect to multiplication. Now, let $A = \{0, 1, a_1, \ldots, a_m\}$ be a finite integral domain and $m \in \mathbb{Z}^+$. Then, $|A| = m + 2$. Let $f_i : A - \{0\} \to A - \{0\}$ be a mapping defined with $f_i(x) = a_i x$, for all $i \in \{1, \ldots, m\}$ (we do not define it for 0 and 1 - zero is not inverible anyway, and 1 is always invertible, it is its own inverse). Then, it is obvious that f_i is a function, because $a_i x \in A - \{0\}$, for all $a_i, x \in A - \{0\}$ (as A is an integral domain, it has no zero divisors, so $a_i x \neq 0$). Also, if $x = y$, then, multiplying by a_i, we have $a_i x = a_i y$, i.e. $f_i(x) = f_i(y)$. Thus, uniqueness is also satisfied. Then, if $a_i x = a_i y$, as $a_i \neq 0$ we have $x = y$, so f_i is injective. Therefore, $\operatorname{ran}(f_i) = \{a_i x : \ x \in A - \{0\}\} = \{a_1 1, a_i a_1, a_i a_2, \ldots, a_i a_m\}$. Assume that $a_i a_j = a_i a_k$, for some $j, k \in \{1, \ldots, m\}$, $j \neq k$, and also allowing $a_j = 1$. That would imply, as A is an integral domain, that $a_j = a_k$, for some $j \neq k$, and that would be a contradiction that $\{1, a_1, \ldots, a_m\}$ are distinct. Thus, $|\operatorname{ran}(f_i)| = |A - \{0\}|$. As $\operatorname{ran}(f_i) \subseteq A - \{0\}$, that, and the latter, implies $A - \{0\} = \operatorname{ran}(f_i)$, i.e. f_i is surjective. Then, it is also bijective. So, if we $a_i \in A$, and if we take $1 \in A - \{0\}$, there must exist $a_j \in A$ such that $f_i(a_j) = 1$, i.e. $a_i a_j = 1$. Thus, every $a_i \in A - \{0\}$, for $i \in \{1, \ldots, m\}$ has an inverse (as does $1 \in A$) and A is a field.

□

Remark. As we now can classify all finite integral domains as field, in the further classification (and only in this chapter), we will conduct proofs for fields and infinite integral domains separately.

Definition. Let A be an integral domain and $p \in A - \{0\}$. We say that p is a **prime** in A if $\langle p \rangle$ is a prime ideal.

Proposition. Let A be an integral domain and let p be a prime in A. Then, if $p|ab$, for some $a, b \in A - \{0\}$, then $p|a$ or $p|b$.

Proof. Let $p|ab$. Then, $ab = pq$, for some $q \in A$. That implies that $ab \in \langle p \rangle$, and as p is prime, $\langle p \rangle$ is a prime ideal. Thus, $a \in \langle p \rangle$ or $b \in \langle p \rangle$. Equivalently, there exists $r \in A$ such that $a = pr$ or $b = pr$. In other words, $p|a$ or $p|b$.

□

Definition. Let A be an integral domain and $a \in A - A^*$, $a \neq 0$. If $a = pq$, for some $p, q \in A$, implies $p \in A^*$ or $q \in A^*$, we say that a is **irreducible** in A. If that is not the case, we say that a is **reducible** in A.

Proposition. Let A be an integral domain and $p \in A$ a prime in A. Then p is irreducible.

Proof. Let $p \in A$ be a prime and assume that $p = qr$, for some $q, r \in A$. Then, as p is a prime, $\langle p \rangle$ is a prime ideal. From that we have $\langle p \rangle = \langle qr \rangle$, so $qr \in \langle p \rangle$. That implies $q \in \langle p \rangle$ or $r \in \langle p \rangle$. If $q \in \langle p \rangle$, then $q = ps$, for some $s \in A$. From that we have $qr = prs$, and as $qr = p$, that implies $p = prs$. As $p \neq 0$ and A is an integral domain, $p \cdot 1 = p(rs)$ implies $rs = 1$, i.e. $r \in A^*$. In other words, p is irreducible.

□

Definition. Let A be an integral domain and $p, q \in A$. If $p = uq$, for some $u \in A^*$, then we say that p is **associate** of q in A.

Definition. Let A be an integral domain. We say that A is an **unique factorization domain** (or UFD for short) if:

1. There exist irreducibles $p_1, \ldots, p_m \in A$, for some $m \in \mathbb{Z}^+$, and a unit $u \in A^*$ such that $a = up_1p_2 \cdots p_m$, for all $a \in A - A^*$, $a \neq 0$.

2. From $a = up_1p_2\cdots p_m$ and $a = vq_1q_2\cdots q_n$, where $p_1, \ldots, p_m, q_1, \ldots, q_n$ are irreducibles in A with $m, n \in \mathbb{Z}^+$ and $u, v \in A^*$, follows that $m = n$, $u = v$ and that there exists a permutation ρ on $\{1, \ldots, m\}$ such that $p_i = q_{\rho(i)}$, for all $i \in \{1, \ldots, m\}$.

Proposition. Every field is a UFD.

Proof. Let F be a field. Take $a \in F - \{0\}$. Then, as F is a field, there exists $a^{-1} \in F - \{0\}$ such that $aa^{-1} = a^{-1}a = 1$. From that we have that $a|1$, i.e. $F - \{0\} \subseteq F^*$. Also, by definition, $F^* \subseteq F - \{0\}$, so we have $F - \{0\} = F^*$. That implies that $(F - \{0\}) - F^* = \emptyset$, so the conditions for UFD vacuously hold (as there are no elements on which to check them).

□

Proposition. Let A be a UFD and $p \in A$. Then, p is prime if and only if it is irreducible.

Proof. *Necessity.* Let p be a prime in A. Then, as UFD A is by definition an integral domain, by previous proposition, which states that if p is prime in integral domain, it is irreducible, we have that p is irreducible in A.

Sufficiency. Let p be irreducible. Let $ab \in \langle p \rangle$. We must prove that $a \in \langle p \rangle$ or $b \in \langle p \rangle$. As $ab \in \langle p \rangle$, and $\langle p \rangle$ is principal ideal, we have $ab = pq$, for some $q \in A$. But, as A is a UFD, then, $q = uq_1 \cdots q_m$, $a = va_1 \cdots a_k$ and $b = wb_1 \cdots b_l$, where q_i, a_j and b_n are irreducible for all $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, k\}$ and $n \in \{1, \ldots, l\}$, and $u, v, w \in A^*$. Then, $(vw)a_1 \cdots a_k b_1 \cdots b_l = upq_1 \cdots q_m$ and we may write that same expression as $ux_1 \cdots x_{k+l} = vy_1 \cdots y_{m+1}$, where $x_i = a_i$ for all $i \in \{1, \ldots, k\}$, $x_{k+i} = b_i$, for all $i \in \{1, \ldots, l\}$, $y_1 = p$ and $y_{i+1} = q_i$, for all $i \in \{1, \ldots, m\}$. As A is a UFD, it also follows that $k + l = 1 + m$, $vw = u$, and that there exists a permutation ρ on $\{1, \ldots, m + 1\}$ such that $x_i = y_{\rho(i)}$. As ρ is a permutation, it is a bijection and has an inverse such that $x_{\rho^{-1}(i)} = y_i$. Specifically, as $p = y_1$ (without loss of generality), we have $p = x_{\rho^{-1}(1)}$, and equivalently, $p = x_{\rho^{-1}(1)}$. Without loss of generality, we can take $p = y_1 = x_{\rho^{-1}(1)} = a_1$. So, $p = a_1$, which implies $a_1 \in \langle p \rangle$. As $a_2 \cdots a_k \in A$, and $\langle p \rangle \trianglelefteq A$ (principal ideal is an ideal), we have $a_1 a_2 \cdots a_k \in \langle p \rangle$, i.e. $a \in \langle p \rangle$. Thus, $\langle p \rangle$ is a prime ideal.

□

Definition. Let A be an integral domain and $a, b \in A - \{0\}$. If there exists $d \in A$ such that $d|a$ and $d|b$, we say that d is a **common divisor** of a and b.

Definition. Let A be an integral domain and $a, b \in A$. Let G be a set such that $g \in G$

if and only if g is a common divisor of a and b such that $g'|a$ and $g'|b$ implies $g'|g$, for all $g' \in A$. If there exists $g \in G$ such that $u \nmid g$, for all $u \in A^* - \{1\}$, we say that g is a **greatest common divisor** of a and b and symbolize that by writing $g = \gcd(a, b)$.

Proposition. Let A be a UFD and $a, b \in (A - \{0\}) - A^*$. Then, there exists a unique $g \in A$ such that $g = \gcd(a, b)$.

Proof. *Existence.* Let $p_1, \ldots, p_k$ be irreducibles in A such that $p_i|a$ and $p_i|b$, for all $i \in \{1, \ldots, k\}$. Then, $a = up_1^{r_1} \cdots p_k^{r_k}$ and $b = vp_1^{s_1} \cdots p_k^{s_k}$, where $r_1, \ldots, r_k \in \mathbb{Z}_0^+$ and $s_1, \ldots, s_l \in \mathbb{Z}_0^+$, for some $k \in \mathbb{Z}^+$ and $u, v \in A^*$. Take $m_i = \min\{r_i, s_i\}$, for all $i \in \{1, \ldots, k\}$. Then, it is obvious that $p_i^{m_i}|p_i^{r_i}$ and $p_i^{m_i}|p_i^{s_i}$, for all $i \in \{1, \ldots, k\}$. That implies that $p_i^{m_i}|a$ and $p_i^{m_i}|b$, for all $i \in \{1, \ldots, k\}$. If we take $g = p_1^{m_1} \cdots p_k^{m_k}$, then $g|a$ and $g|b$. Also $u \nmid g$, for all $u \in A^* - \{1\}$. Then, assume $g'|a$ and $g'|b$. That means that $g' = wp_1^{h_1} \cdots p_k^{h_k}$, where it must be that $p_i^{h_i}|p_i^{r_i}$ and $p_i^{h_i}|p_i^{s_i}$. That implies that $h_i \leq m_i$, for all $i \in \{1, \ldots, k\}$. From that again follows that $p_i^{h_i}|p_i^{m_i}$, for all $i \in \{1, \ldots, k\}$. From that we have $p_i^{m_i} = z_i p_i^{h_i}$, where $z_i = p_i^{c_i}$, for some $c_i \in \mathbb{Z}_0^+$, and then we have $g = w^{-1}(z_1 \cdots z_2)(w(p_1^{h_1} \cdots p_k^{h_k})) = w^{-1}Zg'$, where $Z = z_1, \ldots, z_k$. That implies that $g'|g$ and it must be that $g = \gcd(a, b)$.

Uniqueness. Assume that there exists $g' \in A$ such that $g' = \gcd(a, b)$. That implies that $u \nmid g'$, for all $u \in A^* - \{1\}$, $g'|a$, $g'|b$, and $g''|a$ with $g''|b$ implies $g''|g'$ for all $g'' \in A$. But, as $g|a$ and $g|b$ then it must be that $g|g'$. Also, as $g = \gcd(a, b)$, we have $g'|g$, due to $g'|a$ and $g'|b$. Therefore, from $g'|g$, we have that there exists $u \in A$ such that $g = ug'$. From $g|g'$, we have that there exists $v \in A$ such that $g' = vg$. Then, multiplying the former equality with v gives us $gv = uvg'$, i.e. $g' = uvg'$. As A is a UFD, and from that by definition an integral domain, and as $g' \neq 0$, then $1g' = (uv)g'$ implies $1 = uv$, i.e. $u, v \in A^*$. But, as $u' \nmid g$, for all $u' \in A^* - \{1\}$ and $v' \nmid g'$, for all $v' \in A^* - \{1\}$, by defition, then it must be that $u = v = 1$ and $g = g'$.

□

Definition. Let A be an integral domain. If every ideal of A is principal, we say that A is a **principal ideal domain** (or PID for short).

Lemma. Let A be an integral domain and $a, b \in A - \{0\}$ such that $a = bq$ for some $q \in A$. Then, $q \neq 0$.

Proof. Assume $q = 0$. Then, $a = b \cdot 0 = 0$, which is a contradiction to $a \neq 0$.

□

Lemma. Let A be an integral domain and $a, b \in A - \{0\}$. If $a|b$ and $b|a$ then $a = b$.

Proof. As $a|b$, there exists $p \in A$ such that $b = pa$. As $b|a$, there exists $q \in A$ such that $a = qb$. From $b = pa$, after multiplying equality by q, we have $bq = paq$. From that and $a = qb$, we have $a = paq$, that is $a = pqa$. As A is an integral domain, by cancellation law, that implies $1 = pq$. As $a, b \neq 0$, then also $p, q \neq 0$ by previous lemma, we can apply cancellation law. From $1 \cdot 1 = pq$ (also note that A is not trivial by definition of an integral domain so $1 \neq 0$) we have $p = 1$. Then, $1 = 1 \cdot q$, which implies $q = 1$. Thus, $a = b \cdot 1$ and $b = a \cdot 1$, i.e. $a = b$.

□

Theorem. Let A be a principal ideal domain. Then, for all $a, b \in A - \{0\}$:

1. There exists a unique $g \in A$ such that $g = \gcd(a, b)$.
2. If $g = \gcd(a, b)$, there exist $p, q \in A$ such that $\gcd(a, b) = ap + bq$ (*Bezout's lemma*).

Proof. Let $a, b \in A$ and $J = \{ax + by : \ x, y \in A\}$. Let $ax_1 + by_1, ax_2 + by_2 \in J$. Obviously, $J \subseteq A$. Then, $(ax_1 + by_1) + (ax_2 + by_2) = a(x_1 + x_2) + b(y_1 + y_2) \in J$ and $(ax_1+by_1)(ax_2+by_2) = a^2x_1x_2+ax_1by_2+by_1ax_2+b^2y_1y_2 = a(ax_1x_2+x_1by_2)+b(y_1ax_2+by_1y_2) \in J$. Also, if $c \in A$, then $c(ax_1 + by_1) = (ax_1 + by_1)c = a(x_1c) + b(y_1c) \in J$. Thus, $J \trianglelefteq A$, and that implies that J is a principal ideal of A. In other words, J is generated by some $g \in A$ which means $J = \langle g \rangle$. As $a = a \cdot 1 + b \cdot 0 \in \langle g \rangle$ and $b = a \cdot 0 + b \cdot 1 \in \langle g \rangle$, then there exist $s, t \in A$ such that $a = gs$ and $b = gt$. That implies $g|a$ and $g|b$. Also, as $g \in \langle g \rangle = J$, there exist $p, q \in A$ such that $g = ap + bq$.

Assume that there exists $g' \in A$ such that $g'|a$ and $g'|b$. Then there exist $s', t' \in A$ such that $a = g's'$ and $b = g't'$. From $g = ap + bq$ we have $g = g's'p + g't'q$, i.e. $g = g'(s'p + t'q)$. From that follows $g'|g$ and by definition $g = \gcd(a, b)$. Assume that $h = \gcd(a, b)$. Then, $h|a$ and $h|b$, so, as $g = \gcd(a, b)$, we have $g|h$. Also, as h is a greatest common divisor of a and b, from $g|a$ and $g|b$ we have $g|h$. From $g|h$ and $h|g$ we have, by a previous lemma, $g = h$. So, greatest common divisor is unique.

□

Rings of polynomials

Definition. Let A be a commutative ring with unity, $a_0, a_1, \ldots, a_n \in A$ and x an arbitrary symbol. Every expression of the form:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

is called a **polynomial in x with coefficients in A**, or more simply, a **polynomial in x over A**. The expressions $a_k x^k$, for $k \in \{1, \ldots, n\}$ are called the **terms** of the polynomial. The coefficient a_0 is called the **zero term** of the polynomial.

Remark. The set of all polynomials in x with coefficients in A is defined as:

$$A[x] = \{a_0 + a_1 x + \cdots + a_n x^n : \ (\forall i \in \{0, \ldots, n\})(a_i \in A) \wedge (n \in \mathbb{Z}_0^+)\}.$$

Then, we denote $a(x) = a_0 + a_1 x + \cdots + a_n x^n$. If $a_i \in A$, for all $i \in \{0, \ldots, n\}$, then $a(x) \in A[x]$.

Definition. We say that $a(x) = 0$ is a **zero polynomial**. We define the **degree** of a non-zero polynomial as:

$$\deg a(x) = \max\{k \in \mathbb{Z}_0^+ : \ a_k \neq 0\}.$$

Then, the **zero degree polynomial** is $a(x) = a_0$. Also, the **leading coefficient** is $a_{\deg a(x)}$.

Remark. Let A be a ring and $a(x), b(x) \in A[x]$. Let $m = \deg a(x)$ and $n = \deg b(x)$. Then, $a(x) = b(x)$ if and only if $m = n$ and $a_i = b_i$, for all $i \in \{0, \ldots, m\}$. For example, in $\mathbb{Z}/5\mathbb{Z}[x]$, it is not true that $x^8 + 1 = x^3 + 1$, because $\deg(x^8 + 1) = 8 \neq 3 = \deg(x^3 + 1)$.

Definition. Let $n \in \mathbb{Z}_0^+$ and $a(x), b(x) \in A[x]$ such that[78]:

$$\begin{aligned} a(x) &= a_0 + a_1 x + \cdots + a_n x^n, \\ b(x) &= b_0 + b_1 x + \cdots + b_n x^n. \end{aligned}$$

[78] Notice here that we do not assume they have the same degree; rather we allow coefficients to be zero, to avoid complications with formulae.

Then we define polynomial addition and multiplication, respectively:

$$\begin{aligned} a(x)+b(x) &= (a_0+a_1x+\cdots+a_nx^n)+(b_0+b_1x+\cdots+b_nx^n) \\ &= (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n \\ a(x)b(x) &= (a_0+a_1x+\cdots+a_nx^n)(b_0+b_1x+\cdots+b_nx^n) \\ &= (a_0b_0)+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots+(a_nb_n)x^{2n}. \end{aligned}$$

From now on we will consider $A[x]$ together with these operations. The coefficients of the resulting polynomials, i.e. $c(x)=a(x)+b(x)$ and $d(x)=a(x)b(x)$ can be obtained, by observing formulae from above. For, addition, we simply have $c_k=a_k+b_k$, for all $k\in\{0,\ldots,n\}$. For multiplication[79] it is important to note that for d_k, all indices sum up to k. So, for all $k\in\{0,\ldots,2n\}$:

$$d_k=\sum_{i+j=k}a_ib_j.$$

Finally, notice that:

$$\begin{aligned} \deg\left(a(x)+b(x)\right) &\leq \max\left\{\deg a(x),\deg b(x)\right\} \\ \deg\left(a(x)b(x)\right) &\leq \deg a(x)+\deg b(x). \end{aligned}$$

Lemma. Let A be a ring and $a(x),b(x),c(x)\in A[x]$. Then,

1. $[a(x)+b(x)]+c(x)=a(x)+[b(x)+c(x)]$.
2. $a(x)[b(x)c(x)]=[a(x)b(x)]c(x)$.

Proof. *Ad* 1. Let $d(x)=b(x)+c(x)$. Then, coefficients for $d(x)$ are given for all $i\in\{0,\ldots,n\}$ with $d_i=a_i+b_i$. Let $e(x)=a(x)+[b(x)+c(x)]$, i.e. $e(x)=a(x)+d(x)$. So, coefficients for $e(x)$ are $e_i=a_i+d_i=a_i+(b_i+c_i)=a_i+b_i+c_i$, as A is associative. On the other hand, if we took $d(x)=a(x)+b(x)$ and $e(x)=[a(x)+b(x)]+c(x)$, that is $e(x)=d(x)+c(x)$, we would have $e_i=(a_i+b_i)+c_i=a_i+b_i+c_i$, as A is associative. Therefore, both $e(x)$ have equal degrees and coefficients, so $a(x)+[b(x)+c(x)]=[a(x)+b(x)]+c(x)$.

Ad 2. Let $d(x)=b(x)c(x)$. Coefficients for $d(x)$ are given with $d_k=\sum_{i+j=k}b_ic_j$, where $k\in\{0,\ldots,2n\}$. Let $e(x)=a(x)[b(x)c(x)]$, that is, $e(x)=a(x)d(x)$. From that

[79] Compare with recursive formula for Catalan's numbers in the beginning of the script.

we have coefficients for $e(x)$, given with, $e_l = \sum_{k+m=l} a_m d_k = \sum_{k+m=l} a_m \sum_{i+j=k} b_i c_j = \sum_{k+m=l} \sum_{i+j=k} a_m b_i c_j$, where $l \in \{0, \ldots, 3n\}$. But, as $i + j = k$ and $k + m = l$, then $k + m = l$, i.e. $i + j + m = l$. So, we may write that as $e_l = \sum_{i+j+m=l} a_m (b_i c_j)$. On the other hand, if we take $d(x) = a(x)b(x)$, we have $d_k = \sum_{i+j=k} a_i b_j$. Then, $e_l = \sum_{k+m=l} \left(\sum_{i+j=k} a_i b_j \right) c_m = \sum_{k+m=l} (a_i b_j) c_m$. As A is a ring, then it is associative, and the expressions for e_l are equal.

□

Lemma. Let A be a ring and $a(x), b(x), c(x) \in A[x]$. Then,

1. $a(x) + b(x) = b(x) + a(x)$.
2. $a(x)[b(x) + c(x)] = [a(x)b(x)] + [a(x)c(x)]$.
3. $[a(x) + b(x)]c(x) = [a(x)c(x)] + [b(x)c(x)]$.

Proof. *Ad* 1. Coefficients for $[a(x) + b(x)]$ are $a_i + b_i$, which is equal to $b_i + a_i$, because additive A is commutative. These are the coefficients for $[b(x) + a(x)]$. *Ad* 2. Let $d(x) = b(x) + c(x)$. Then, coefficients for $d(x)$ are given with $d_i = b_i + c_i$, where $i \in \{0, \ldots, n\}$. Now, take $e(x) = a(x)[b(x) + c(x)]$, so $e(x) = a(x)d(x)$. We can see that coefficients for $e(x)$ are given by:

$$\begin{aligned} e_k &= \sum_{i+j=k} a_j d_i = \sum_{i+j=k} a_j (b_i + c_i) \\ &= \sum_{i+j=k} a_j b_i + a_j c_i = \sum_{i+j=k} a_j b_i + \sum_{i+j=k} a_j c_i. \end{aligned}$$

It is easy to see that the given sum is equal to the coefficients for $[a(x)b(x)] + [a(x)c(x)]$. *Ad* 3. Proof analogous to the proof of the previous result.

□

Theorem. If A is a ring, then $A[x]$ is a ring.

Proof. Let A be a ring. Then, by previous two lemmas, associativity and distribudive laws hold for $A[x]$. Also additive $A[x]$ is commutative. Let $a(x) \in A[x]$. Then, zero is $o(x) = 0$, where $0 \in A$, because $0 + a_i = a_i + 0 = a_i$, for all $i \in \{0, \ldots, n\}$. Negative of $a(x)$ is $-a(x) = -a_0 + \cdots + (-a_n)x^n$.

□

Proposition. Let A be a ring. Then,

1. If A is commutative, then $A[x]$ is commutative.

2. If $1 \in A$, then $A[x]$ is a ring with unity.

Proof. *Ad* 1. Let $ab = ba$, for all $a, b \in A$. Then, let $c(x) = a(x)b(x)$. Coefficients for $c(x)$ are $c_k = \sum_{i+j=k} a_i b_j$. As A is commutative, $c_k = \sum_{i+j=k} b_j a_i$, but those are the coefficients for $b(x)a(x)$. So, $a(x)b(x) = b(x)a(x)$. *Ad* 2. Let $1 \in A$. Then, in $A[x]$, unity is $u(x) = 1$ because $u(x)a(x) = 1(a_0 + \cdots + a_n x^n) = 1a_0 + \cdots + 1a_n x^n = a(x)$. One can see that the same holds for $a(x)u(x)$.

□

Theorem. If A is an integral domain, then $A[x]$ is an integral domain and:

$$\deg a(x)b(x) = \deg a(x) + \deg b(x).$$

Proof. Let A be an integral domain. Then it is also a commutative ring with unity. By a previous proposition, $A[x]$ is a commutative ring with unity. Now, A has no divisors of zero. Therefore, we must show that, if $a(x)b(x) = 0$, then either $a(x) = 0$ or $b(x) = 0$. Conversely, if $a(x), b(x) \neq 0$, then $a(x)b(x) \neq 0$. As $a(x)$ and $b(x)$ are non-zero polynomials, then their leading coefficient is not zero. In other words, if $\deg a(x) = m$ and $\deg b(x) = n$, then $a_n \neq 0$ and $b_n \neq 0$. Therefore, as A is an integral domain, it must be that $a_n b_m \neq 0$. Assume $n > m$. Then, we can take $a(x)b(x) = (a_0 + \cdots + a_m x^m)(b_0 + \cdots + b_n x^n)$. Then, the coefficient for x^{n+m} is $a_m b_n$, because in $\{0, \ldots, m\}$ and $\{0, \ldots, n\}$ no other power can add up to $n + m$. Therefore, leading coefficient of $c(x)$ is $a_m b_n$ and $\deg a(x)b(x) = m + n = \deg a(x) + \deg b(x)$. That also implies that $a(x)b(x)$ is a non-zero polynomimal because it has at least one non-zero coefficient and that is its leading coefficient. So, $A[x]$ is an integral domain.

□

Remark. If A is an integral domain, then $A[x]$ is called **domain of polynomials**. Notice that, if F is a field, then $F[x]$ is not necessarily a field, but as F is also an integral domain, then $F[x]$ is at least an integral domain, by the previous theorem.

Remark. In the proof of the following theorem, we will follow the elementary procedure of dividing two polynomials and it will be proved by strong induction over difference of degrees of two polynomials.

Theorem (Division algorithm for polynomials). Let F be a field and $a(x), b(x) \in F[x]$. Then, there exist unique $q(x), r(x) \in F[x]$ such that $a(x) = b(x)q(x) + r(x)$, where $\deg r(x) < \deg b(x)$.

Proof. *Existence.* Let $b(x) \in F[x]$. We will show that for all $a(x)$ there exist $q(x), r(x) \in F[x]$ such that $a(x) = b(x)q(x) + r(x)$ with $\deg r(x) < \deg b(x)$. If $\deg a(x) < \deg b(x)$, then $a(x) = b(x) \cdot 0 + a(x)$ (we have $q(x) = 0$ and $r(x) = a(x)$) and obviously $\deg r(x) = \deg a(x) < \deg b(x)$.

Let $m = \deg a(x) \geq \deg b(x) = n$. We will prove this case by strong induction on m. If $m = n$, i.e. $\deg a(x) = \deg b(x)$ and, if $a(x) = a_0 + \cdots + a_m x^m$ (where $m = \deg a(x) = \deg b(x)$, so $a_m \neq 0$) and $b(x) = b_0 + \cdots + b_m x^m$, then we can take, as F is a field, $b_m^{-1} \in F$ so that $q(x) = b_m^{-1} a_m$ (notice that $q(x) \in F[x]$). Then, we have:

$$\begin{aligned} b(x)q(x) &= (b_0 + b_1 x + \cdots + b_{m-1}x^{m-1} + b_m x^m)(b_m^{-1} a_m) \\ &= b_0 b_m^{-1} a_m + b_1 b_m^{-1} a_m x + \cdots + b_{m-1} b_m^{-1} a_m x^{m-1} + a_m x^m. \end{aligned}$$

It is easy to see that all we need to do is subtract new coefficients and add ones from $a(x)$ to get the residue:

$$r(x) = (a_0 - b_0 b_m^{-1} a_m) + (a_1 - b_1 b_m^{-1} a_m)x + \cdots + (a_{m-1} - b_{m-1} b_m^{-1} a_m)x^{m-1}.$$

So, it is evident, I hope, that $a(x) = b(x)q(x) + r(x)$, and that $\deg r(x) \leq m - 1 < m = \deg b(x)$, which proves the basis of induction (when $d = 0$).

Now, assume that the statement is true for all $a(x) \in F[x]$ with degree k such that $n \leq k < m$. We will show that it is true for all $a(x)$ of degree m. Let $a(x) = a_0 + \cdots + a_m x^m$, where $m = \deg a(x)$ and $b(x) = b_0 + \cdots + b_n x^n$, where $n = \deg b(x)$. Now, as $b_n \in F$, then $b_n^{-1} \in F$. As $m \geq n$ (from $m = \deg a(x) \geq \deg b(x) = n$), we have that $m - n \geq 0$. Thus, if we take $q_1(x) = a_m b_n^{-1} x^{m-n}$, as $m - n \geq 0$, we have $q_1(x) \in F[x]$. We are taking x^{m-n} to remove the leading term of $b(x)$ and make it into the leading term of $a(x)$. Now, let us see what happens when we take the product of $b(x)$ and $q_1(x)$:

$$\begin{aligned} b(x)q_1(x) &= (b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + b_n x^n)(a_m b_n^{-1} x^{m-n}) \\ &= b_0 a_m b_n^{-1} x^{m-n} + b_1 a_m b_n^{-1} x^{m-n+1} + \cdots + b_{n-1} a_m b_n^{-1} x^{m-1} + a_m x^m. \end{aligned}$$

Notice that then $a(x) - b(x)q_1(x)$ is equal to:

$$a_0 + \cdots + a_{m-n-1}x^{m-n-1} + (a_{m-n} - b_0 a_m b_n^{-1})x^{m-n} + \cdots + (a_{m-1} - b_{n-1} a_m b_n^{-1})x^{m-1}.$$

That implies that $\deg(a(x) - b(x)q_1(x)) \leq m - 1$. But, as $m - 1 < m$ we can apply assumption of induction on $a(x) - b(x)q_1(x)$ (by dividing with $b(x)$. We have that there exist $q_2(x), r(x) \in F[x]$ such that $a(x) - b(x)q_1(x) = b(x)q_2(x) + r(x)$, where $\deg r(x) < \deg b(x)$. From that we have $a(x) = b(x)[q_1(x) + q_2(x)] + r(x)$. Taking $q(x) = q_1(x) + q_2(x)$ proves the existence part of the theorem.

Uniqueness. Let $a(x) = b(x)q_1(x) + r_1(x)$ and $a(x) = b(x)q_2(x) + r_2(x)$, where $\deg r_1(x), \deg r_2(x) < \deg b(x)$. That implies $b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x)$, which is equivalent to $b(x)[q_1(x) - q_2(x)] = [r_2(x) - r_1(x)]$. Assume $\deg(q_1(x) - q_2(x)) \geq 0$. Then, as $F[x]$ is an integral domain,

$$\deg(b(x)[q_1(x) - q_2(x)]) = \deg b(x) + \deg(q_1(x) - q_2(x)).$$

But, that would mean that $\deg b(x) + \deg q_1(x) - q_2(x) = \deg r_2(x) - r_1(x) < \deg b(x)$ from which we would have $\deg q_1(x) - q_2(x) < 0$, which is a contradiction. Therefore, $\deg q_1(x) - q_2(x)$ is undefined and it follows that $q_1(x) - q_2(x) = 0$, i.e. $q_1(x) = q_2(x) = q(x)$. Then, $b(x)q(x) + r_1(x) = b(x)q(x) + r_2(x)$ implies $r_1(x) = r_2(x)$.

□

Problem. Let $a(x) = 2x^2 + 3x + 1$ and $b(x) = x^3 + 5x^2 + x$. Compute[80] $a(x) + b(x)$, $a(x) - b(x)$ and $a(x)b(x)$ in (a) $\mathbb{Z}[x]$, (b) $\mathbb{Z}/5\mathbb{Z}[x]$, (c) $\mathbb{Z}/6\mathbb{Z}[x]$ and (d) $\mathbb{Z}/7\mathbb{Z}[x]$.
Solution. (a) In $\mathbb{Z}[x]$, we have:

$$\begin{aligned} a(x) + b(x) &= (2x^2 + 3x + 1) + (x^3 + 5x^2 + x) = x^3 + 7x^2 + 4x + 1, \\ a(x) - b(x) &= (2x^2 + 3x + 1) - (x^3 + 5x^2 + x) = -x^3 - 3x^2 + 2x + 1, \\ a(x)b(x) &= (2x^2 + 3x + 1)(x^3 + 5x^2 + x) = 2x^5 + 13x^4 + 18x^3 + 8x^2 + x. \end{aligned}$$

We will use this to compute polynomials in (b), (c) and (d). Note that if we add two polynomials in, e.g. $\mathbb{Z}/5\mathbb{Z}[x]$, we first add their representatives, but then take residue modulo 5 to get the cosets. Therefore, for (b):

$$\begin{aligned} a(x) + b(x) &= x^3 + \overline{2}x^2 + \overline{4}x + \overline{1}, \\ a(x) - b(x) &= \overline{4}x^3 + \overline{2}x^2 + \overline{2}x + \overline{1}, \\ a(x)b(x) &= \overline{2}x^5 + \overline{3}x^4 + \overline{3}x^3 + \overline{3}x^2 + x. \end{aligned}$$

For (c):

[80] For (b), (c) and (d) we consider $a(x) = \overline{2}x^2 + \overline{3}x + \overline{1}$ and $b(x) = x^3 + \overline{5}x^2 + x$.

$$\begin{aligned} a(x)+b(x) &= x^3+\overline{1}x^2+\overline{4}x+\overline{1} \\ &= x^3+x^2+\overline{4}x+\overline{1}, \\ a(x)-b(x) &= \overline{5}x^3+\overline{3}x^2+\overline{2}x+\overline{1}, \\ a(x)b(x) &= \overline{2}x^5+\overline{1}x^4+\overline{0}x^3+\overline{2}x^2+x \\ &= \overline{2}x^5+x^4+\overline{2}x^2+x. \end{aligned}$$

Finally, for (d):

$$\begin{aligned} a(x)+b(x) &= x^3+\overline{0}x^2+\overline{4}x+\overline{1} \\ &= x^3+\overline{4}x+\overline{1}, \\ a(x)-b(x) &= \overline{6}x^3+\overline{4}x^2+\overline{2}x+\overline{1}, \\ a(x)b(x) &= \overline{2}x^5+\overline{6}x^4+\overline{4}x^3+\overline{1}x^2+x \\ &= \overline{2}x^5+\overline{6}x^4+\overline{4}x^3+x^2+x. \end{aligned}$$

Problem. Find the quotient and remainder when we divide: (a) x^3+x^2+x+1 by x^2+3x+2 in $\mathbb{Z}[x]$ and (b) $x^3+x^2+x+\overline{1}$ by $x^2+\overline{3}x+\overline{2}$ in $\mathbb{Z}/5\mathbb{Z}[x]$.

Solution. For (a):

$$\begin{array}{ll} & (x^3+x^2+x+1):(x^2+3x+2)=x-2 \\ - & \underline{(x^3+3x^2+2x)} \\ & -2x^2-x+1 \\ - & \underline{(-2x^2-6x-4)} \\ & 5x+5 \end{array}$$

We have $q(x)=x-2$ and $r(x)=5(x-1)$, so $x^3+x^2+x+1=(x^2+3x+2)(x-2)+5(x+1)$. Now, for (b) we need to take care of multiplication and addition in $\mathbb{Z}/5\mathbb{Z}$:

$$\begin{array}{ll} & (x^3+x^2+x+\overline{1}):(x^2+\overline{3}x+\overline{2})=x+\overline{3} \\ - & \underline{(x^3+\overline{3}x^2+\overline{2}x)} \\ & \overline{3}x^2+\overline{4}x+\overline{1} \\ - & \underline{(\overline{3}x^2+\overline{4}x+\overline{1})} \\ & \overline{0} \end{array}$$

That gives us $q(x) = x + \overline{3}$ and $r(x) = \overline{0}$, so $x^3 + x^2 + x + \overline{1} = (x^2 + \overline{3}x + \overline{2})(x + \overline{3})$.

Problem. Find the quotient and remainder when $x^3 + 2$ is divided by $2x^2 + 3x + 4$ in (a) $\mathbb{Z}[x]$ and when $x^3 + \overline{2}$ is divided by $\overline{2}x^2 + \overline{3}x + \overline{4}$ in (b) $\mathbb{Z}/3\mathbb{Z}[x]$ and (c) $\mathbb{Z}/5\mathbb{Z}[x]$.

Solution. Notice that we cannot use division with remainder theorem in $\mathbb{Z}[x]$ because there does not exist $m \in \mathbb{Z}$ such that $2x^2mx = x^3$, i.e. $2m = 1$. For (b), in $\mathbb{Z}/3\mathbb{Z}[x]$, first we have that $\overline{2}x^2 + \overline{3}x + \overline{4} = \overline{2}x^2 + \overline{1}$ and then:

$$\begin{array}{rl} & (x^3 + \overline{2}) : (\overline{2}x^2 + \overline{1}) = \overline{2}x \\ - & \underline{(x^3 + \overline{2}x)} \\ & -\overline{2}x + \overline{2} \end{array}$$

Therefore, $q(x) = \overline{2}x$ and $r(x) = \overline{2} - \overline{2}x = \overline{2} + x$, i.e. $x^3 + \overline{2} = (\overline{2}x^2 + \overline{1})(\overline{2}x) + (\overline{2} + x)$. For (c), or $\mathbb{Z}/5\mathbb{Z}[x]$, we have:

$$\begin{array}{rl} & (x^3 + \overline{2}) : (\overline{2}x^2 + \overline{3}x + \overline{4}) = \overline{3}x - \overline{2} \\ - & \underline{(x^3 + \overline{4}x^2 + \overline{2}x)} \\ & -\overline{4}x^2 - \overline{2}x + \overline{2} \\ - & \underline{(-\overline{4}x^2 - x - \overline{3})} \\ & -x \end{array}$$

That is, $q(x) = \overline{3}x - \overline{2} = \overline{3}(x + \overline{1})$ and $r(x) = -x = \overline{4}x$, so $x^3 + \overline{2} = (\overline{2}x^2 + \overline{3}x + \overline{4})\overline{3}(x + \overline{1}) + \overline{4}$.

Definition. Let A be a ring and $a(x), b(x) \in A[x]$. If there exists $q(x) \in A[x]$ such that $a(x) = b(x)q(x)$, we say that $b(x)$ is a **factor** of $a(x)$ and write $b(x)|a(x)$.

Proposition. Let A be a ring and $m \in \mathbb{Z}^+ - 2\mathbb{Z}$. Then, in $A[x]$:

1. $x + 1|x^m + 1$.
2. $x + 1|x^m + x^{m-1} + \cdots + x + 1$.

Proof. *Ad* 1. Proof by induction. Let $m = 1$. Then, $x + 1 = 1 \cdot (x + 1)$, so $x + 1|x + 1$. Assume the following is true for some odd m. Then we will prove it is true for $m + 2$. Using the division algorithm we get:

$$
\begin{array}{rl}
 & (x^{m+2}+1) : (x+1) = x^m x - x^m \\
- & \underline{(x^{m+2}+x^{m+1})} \\
 & -x^{m+1}+1 \\
- & \underline{(-x^{m+1}-x^m)} \\
 & 1+x^m
\end{array}
$$

We can check if that is true: $(x+1)(x^{m+1}-x^m)+(x^m+1) = (x+1)x^{m+1}-(x+1)x^m+x^m+1 = x^{m+2}+x^{m+1}-x^{m+1}-x^m+x^m+1 = x^{m+2}+1$. Indeed, $(x^{m+2}+1) = (x+1)(x^{m+1}-x^m)+(1+x^m)$. But, by assumption of induction, we have that there exists $q(x) \in A[x]$ such that $(x^m+1) = (x+1)q(x)$, so $(x^{m+2}+1) = (x+1)(x^{m+1}-x^m)+(x+1)q(x)$. That implies $(x^{m+2}+1) = (x+1)[x^{m+1}-x^m+q(x)]$. Thus, as $x^{m+1}-x^m+q(x) \in A[x]$ and that implies $x+1|x^{m+2}+1$, the statement is true for any odd m.

Ad 2. Proof by induction. Let $m = 1$. Then, $x+1|x+1$ is again obvious. Assume that $x+1|x^m+x^{m-1}+\cdots+x+1$ for some odd m. We will prove it is true for $m+2$. We have $x^{m+2}+x^{m+1}+\cdots+x+1 = (x+1)x^{m+1}+(x^m+x^{m-1}+\cdots+x+1)$. But, by assumption of induction, there exists $q(x) \in A[x]$ such that $(x^m+x^{m-1}+\cdots+x+1) = (x+1)q(x)$. Therefore, $x^{m+2}+x^{m+1}+\cdots+x+1 = (x+1)x^{m+1}+(x+1)q(x) = (x+1)[x^{m+1}+q(x)]$. As $x^{m+1}+q(x) \in A[x]$, we have that $x+1|x^{m+2}+x^{m+2}+\cdots+x+1$, and the statement is true for all odd m.

□

Proposition. Let $m \in \mathbb{Z}^+ - \{1\}$ and $n \in \mathbb{Z}^+$. In $\mathbb{Z}/m\mathbb{Z}[x]$, $x+\overline{m-1}|x^n+\overline{m-1}$.

Proof. Let $m \in \mathbb{Z}^+ - \{1\}$. We will prove the statement by induction on n. If $n = 1$, then $x+\overline{m-1}|x+\overline{m-1}$. Assume that the statement is true for some n in $\mathbb{Z}/m\mathbb{Z}[x]$, i.e. there exists $q(x) \in \mathbb{Z}/m\mathbb{Z}[x]$ such that $x^n+\overline{m-1} = (x+\overline{m-1})q(x)$. Then, for $n+1$, we have:

$$
\begin{array}{rl}
 & (x^{n+1}+\overline{m-1}) : (x+\overline{m-1}) = x^n \\
- & \underline{(x^{n+1}+\overline{m-1}x^n)} \\
 & -\overline{m-1}x^n+\overline{m-1}
\end{array}
$$

Thus, $x^{n+1}+\overline{m-1} = (x+\overline{m-1})x^n-\overline{m-1}x^n+\overline{m-1}$ and it seems we cannot use the assumption. But, we can write $-\overline{m-1} = \overline{-(m-1)} = \overline{1-m} = \overline{1}-\overline{m}$. In $\mathbb{Z}/m\mathbb{Z}$, $\overline{m} = \overline{0}$, so $-\overline{m-1} = \overline{1}-\overline{0} = \overline{1}$. Therefore, $-\overline{m-1}x^n+\overline{m-1} = x^n+\overline{m-1}$ and also

$x^{n+1} + \overline{m-1} = (x + \overline{m-1})x^n + (x^n + \overline{m-1})$. So, by assumption of induction that is equivalent to $x^{n+1} + \overline{m-1} = (x + \overline{m-1})x^n + (x + \overline{m-1})q(x)$, i.e. $x^{n+1} + \overline{m-1} = (x + \overline{m-1})(x^n + q(x))$. As $x^n, q(x) \in \mathbb{Z}/m\mathbb{Z}[x]$, then $x^n + q(x) \in \mathbb{Z}/m\mathbb{Z}[x]$, due to $\mathbb{Z}/m\mathbb{Z}[x]$ being a ring and therefore closed with respect to additives. In conclusion, $x + \overline{m-1} | x^{n+1} + \overline{m-1}$, for all $m \in \mathbb{Z}^+ - \{1\}$ and $n \in \mathbb{Z}^+$.

□

Problem. Show that there is no $m \in \mathbb{Z}$ such that $3x^2 + 4x + m | 6x^4 + 50$ in $\mathbb{Z}[x]$.

Solution. Assume that there exists $q(x) \in \mathbb{Z}[x]$ such that $6x^4+50 = q(x)(3x^2+4x+m)$. Obviously, it must be $\deg q(x) = 2$, so $q(x) = q_0+q_1x+q_2x^2$, where $q_0, q_1, q_2 \in \mathbb{Z}$. Now, $6x^4 + 50 = (q_0 + q_1x + q_2x^2)(3x^2 + 4x + m)$, i.e. $50 + 6x^4 = q_0m + (4q_0 + q_1m)x + (3q_0 + 4q_1 + q_2m)x^2 + (3q_1 + 4q_2)x^3 + 3q_2x^4$. From that we have $50 = q_0m$ and $6 = 3q_2$ (from which we get $q_2 = 2$), but also $4q_0 + q_1m = 0$, $3q_0 + 4q_1 + q_2m = 0$ and $3q_1 + 4q_2 = 0$. From the last equation we get $3q_1 + 4 \cdot 2 = 0$, i.e. $3q_1 + 8 = 0$. But, that would mean that $3q_1 = -8$, but there does not exist such $q_1 \in \mathbb{Z}$, as it would imply that $3|8$. Therefore, there does not exist m such that $3x^2+4x+m$ is a factor of $6x^4+50$ in $\mathbb{Z}[x]$.

Problem. For what values of $m \in \mathbb{Z}^+$ is $x^2 + \overline{1}$ a factor of $x^5 + \overline{5}x + \overline{6}$ in $\mathbb{Z}/m\mathbb{Z}[x]$?

Solution. We will act by division algorithm as if $\mathbb{Z}/m\mathbb{Z}[x]$ were a field, and then observe when we were taking inverses to broaden our range for m (if that happens):

$$\begin{array}{rl} & (x^5 + \overline{5}x + \overline{6}) : (x^2 + \overline{1}) = x^3 - x \\ - & \underline{(x^5 + x^3)} \\ & -x^3 + \overline{5}x + \overline{6} \\ - & \underline{(-x^3 - x)} \\ & \overline{6}x + \overline{6} \end{array}$$

We have $x^5 + \overline{5}x + \overline{6} = (x^2 + \overline{1})(x^3 - x) + (\overline{6}x + \overline{6})$. In order to $x^2 + \overline{1}$ be a factor of $x^5 + \overline{5}x + \overline{6}$ we need to have $\overline{6}x + \overline{6} = \overline{0}$ (the remainder must be zero, in the sense of a zero polynomial). Remember, we are not looking for x that will be equal to zero (this is not an equation, as x is only a placeholder). Therefore, we must have $\overline{6} = \overline{0}$ (when considering $\overline{6}x = \overline{0}x$) and $\overline{6} = \overline{0}$ (when considering $\overline{6} = \overline{0}$). Of course, that means that we must have $6 \equiv 0 \mod m$, i.e. $m|6$. So, the values of m are 2, 3 or 6 (we do not consider $m = 1$ as then we have a trivial ring, i.e. $\{0\}$) in which $x^2 + \overline{1}$ will be a factor of $x^5 + \overline{5}x + \overline{6}$ in $\mathbb{Z}/m\mathbb{Z}[x]$.

Proposition. There are $m^n(m-1)$ polynomials of degree $n \in \mathbb{Z}_0^+$ in $\mathbb{Z}/m\mathbb{Z}[x]$, where $m \in \mathbb{Z}^+ - \{1\}$.

Proof. We will observe $q(x) \in \mathbb{Z}/m\mathbb{Z}[x]$. We have $q(x) = q_0 + q_1x + \cdots + q_{n-1}x^{n-1} + q_nx^n$. Now, each for each q_i, $i \in \{0, \ldots, n\}$ we have m choices, except for q_n which cannot be zero (then degree would not be n, but $n-1$ or less), bringing us to $m-1$ choices. So, as there are n of q_i that can be zero, and only first cannot be zero. That implies that in $\mathbb{Z}/m\mathbb{Z}[x]$ there are $(m-1)\underbrace{m \cdot m \cdots m}_{n \text{ times}} = (m-1)m^n$ polynomials of degree n.

□

Problem. Let A be an integral domain. Then:

1. If $(x+1)^2 = x^2+1$ in $A[x]$, then $\operatorname{char}(A) = 2$;
2. If $(x+1)^4 = x^4+1$ in $A[x]$, then $\operatorname{char}(A) = 2$;
3. If $(x+1)^6 = x^6+2x^3+1$ in $A[x]$, then $\operatorname{char}(A) = 3$.

Solution.

1. *If* $(x+1)^2 = x^2+1$ *in* $A[x]$, *then* $\operatorname{char}(A) = 2$. We know that $(x+1)^2 = x^2+2x+1$. But, that implies $x^2+1 = x^2+2x+1$, i.e. $2x = 0$. Note here that $2 \notin A$, but $2 \in \mathbb{Z}$, as an integral multiple to symbolize $x+x$ (which is actually $1x+1x$). Also, we should not think of x as an unknown, but as a placeholder, so we have $2x = 0x$, i.e. $2 \cdot (1x) = 0x$, which is $(2 \cdot 1)x = 0x$. From that it follows that $2 \cdot 1 = 0$ (as we said polynomials are equal if their coefficients are equal). As $1+1 = 0$ in A, then obviously $\operatorname{char}(A) = 2$.

2. *If* $(x+1)^4 = x^4+1$ *in* $A[x]$, *then* $\operatorname{char}(A) = 2$. We have $(x+1)^4 = x^4+4x^3+6x^2+4x+1$. But, $x^4+1 = x^4+4x^3+6x^2+4x+1$, that is $4x^3+6x^2+4x = 0$. We can factor out $2x$ and get $2x(2x^2+3x+2) = 0$. As $A[x]$ is an integral domain, then $2x = 0$ or $2x^2+3x+2 = 0$. If $2x = 0$, then, following the same reasoning as above, $\operatorname{char}(A) = 2$. If $2x^2+3x+2 = 0$, then $2x^2+3x+2 = 0x^2+0x+0$ implies $2 \cdot 1 = 0$, $3 \cdot 1 = 0$ and $2 \cdot 1 = 0$. Now, as $2 \cdot 1 = 0$, we have $\operatorname{char}(A) = 2$. But, then $0 = 3 \cdot 1 = 2 \cdot 1 + 1 = 0 + 1 = 1$, giving us contradiction to the fact that A is an integral domain (it cannot be a trivial ring, which happens if $1 = 0$).

3. *If* $(x+1)^6 = x^6+2x^3+1$ *in* $A[x]$, *then* $\operatorname{char}(A) = 3$. We know that $(x+1)^6 = x^6+6x^5+15x^4+20x^3+15x^2+6x+1$. Then, $x^6+2x^3+1 = x^6+6x^5+15x^4+20x^3+15x^2+6x+1$, so $6x^5+15x^4+18x^3+15x^2+6x = 0$. We can factor

out $3x$ to get $3x(2x^4 + 5x^3 + 6x^2 + 5x + 2x) = 0$. As A is an integral domain, then, so is $A[x]$ and we have either $3x = 0$ or $2x^4 + 5x^3 + 6x^2 + 5x + 2x = 0$. If $3x = 0$, then, as $3x = x + x + x = 1x + 1x + 1x = 3 \cdot (1x) = (3 \cdot 1)x$, we have $3 \cdot 1 = 0$, and $\mathrm{char}\,(A) = 3$. If $2x^4 + 5x^3 + 6x^2 + 5x + 2x = 0$, then we would have $2 \cdot 1 = 0$ and $5 \cdot 1 = 0$ which is impossible because $2 \cdot 1 = 0$ would imply $0 = 5 \cdot 1 = 2 \cdot 1 + 2 \cdot 1 + 1 = 0 + 0 + 1 = 1$, that is, it would imply that A is a trivial ring, and, by definition, integral domain is a non-trivial ring.

Problem. Show that $F[x]$ can never be a field (even if F is a field).

Solution. If $F[x]$ were a field, then each element of $F[x]$ would have to be invertible. So, as $x \in F[x]$, we would have $p(x) \in F[x]$ such that $xp(x) = 1$. We know that $\deg x = 1$ and $\deg 1 = 0$. But, then, if $\deg p(x) = m$, we would have, as $F[x]$ is at least an integral domain, $\deg x + \deg p(x) = \deg 1$, i.e. $m + 1 = 0$. But, that would mean that $m = -1$, and a degree cannot be negative. If it were undefined, still we would have zero polynomial and we could not have unity as a result.

Remark. Note that, e.g. in $\mathbb{Z}/8\mathbb{Z}[x]$, we can think of divisors of zero $(\overline{4}x+\overline{4})(\overline{2}x+\overline{6}) = \overline{8}x^2 + \overline{24}x + \overline{8}x + \overline{24} = \overline{0}$. Also, we can think of an inverse by observing $(\overline{4}x + \overline{3})^2 = \overline{16}x^2+2\cdot\overline{12}x+\overline{9}$. As $2\cdot\overline{12} = \overline{12}+\overline{12} = \overline{24} = \overline{0}$ and $\overline{9} = \overline{1}$, we have $(\overline{4}x+\overline{3})(\overline{4}x+\overline{3}) = \overline{1}$. As $\mathbb{Z}/8\mathbb{Z}[x]$ is commutative, $(\overline{4}x + \overline{3})^{-1} = \overline{4}x + \overline{3}$, meaning there do exist inverse polynomials, but not in general and never can every polynomial have an inverse in a field, by a previous proposition.

Problem. Show that $A[x]$ can never have all elements different than zero and unity be divisors of zero (even if A is not an integral domain).

Solution. Assume that for all $p(x) \in A[x]$, $p(x) \neq 0, 1$, there exists $q(x) \in A[x]$, $q(x) \neq 0, 1$, such that $p(x)q(x) = 0$. That would also mean that for x there exists some $q(x) \in A[x]$, $q(x) \neq 0, 1$, such that $xq(x) = 0$. Assume $q(x) = q_0 + \cdots + q_n x^n$. Then, $xq(x) = q_0 x + \cdots + q_n x^{n-1} = 0$. But, that would imply $q_0 = q_1 = \ldots = q_n = 0$, i.e. $q(x) = 0$, which is against our assumption that $q(x) \neq 0$.

Problem. Show that in every $A[x]$, there are elements different from zero and unity that are not idempotent and that there are elements different from zero and unity that are not nilpotent.

Solution. Assume that for all $q(x) \in A[x] - \{0, 1\}$ there exists $m \in \mathbb{Z}^+$ such that $q(x)^m = 0$. That would mean, if $q(x) = x$ that $x^m = 0$, i.e. $1x^m = 0x^m$, giving us $1 = 0$ and implying that $A[x]$ is a trivial ring.

Problem. Show that if A is not an integral domain, neither is $A[x]$.

Solution. If A is not an integral domain, then there exist $a, b \in A - \{0\}$ such that $ab = 0$. But, there are constant polynomials $a, b \in A[x]$ and we would have $ab = 0$, i.e. $A[x]$ would have divisors of zero, and could not be an integral domain.

Problem. Give examples of divisors of zero, of degrees 0, 1 and 2 in $\mathbb{Z}/4\mathbb{Z}[x]$.

Solution. For degree 0, we have $\overline{2} \in \mathbb{Z}/4\mathbb{Z}[x]$ and $(\overline{2})(\overline{2}) = \overline{4} = \overline{0}$. Similarly, $(\overline{2}x)(\overline{2}x) = \overline{4}x^2 = \overline{0}$ and $(\overline{2}x^2)(\overline{2}x^2) = \overline{4}x^4 = \overline{0}$.

Problem. In $\mathbb{Z}/10\mathbb{Z}[x]$, $(\overline{2}x + \overline{2})(\overline{2}x + \overline{2}) = (\overline{2}x + \overline{2})(\overline{5}x^3 + \overline{2}x + \overline{2})$, yet $(\overline{2}x + \overline{2})$ cannot be canceled in this equation. Explain why this is possible in $\mathbb{Z}/10\mathbb{Z}[x]$, but not in $\mathbb{Z}/5\mathbb{Z}[x]$.

Solution. The reason $(\overline{2}x + \overline{2})$ cannot be cancelled is because that would imply $\overline{2}x + \overline{2} = \overline{5}x^3 + \overline{2}x + \overline{2}$, i.e. $\overline{5}x^3 = \overline{0}$. That means $\overline{5} = \overline{0}$, which is not true in $\mathbb{Z}/10\mathbb{Z}[x]$. This is due to the fact that $\mathbb{Z}/10\mathbb{Z}$ is not an integral domain, as we have $\overline{25} = \overline{0}$. But, note that this could not happen in $\mathbb{Z}/5\mathbb{Z}[x]$, as $\mathbb{Z}/5\mathbb{Z}$ is a field (because $5 \in P$), so $\mathbb{Z}/5\mathbb{Z}[x]$ is an integral domain and cancellation law holds.

Problem. Give examples (a) in $\mathbb{Z}/4\mathbb{Z}[x]$, (b) in $\mathbb{Z}/6\mathbb{Z}[x]$ and (c) in $\mathbb{Z}/9\mathbb{Z}[x]$ of polynomials $a(x)$ and $b(x)$ such that $\deg a(x)b(x) < \deg a(x) + \deg b(x)$.

Solution. (a) For, $\mathbb{Z}/4\mathbb{Z}[x]$, we have $a(x) = \overline{2}x + \overline{1}$, $\deg a(x) = 1$ and $b(x) = \overline{2}x^2 + \overline{3}$, $\deg b(x) = 2$. Then, $a(x)b(x) = (\overline{2}x + \overline{1})(\overline{2}x^2 + \overline{3}) = \overline{4}x^3 + \overline{2}x^2 + \overline{3} + \overline{6}x = \overline{2}x^2 + \overline{2}x + \overline{3}$, so $\deg a(x)b(x) = 2 < 2 + 1 = \deg a(x) + \deg b(x)$. (b) In $\mathbb{Z}/6\mathbb{Z}[x]$, take $a(x) = \overline{2}x^2$ and $b(x) = \overline{3}x + \overline{1}$. Then, $\deg a(x) = 2$ and $\deg b(x) = 1$. So, $a(x)b(x) = \overline{6}x^3 + \overline{2}x^2 = \overline{2}x^2$. We see that $\deg a(x)b(x) = 2 < 2 + 1 = \deg a(x) + \deg b(x)$. (c) In $\mathbb{Z}/9\mathbb{Z}[x]$, we have $a(x) = \overline{3}x^2 + \overline{1}$ and $b(x) = \overline{3}x^4 + \overline{2}$, so $a(x)b(x) = \overline{9}x^6 + \overline{3}x^4 + \overline{6}x^2 + \overline{2} = \overline{3}x^4 + \overline{6}x^2 + \overline{2}$. So, $\deg a(x)b(x) = 4 < 2 + 4 = \deg a(x) + \deg b(x)$.

Proposition. Let A be a ring that is not an integral domain. Then, there exist $a(x), b(x) \in A[x]$ such that $\deg a(x)b(x) < \deg a(x) + \deg b(x)$.

Proof. Let A be a ring such that A is not an integral domain. Then, there exist $a, b \in A$, such that $ab = 0$ and $a \neq 0$ and $b \neq 0$. But, then $ax + 1, b \in A[x]$. We have $\deg a(x) + \deg b(x) = 1 + 0 = 1$ and $a(x)b(x) = (ax + 1)b = abx + b = 0x + b = b$, so $\deg a(x)b(x) = 0 < 1 \deg a(x) + \deg b(x)$.

□

Proposition. If A is an integral domain, then the only invertible non-zero elements in $A[x]$ are constant polynomials.

Proof. Let $a(x), b(x) \in A[x]$ with $\deg a(x) = m$ and $\deg a(x) = n$, where $m, n \in \mathbb{Z}_0^+$. Assume $a(x)b(x) = 1$. Then, as A is an integral domain, also $A[x]$ is an integral domain and we have $\deg a(x)b(x) = \deg a(x) + \deg b(x) = m + n$ and $\deg 1 = 0$. That would imply $0 = m + n$. But, as $m, n \in \mathbb{Z}_0^+$, it can on only be that $m = n = 0$, i.e. $a(x)$ and $b(x)$ are constant polynomials.

□

Problem. Show that in $\mathbb{Z}/4\mathbb{Z}[x]$ there are invertible polynomials of all degrees.

Solution. We can take our inspiration from $(\overline{2}x + \overline{3})(\overline{2}x + \overline{3}) = \overline{4}x^2 + (\overline{6} + \overline{6})x + \overline{9} = \overline{12}x + \overline{1} = \overline{1}$. Let $m \in \mathbb{Z}^+$ and $a(x) = \overline{a_m}x^m + \overline{a_0}$, $b(x) = \overline{b_m}x^m + \overline{b_0}$ with $\overline{a_m}, \overline{b_m} \neq \overline{0}$. Then, we want $a(x)b(x) = \overline{a_m b_m}x^{2m} + \overline{a_m b_0 + b_m a_0}x^m + \overline{a_0 b_0} = \overline{1}$. But, that means that $\overline{a_m b_m} = \overline{0}$, and as $\overline{a_m}, \overline{b_m} \neq \overline{0}$, it must be $\overline{a_m} = \overline{b_m} = 2$. Also, it must be that $\overline{a_0 b_0} = \overline{1}$. But, in $\mathbb{Z}/4\mathbb{Z}$, the only invertible elements are $\overline{1}$ and $\overline{3}$ (as they are relatively prime to and less than 4). Also $\overline{1 \cdot 1} = \overline{1}$ and $\overline{3 \cdot 3} = \overline{9} = \overline{1}$. If it were that $\overline{a_0} = \overline{b_0} = 1$, we would also need $\overline{a_m b_0 + b_m a_0} = \overline{0}$, i.e. $\overline{2 \cdot 1 + 2 \cdot 1} = \overline{4} = \overline{0}$, so that would work. If it were that $\overline{a_0} = \overline{b_0} = 3$, then we would need $\overline{3 \cdot 2 + 3 \cdot 2} = \overline{12} = \overline{0}$. Therefore, $\left[\overline{2}x^m + \overline{1}\right]^{-1} = \overline{2}x^m + \overline{1}$ and $\left[\overline{2}x^m + \overline{3}\right]^{-1} = \overline{2}x^m + \overline{3}$.

Problem. Give all the ways of factoring x^2 into two polynomials of degree 1 in $\mathbb{Z}/9\mathbb{Z}[x]$ and $\mathbb{Z}/5\mathbb{Z}[x]$.

Solution. We know that $\deg x^2 = 2$, so if $a(x) = \overline{a_1}x + \overline{a_0}$ and $b(x) = \overline{b_1}x + \overline{b_0}$, we insist that $\deg a(x) = 1$ and $\deg b(x) = 1$, implying $\overline{a_1}, \overline{b_1} \neq \overline{0}$. Let us observe $a(x)b(x) = \overline{a_1 b_1}x^2 + \overline{a_1 b_0 + b_1 a_0}x + \overline{a_0 b_0}$. Then we must have $\overline{a_1 b_1} = \overline{1}$, and the invertible elements in $\mathbb{Z}/9\mathbb{Z}$ are $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{7}$ and $\overline{8}$. We notice that that gives us four cases: (a) $\overline{a_1} = \overline{b_1} = \overline{1}$, (b) $\overline{a_1} = \overline{2}$ and $\overline{b_1} = \overline{5}$, (c) $\overline{a_1} = \overline{4}$ and $\overline{b_1} = \overline{7}$ and (d) $\overline{a_1} = \overline{b_1} = \overline{8}$. Notice that in all cases we must have $\overline{a_0 b_1 + a_1 b_0} = \overline{a_0 b_0} = \overline{0}$, the candidates for which can only be $\overline{0}$ (which we will examine later), $\overline{3}$ and $\overline{6}$. We will give an example how to work out the first case and then list all the other cases. (a) We have $\overline{a_1} = \overline{b_1} = \overline{1}$. Then, $\overline{a_0 b_1 + a_1 b_0} = \overline{a_0 \cdot 1 + 1 \cdot b_0} = \overline{a_0 + b_0}$. If $\overline{a_0} = \overline{3}$, then we can take $\overline{b_0} \in \{\overline{3}, \overline{6}\}$. Also, if $\overline{a_0} = \overline{6}$, then we have $\overline{b_0} \in \{\overline{3}, \overline{6}\}$. But can it be that $\overline{a_0} = \overline{b_0}$? Then we would have $\overline{3 + 3} = \overline{6} \neq \overline{0}$ or $\overline{6 + 6} = \overline{12} = \overline{3} \neq \overline{0}$. So, we have the only option:

$$x^2 = \left(x + \overline{3}\right)\left(x + \overline{6}\right).$$

It would be tedious to write the same process over and over again, so I will list all other possibilities:

$$\begin{aligned} x^2 &= \left(\overline{2}x+\overline{3}\right)\left(\overline{5}x+\overline{6}\right) \\ &= \left(\overline{2}x+\overline{6}\right)\left(\overline{5}x+\overline{3}\right) \\ &= \left(\overline{4}x+\overline{3}\right)\left(\overline{7}x+\overline{6}\right) \\ &= \left(\overline{4}x+\overline{6}\right)\left(\overline{7}x+\overline{3}\right) \\ &= \left(\overline{8}x+\overline{3}\right)\left(\overline{8}x+\overline{6}\right). \end{aligned}$$

Now, if we also consider $\overline{a_0}=\overline{b_0}=\overline{0}$, we would have:

$$x^2 = x\cdot x = \left(\overline{2}x\right)\left(\overline{5}x\right) = \left(\overline{4}x\right)\left(\overline{7}x\right) = \left(\overline{8}x\right)\left(\overline{8}x\right).$$

Now, in $\mathbb{Z}/5\mathbb{Z}[x]$, there are no zero divisors, so there is no way we can get rid of $\overline{a_0b_0}$ except by setting $\overline{a_0}=\overline{b_0}=\overline{0}$. Then, $\overline{a_0b_1+b_0a_1}=\overline{0\cdot b_1+0\cdot a_1}=\overline{0+0}=\overline{0}$. And, the invertible elements are, $\overline{1}$, $\overline{2}$ and $\overline{3}$, $\overline{4}$. So, we only have:

$$x^2 = x\cdot x = \left(\overline{2}x\right)\left(\overline{3}x\right) = \left(\overline{4}x\right)\left(\overline{4}x\right).$$

Problem. (a) Find all the square roots of $x^2+x+\overline{4}\in\mathbb{Z}/5\mathbb{Z}[x]$. (b) Show that in $\mathbb{Z}/8\mathbb{Z}[x]$, there are infinitely many square roots of $\overline{1}$.

Solution. (a) We want to find $a(x)\in\mathbb{Z}/5\mathbb{Z}[x]$ such that $[a(x)]^2=x^2+x+\overline{4}$. As $\mathbb{Z}/5\mathbb{Z}$ is a field, due to 5 being prime, then it must be $\deg\left(x^2+x+\overline{4}\right)=2=\deg\left([a(x)]^2\right)=\deg\left(a(x)a(x)\right)=\deg a(x)+\deg a(x)=2\deg a(x)$, i.e. $\deg a(x)=1$. So, $a(x)=\overline{a_1}x+\overline{a_0}$. We have $\left(\overline{a_1}x+\overline{a_0}\right)^2=\overline{a_1^2}x^2+\overline{2a_1a_0}x+\overline{a_0^2}=x^2+x+\overline{4}$. So, it must be that $\overline{a_0^2}=\overline{4}$. Surely, we can have $\overline{a_0}\in\{\overline{2},\overline{3}\}$. Similarly, we have $\overline{a_1^2}=\overline{1}$ and that implies $\overline{a_1}\in\{\overline{1},\overline{4}\}$. Finally, we have $\overline{2a_1a_0}=\overline{1}$, i.e. $\overline{2}\overline{a_1a_0}=\overline{1}$. Multiplying that equality by $\overline{3}$ gives us $\overline{a_1a_0}=\overline{3}$. Assume $\overline{a_0}=\overline{2}$. Assume $\overline{a_1}=\overline{1}$. That cannot be, due to the latter condition. Assume $\overline{a_1}=\overline{4}$. That can be, as $\overline{a_0a_1}=\overline{2\cdot4}=\overline{8}=\overline{3}$. So, we have:

$$\left(\overline{4}x+\overline{2}\right)^2=\overline{16}x^2+\overline{2\cdot4\cdot2}x+\overline{4}=x^2+x+\overline{4}.$$

Now, assume $\overline{a_0}=\overline{3}$. Let $\overline{a_1}=\overline{1}$. That can be as $\overline{1\cdot3}=\overline{3}$ and we have:

$$\left(x+\overline{3}\right)^2 = x^2 + \overline{6}x + \overline{9} = x^2 + x + \overline{4}.$$

Finally, assume $\overline{a_1} = \overline{4}$. That cannot be as $\overline{3 \cdot 4} = \overline{2}$. So, the only square roots of $x^2 + x + \overline{4}$ are the forementioned two. (b) Let $a(x) = \overline{a_m}x^m + \overline{a_0}$, where $\overline{a_m}, \overline{a_0} \in \mathbb{Z}/8\mathbb{Z}$ and $m \in \mathbb{Z}^+$. We have $(\overline{a_m}x^m + \overline{a_0})^2 = \overline{a_m^2}x^{2m} + \overline{2a_m a_0}x + \overline{a_0^2} = \overline{1}$. Now, we must have $\overline{a_m^2} = \overline{0}$, but $\overline{a_m} \neq 0$, then $\overline{2a_m a_0} = 0$ and $\overline{a_0^2} = \overline{1}$. It can easily be checked that $\overline{a_0} \in \{\overline{1}, \overline{5}, \overline{7}\}$ and $\overline{a_m} = \overline{4}$. Now, we only need $\overline{2 \cdot 4a_0} = \overline{0}$, i.e. $\overline{8a_0} = \overline{0}$. But, that is always true, so our choice of $\overline{a_0}$ is arbitrary. We have:

$$\begin{aligned}
\left(\overline{4}x^m + \overline{1}\right)^2 &= \overline{1}, \\
\left(\overline{4}x^m + \overline{5}\right)^2 &= \overline{1}, \\
\left(\overline{4}x^m + \overline{7}\right)^2 &= \overline{1}.
\end{aligned}$$

As this is true for all $m \in \mathbb{Z}^+$, there are infinitely many square roots of $\overline{1} \in \mathbb{Z}/8\mathbb{Z}[x]$.

Proposition. Let A be an integral domain. If $\mathrm{char}\,(A) = p$, then $\mathrm{char}\,(A[x]) = p$.

Proof. As $\mathrm{char}\,(A) = p$, then $p \cdot 1 = 0$. Now, take $u(x) \in A[x]$ where $u(x) = 1$, i.e. $u(x)$ is unity in $A[x]$. Then, $p \cdot u(x) = p \cdot 1 = 0$. If it were that $q \cdot u(x) = 0$, for some $0 \leq q < p$, we would have $q \cdot u(x) = q \cdot 1 = 0$, and that would contradict the fact that $p = \mathrm{char}\,(A)$ (it has to be the least number satisfying that condition).

□

Problem. Give an example of an infinite integral domain with finite characteristic.

Solution. We know that $\mathbb{Z}/p\mathbb{Z}$, for $p \in P$, is an integral domain and that $p \cdot \overline{1} = \overline{0}$. Then, $\mathbb{Z}/p\mathbb{Z}[x]$ is also an integral domain and we have $p \cdot \overline{1} = \overline{0}$, where $\overline{1}, \overline{0} \in \mathbb{Z}/p\mathbb{Z}[x]$ are its unity and zero, respectively (corresponding to unity and zeto in $\mathbb{Z}/p\mathbb{Z}$). But, $\mathbb{Z}/p\mathbb{Z}[x]$ is infinite because every $p(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ is of the form $p(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_m}x^m$. As $m \in \mathbb{Z}^+$, there are infinitely many polynomials (when considering their degrees).

Proposition. Let A be a ring with unity. Then, $x - 1 | x^m - 1$, for all $m \in \mathbb{Z}^+$.

Proof. Let $m = 1$. Then, $(x-1) \cdot 1 = x - 1 = x^1 - 1$. Assume the statement is true for some m, i.e. there exists $q(x) \in A[x]$ such that $(x-1)q(x) = x^m - 1$. Now, let us prove it is true for $m+1$. We have $x^{m+1} - 1 = x^m x - x + x - 1 = x(x^m - 1) + (x - 1)$. But, by assumption, $x^m - 1 = (x-1)q(x)$, so we have $x^{m+1} - 1 = x(x-1)q(x) + (x-1) = (x-1)(xq(x) + 1)$. Therefore, $x - 1 | x^{m+1} - 1$ so the statement is true for all $m \in \mathbb{Z}^+$.

□

Proposition. Let A be an integral domain where $1_A \in A$ denotes unity in A. If $\text{char}\,(A) = p$, for some $p \in P$, then $x + (p-1) \cdot 1_A$ is a factor of $x^m + (p-1) \cdot 1_A$, for all $m \in \mathbb{Z}^+$.

Proof. We have $x + (p-1) \cdot 1_A = x + p \cdot 1_A - 1 \cdot 1_A$. As $\text{char}\,(A) = p$, then $p \cdot 1_A = 0$, so $x + (p-1) \cdot 1_A = x - 1_A$. Similarly, $x^m + (p-1) \cdot 1_A = x^m - 1_A$, and the rest of the proof follows from the previous proposition.

□

Proposition. Let A be an integral domain, $a \in A$ and let $\text{char}\,(A) = p$, for some $p \in P$. Then[81], in $A[x]$, $(ax + c)^p = a^p x^p + c^p$, for all $c \in A$.

Proof. Using the binomial formula, we have:

$$(ax + c)^p = \sum_{k=0}^{p} \binom{p}{k} (ax)^k c^{p-k}.$$

Now, we remember that $p | \binom{p}{k}$ for all $k \in \{1, \ldots, p-1\}$. So, there exists $z_k \in \mathbb{Z}$ such that $\binom{p}{k} = z_k p$, for all $k \in \{1, \ldots, p-1\}$. Also notice that $\binom{p}{0} = 1$ and $\binom{p}{p} = 1$. Thus, we have:

$$(ax + c)^p = (ax)^p + \sum_{k=1}^{p-1} (z_k p) \cdot ((ax)^k c^{p-k}) + c^p.$$

As $\text{char}\,(A) = p$, then $\text{char}\,(A[x]) = p$, so $(z_k p) \cdot ((ax)^k c^{p-k}) = p \cdot (z_k \cdot ((ax)^k c^{p-k})) = 0$. Therefore, we are only left with $(ax + c)^p = (ax)^p + c^p = a^p x^p + c^p$.

□

Proposition. Let A be an integral domain and $\text{char}\,(A) = p$, for some $p \in P$. Let $m \in \mathbb{Z}_0^+$ and $a_i \in A$, for $i \in \{0, \ldots, m\}$. Then:

$$(a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0)^p = a_m^p x^{mp} + a_{m-1}^p x^{(m-1)p} + \cdots + a_1^p x^p + a_0^p.$$

Proof. Let $m = 0$. Then $(a_0)^p = a_0^p$. If $m = 1$, then by previous proposition,

[81] One should conduct a proof with some care here, as using the previous result that $(a+c)^p = a^p + c^p$ for all $a, c \in A$ would be invalid. That is because of the definition of x as a placeholder, not as an element of A, so the equality must imply that degrees and coefficients are equal. Exempli gratia, in $\mathbb{Z}/2\mathbb{Z}$, $a^2 + 1 = a^4 + 1$, but, in $\mathbb{Z}/2\mathbb{Z}[x]$, $x^2 + 1 \neq x^4 + 1$.

$(a_1x+a_0)^p = a_1^px^p+a_0^p$. Assume the statement is true for some $m \in \mathbb{Z}_0^+$. We will prove that it implies truth for $m+1$. We have:

$$(a_{m+1}x^{m+1} + \cdots + a_1x + a_0)^p = (a_{m+1}x^{m+1} + (a_mx^m + \cdots + a_1x + a_0))^p.$$

It is easy to see, by observing previous proposition, that:

$$(a_{m+1}x^{m+1} + (a_mx^m + \cdots + a_1x + a_0))^p = a_{m+1}^px^{(m+1)p} + (a_mx^m + \cdots + a_1x + a_0)^p.$$

Using the assumption of induction we get:

$$a_{m+1}^px^{(m+1)p} + (a_mx^m + \cdots + a_1x + a_0)^p = a_{m+1}^px^{(m+1)p} + a_m^px^{mp} + \cdots + a_1^px^p + a_0^p.$$

Therefore, by principle of mathematical induction, the statement is true for all $m \in \mathbb{Z}_0^+$.

□

Proposition. Let A be a ring. If $B \leq A$, then $B[x] \leq A[x]$.

Proof. Let $b(x) \in B[x]$. Then $b(x) = b_mx^m + \cdots + b_1x + b_0$, where $b_i \in B$, for all $i \in \{0, \ldots, m\}$. But, as $B \leq A$, then also $b_i \in A$. So, $b(x) \in A[x]$ and $B[x] \subseteq A[x]$. Let $b(x), b'(x) \in B[x]$. Then, if $b(x) = b_mx^m+\cdots+b_1x+b_0$ and $b'(x) = b'_mx^m+\cdots+b'_1x+b'_0$ (allowing some b'_i or b_i to be zero), we have $b(x) - b'(x) = (b_m - b'_m)x^m + \cdots + (b_1 - b'_1)x+(b_0-b'_0)$. It is obvious that $b_i-b'_i \in B$ because $B \leq A$, so also $b(x)-b'(x) \in B[x]$. Finally, one can see that $b(x)b'(x) \in B[x]$ because the coefficients in $b(x)b'(x)$ consist of factors of coefficients of $b(x)$ and $b'(x)$, and as $B \leq A$, that implies that the coefficients remain in B. From that we have $b(x)b'(x) \in B[x]$ and $B[x] \leq A[x]$.

□

Proposition. Let A be a ring. If $B \trianglelefteq A$, then $B[x] \trianglelefteq A[x]$.

Proof. By the previous proposition, $B[x] \leq A[x]$. If $a(x) \in A[x]$ and $b(x) \in B[x]$, then the coefficients in $a(x)b(x)$ (or $b(x)a(x)$) consists of factors of coefficients $a_i \in A$ and $b_i \in B$. But, as $B \trianglelefteq A$, those coefficients are again in B, so $a(x)b(x) \in B[x]$ (and similarly $b(x)a(x) \in B[x]$).

□

Proposition. Let A be a ring and $S = \{a^m x^m + \cdots + a_1 x + a_0 \in A[x] : \ a_i = 0 \text{ for odd } i)\}$. Then, $S \leq A[x]$.

Proof. It is obvious from definition of S that $S \subseteq A[x]$. Take $a(x), b(x) \in S$ with $a(x) = a_m x^m + \cdots + a_1 x + a_0$ and $b(x) = b_m x^m + \cdots + b_1 x + b_0$ (allowing some a_i or b_i to be zero, so they are not necessarily of the same degree). It is also obvious that the difference $a_i - b_i$ will be zero for odd i, so $a(x) - b(x) \in S$. Then, let us odd coefficients in $a(x)b(x)$:

$$c_k = \sum_{i+j=k} a_i b_j.$$

If k is odd, then either i is odd or j is odd (they cannot be both even or both odd). Therefore, either $a_i = 0$ or $b_j = 0$ so always $a_i b_j = 0$ and the sum of zeros is again zero. Therefore, $a(x)b(x) \in S$ and $S \leq A[x]$.

□

Remark. Notice that the proposition above does not hold for polynomials if all even-indexed coefficents are equal to zero, because in multiplication we would allow both of them to be odd-indexed, and not necessarily equal to zero. Due to the same fact S is not necessarily an ideal of $A[x]$.

Proposition. Let A be a ring. Let $J = \{a_m x^m + \cdots + a_1 x + a_0 \in A[x] : \ a_0 = 0\}$. Then, $J \trianglelefteq A[x]$. If A is an integral domain, then J is a prime ideal of $A[x]$.

Proof. Obviously $J \subseteq A$. Let $a(x), b(x) \in J$, i.e. $a(x) = a_m x^m + \cdots + a_1 x$ and $b(x) = b_m x^m + \cdots + b_1 x$ (allowing some coefficients to be zero). Then, constant coefficient of $a(x) - b(x)$ is obviously equal to zero and the constant coefficient of $a(x)b(x)$ is just $a_0 b_0$, so it is again zero. If we take some other $c(x) \in A[x]$, then constant coefficient of $c(x)a(x)$ is $c_0 a_0$, i.e. $c_0 0$ so it is zero. Same goes for $a(x)c(x)$ so we have $J \trianglelefteq A[x]$. But, if we take $a(x)b(x) \in J$, that means that $a_0 b_0 = 0$. But, as A is an integral domain, either $a_0 = 0$ or $b_0 = 0$. So, it must be that either $a(x) \in J$ or $b(x) \in J$, meaning J is a prime ideal of $A[x]$.

□

Proposition. Let A be a ring and $J = \{a_m x^m + \cdots + a_1 x + a_0 \in A[x] : \ a_m + \cdots + a_1 + a_0 = 0\}$. Then, $J \trianglelefteq A[x]$. If A is an integral domain, then J is a prime ideal of $A[x]$.

Proof. From definition of J, we have that $J \subseteq A$. If we take $a(x), b(x) \in J$ with

$a(x) = a_m x^m + \cdots + a_1 x + a_0$ and $b(x) = b_m x^m + \cdots + b_1 x + b_0$ (granting some b_i might be equal to zero, which does not change the definition of the set), we have $a_m + \cdots + a_1 + a_0 = 0$ and $b_m + \cdots + b_1 + b_0 = 0$. If we take c_i as the i-th coefficient of the difference $a(x) - b(x)$, then $c_i = a_i - b_i$. But, $c_m + \cdots + c_1 + c_0 = (a_m - b_m) + \cdots + (a_1 - b_1) + (a_0 - b_0) = (a_m + \cdots + a_1 + a_0) - (b_m + \cdots + b_1 + b_0) = 0 - 0 = 0$, so $a(x) - b(x) \in J$. Now, we will move ahead to simplify the proof. Notice that the sum of coefficients can be obtained by substituting x with 1. So, the sum of coefficients of $c(x) = a(x)b(x)$ is equal to $c(1)$ and that is of course $c(1) = a(1)b(1)$. Therefore, as $a(1) = 0$ and $b(1) = 0$ it must be that $c(1) = 0 \cdot 0 = 0$. Similarly, if $a(x) \in J$ and $b(x) \in A[x]$, then $a(1)b(1) = 0 \cdot b(1) = 0$, so $a(x)b(x) \in J$ (same goes for $b(x)a(x)$). Thus, $J \trianglelefteq A[x]$.

□

Proposition. Let A be an integral domain. Then[82], $A[x]/\langle x \rangle \cong A$.

Proof. Let $f : A[x] \to A$ be a mapping defined with $h(a^m + \cdots + a_1 x + a_0) = a_0$, for all $a^m + \cdots + a_1 x + a_0 \in A[x]$. It is easy to see from definition of f that it is a well-defined function. If we take $a(x) \in A[x]$, then it has a constant term, so there exists $a_0 \in A$ so that $f(a(x)) = a_0$. If we take $a(x), b(x) \in A[x]$, and $a(x) = b(x)$, then their degrees are equal and their respective coefficients are equal, and so are their constant terms, i.e. $a_0 = b_0$, so that implies $f(a(x)) = f(b(x))$. Now that we have argued that f is a well-defined function, we need to show that it is surjective. If we take $a_0 \in A$, then simply $a_0 \in A[x]$, so $f(a_0) = a_0$. Now, let $a(x), b(x) \in A[x]$ with $a(x) = a_m x^m + \cdots + a_1 x + a_0$ and $b(x) = b_m x^m + \cdots + b_1 x + b_0$ (allowing some b_i to be equal to zero). Then, $f(a(x) + b(x)) = f((a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)) = a_0 + b_0 = f(a(x)) + f(b(x))$ and $f((a_m x^m + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0)) = f(c_{2m} x^{2m} + \cdots + c_1 x + c_0)$, where $c_k = \sum_{i+j=k} a_i b_j$, for all $k \in \{0, \ldots, 2m\}$. Then, $c_0 = a_0 b_0$, so $f(a(x)b(x)) = a_0 b_0 = f(a(x))f(b(x))$. Therefore, as f is a surjective homomorphism, we can apply the fundamental homomorphism theorem for rings. We have $A[x]/\ker(f) \cong A$. The only thing left is to investigete the kernel of f. We have $\ker(f) = \{a_m x^m + \cdots + a_1 x + a_0 \in A[x] : \ a_0 = 0\} = \{a_m x^m + \cdots + a_1 x \in A[x]\} = \{x(a_m x^{m-1} + \cdots + a_1) \in A[x]\}$. That reminds us exactly of $\langle x \rangle$. If we take $a(x) \in \langle x \rangle$, then $a(x) = xb(x)$, for some $b(x) \in A[x]$, i.e. constant term of $a(x)$ is equal to zero, so $a(x) \in \ker(f)$, i.e. $\langle x \rangle \subseteq \ker(f)$. If we take $a(x) \in \ker(f)$, then it is equal to $xb(x)$, where $b(x) \in A[x]$. But, that precisely means that $xb(x) \in \langle x \rangle$, i.e. $a(x) \in \langle x \rangle$. The result of that is $\ker(f) \subseteq \langle x \rangle$ implying $\ker(f) = \langle x \rangle$. Thus we have $A[x]/\langle x \rangle \cong A$.

□

[82]Do not confuse the notation for principal ideal with that of a cyclic group; if G were a group and $x \in G$, then $\langle x \rangle = \{x^m : \ m \in \mathbb{Z}\}$. But here, as $x \in A[x]$ (regard it as $1 \cdot x$ for easier understanding), then $\langle x \rangle = \{xa(x) : \ a(x) \in A[x]\}$.

Problem. Let A be an integral domain and $g : A[x] \to A$ send every polynomial to the sum of its coefficients. Prove that g is a surjective homomorphism, and describe its kernel.

Solution. Let g be defined with $g(a_m x^m + \cdots + a_1 x + a_0) = a_m + \cdots + a_1 + a_0$. Then, g is obviously defined for all $a(x) \in A[x]$ and $a_m x^m + \cdots + a_1 x + a_0 = b_m x^m + \cdots + b_1 x + b_0$ implies $a_i = b_i$, so $a_m + \cdots + a_1 + a_0 = b_m + \cdots + b_1 + b_0$ (can be proven inductively), for all $a_m x^m + \cdots + a_1 x + a_0 \in A[x]$ and $b_m x^m + \cdots + b_1 x + b_0 \in A[x]$ (allowing some b_i to be equal to zero). Then, if we take $a \in A$, there exists $a \in A[x]$ such that $g(a) = a$. Thus, g is surjective. Finally, if $a_m x^m + \cdots + a_1 x + a_0, b_m x^m + \cdots + b_1 x + b_0 \in A[x]$ (allowing some b_i to be equal to zero), then, $g((a_m x^m + \cdots + a_1 x + a_0) + (b_m x^m + \cdots + b_1 x + b_0)) = g((a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)) = (a_m + b_m) + \cdots + (a_1 + b_1) + (a_0 + b_0) = (a_m + \cdots + a_1 + a_0) + (b_m + \cdots + b_1 + b_0) = g(a_m x^m + \cdots + a_1 x + a_0) + g(b_m x^m + \cdots + b_1 x + b_0)$. Also, $g((a_m x^m + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0)) = g(c_{2m} x^{2m} + \cdots + c_1 x + c_0) = c_{2m} + \cdots + c_1 + c_0$, where $c_k = \sum_{i+j=k} a_i b_j$, for all $k \in \{0, \ldots, 2m\}$. We realize that $a(x)b(x) = c(x)$ implies $a(1)b(1) = c(1)$. But, $c_{2m} + \cdots + c_1 + c_0 = c(1)$, so $c_{2m} + \cdots + c_1 + c_0 = a(1)b(1)$, i.e. $c_{2m} + \cdots + c_1 + c_0 = (a_m + \cdots + a_1 + a_0)(b_m + \cdots + b_1 + b_0)$. Therefore, $g((a_m x^m + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0)) = (a_m + \cdots + a_1 + a_0)(b_m + \cdots + b_1 + b_0) = g(a(x))g(b(x))$. Therefore, g is an injective homomorphism and we can apply fundamental homomorphism theorem to obtain $A[x]/\ker(g) \cong A$. It is obvious to see that $\ker(g) = \{a_m x^m + \cdots + a_1 x + a_0 \in A[x] : \ a_m + \cdots + a_1 + a_0 = 0\}$, which is equal to the ideal J of $A[x]$ described in a previous proposition.

Proposition. Let A be an integral domain and $c \in A$. Let $h : A[x] \to A[x]$ be defined by $h(a(x)) = a(cx)$. Then, h is an automorphism if and only if c is invertible.

Proof. First we will prove that h is a homomorphism. Take $a(x) \in A[x]$ with $a(x) = a_m x^m + \cdots + a_1 x + a_0$. Then, $a(cx) = a_m(cx)^m + \cdots + a_1(cx) + a_0 = a_m c^m x^m + \cdots + a_1 cx + a_0$. As $a_i c^i \in A$, then $a(cx) \in A[x]$. Also, if $b(x) \in A[x]$ with $b(x) = b_m x^m + \cdots + b_1 x + b_0$ (allowing some b_i to be equal to zero) and $a(x) = b(x)$, then $a_i = b_i$, for all $i \in \{0, \ldots, m\}$. That implies $a_i c^i = b_i c^i$, i.e. $a_m c^m x^m + \cdots + a_1 cx + a_0 = b_m c^m x^m + \cdots + b_1 cx + b_0$, i.e. $a(cx) = b(cx)$. That is equivalent to $h(a(x)) = h(b(x))$ implying that h is well-defined. Then, $h(a(x) + b(x)) = h((a_m x^m + \cdots + a_1 x + a_0) + (b_m x^m + \cdots + b_1 x + b_0)) = h((a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)) = (a_m + b_m)c^m x^m + \cdots + (a_1 + b_1)cx + (a_0 + b_0) = (a_m c^m x^m + \cdots + a_1 cx + a_0) + (b_m c^m x^m + \cdots + b_1 cx + b_0) = h(a(x)) + h(b(x))$. From that follows that h is a homomorphism.

Necessity. Assume h is automorphism. We must show that c is invertible. Let $a(x) = x$. Then, as $a(x) \in A[x]$ and h is surjective, there exists $b(x) \in A[x]$ such that $h(b(x)) = x$, i.e. $b(cx) = x$. As polynomial $b(cx)$ is equal to x it also must be of degree 1 and have all other coefficients (except b_1) zero. That means that $b(cx) = b_1(cx)$.

As coefficients for $b_1(cx)$ and x (read $1x$) must be equal, then $b_1c = 1$. As $A[x]$ is commutative then also $cb_1 = 1$ and it follows that c is invertible.

Sufficiency. Assume c is invertible. Then, if $h(a(x)) = h(b(x))$, we have $a(cx) = b(cx)$. That means that coefficients of $a(cx)$ and $b(cx)$ are equal and the two polynomials are of equal degrees. So we have $c^i a_i = c^i b_i$. But, as c is invertible, we can multiply that by c^{-i} and get $a_i = b_i$, meaning $a(x) = b(x)$, i.e. h is injective. Also, if we take $a(x) \in A[x]$, then we must prove that there exists $b(x) \in A[x]$ such that $h(b(x)) = a(x)$. But, as $h(b(x)) = b(cx)$, we have $b(cx) = a(x)$. It is obvious that it must be $b(x) = a(c^{-1}x)$. Then, we have $b(cx) = a(c^{-1}cx) = a(x)$. Therefore, h is surjective, and h is an automorphism.

□

Proposition. Let A and B be rings and let $h : A \underset{K}{\longrightarrow} B$ be a homomorphism. Let[83] $\overline{h} : A[x] \to B[x]$ be defined as

$$\overline{h}(a_0 + a_1x + \cdots + a_nx^n) = h(a_0) + h(a_1)x + \cdots + h(a_m)x^m.$$

Then:

1. $\overline{h}$ is homomorphism.
2. $\overline{h}$ is surjective if and only if h is surjective.
3. $\overline{h}$ is injective if and only if h is injective.

Proof. *Ad* 1. If we take $a(x) \in A[x]$, then $a(x) = a_0 + a_1x + \cdots + a_mx^m$. As h is a well-defined function by assumption, then there exist $h(a_i)$ such that $\overline{h}(a(x)) = h(a_0) + h(a_1)x + \cdots + h(a_m)x^m$, so $\overline{h}$ is well-defined. Also, if $a(x) = b(x)$, then $a_i = b_i$ and so, as h has a property of uniqueness, $h(a_i) = h(b_i)$. Therefore, the coefficients of $\overline{h}(a(x))$ and $\overline{h}(b(x))$ are equal and $\overline{h}(a(x)) = \overline{h}(b(x))$. That implies $\overline{h}$ satisfies the property of uniqueness. Now, $\overline{h}((a_0 + a_1x + \cdots + a_mx^m) + (b_0 + b_1x + \cdots + b_mx^m)) = \overline{h}((a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m) = h(a_0+b_0)+h(a_1+b_1)x+\cdots+h(a_m+b_m)x^m$. But, as h is a homomorphism, we have $h(a_0+b_0)+h(a_1+b_1)x+\cdots+h(a_m+b_m)x^m = h(a_0)+h(b_0)+h(a_1)x+h(b_1)x+\cdots+h(a_m)x^m+h(b_m)x^m = \overline{h}(a_0+a_1x+\cdots+a_mx^m)+\overline{h}(b_0 + b_1x + \cdots + b_mx^m)$. Also, $\overline{h}((a_0 + a_1x + \cdots + a_mx^m)(b_0 + b_1x + \cdots + b_mx^m)) = \overline{h}(c_0 + c_1x + \cdots + c_{2m}x^{2m}) = h(c_0) + h(c_1)x + \cdots + h(c_{2m})x^{2m}$, where $c_k = \sum_{i+j=k} a_ib_j$, for all $k \in \{0, \ldots, 2m\}$. As h is a homomorphism, then $h(c_k) = h\left(\sum_{i+j=k} a_ib_j\right) = \sum_{i+j=k} h(a_ib_j) = \sum_{i+j=k} h(a_i)h(b_j)$. But, these are coefficients of $\overline{h}(a(x))$ and $\overline{h}(b(x))$, so $\overline{h}(a(x)b(x)) = \overline{h}(c(x)) = \overline{h}(a(x))\overline{h}(b(x))$ and that implies that $\overline{h}$ is a homomorphism.

[83] We say that $\overline{h}$ is induced by h.

Ad 2. *Necessity.* Assume $\overline{h}$ is surjective and take $b \in B$. We must show that there exists $a \in A$ such that $h(a) = b$. As $b \in B$, then also $b \in B[x]$. As $\overline{h}$ is surjective, there exists $c(x) \in A[x]$ such that $\overline{h}(c(x)) = b$. The coefficients of $\overline{h}(c(x))$ are all $h(c_i)$ by definition, and as $\overline{h}(c(x))$ equals a zero-degree polynomial b, all it's coefficients, except the constant term, equal zero. So, it only remains that $h(c_0) = b$, proving that h is surjective. *Sufficiency.* Assume h is surjective and take $b(x) \in B[x]$. We must show that there exists $a(x) \in A[x]$ such that $\overline{h}(a(x)) = b(x)$. Let $b(x) = b_0 + b_1x + \cdots + b_mx^m$. Then, $b_i \in B$, for all $i \in \{0, \ldots, m\}$, and as h is surjective, there exist $a_i \in A$ such that $h(a_i) = b_i$. Therefore, $a(x) = a_0 + b_1x + \cdots + a_mx^m$ is the polynomial we sought and $\overline{h}$ is surjective.

Ad 3. *Necessity.* Assume $\overline{h}$ is injective and let $a, b \in A$ such that $a \neq b$. But, also $a, b \in A[x]$ and, as $a \neq b$, then $\overline{h}(a) \neq \overline{h}(b)$. But, $\overline{h}(a)$ is of degree zero, and so iz $\overline{h}(b)$. Therefore, it must be that the constant terms are different, i.e. $h(a) \neq h(b)$, meanining h is injective. *Sufficiency.* Assume h is injective and let $a(x), b(x) \in A[x]$. Then, assume $\overline{h}(a(x)) = \overline{h}(b(x))$. That implies that those two polynomials are of the same degree and that their coefficients are equal. But, their coefficients are $h(a_i)$ and $h(b_i)$, respectively, so it must be $h(a_i) = h(b_i)$. As h is injective, that implies $a_i = b_i$, i.e. $a(x) = b(x)$, so $\overline{h}$ is injective also.

□

Proposition. Let A and B be rings and let $\overline{h}$ be induced by homomorphism $h : A \underset{K}{\longrightarrow} B$. Let $a(x), b(x) \in A[x]$. If $a(x)$ is a factor of $b(x)$, then $\overline{h}(a(x))$ is a factor of $\overline{h}(b(x))$.

Proof. Let $a(x)$ be a factor of $b(x)$, i.e. there exists $q(x) \in A[x]$ such that $b(x) = q(x)a(x)$. Then, as $q(x)a(x) \in A[x]$ and $\overline{h}$ is well-defined, we have:

$$\overline{h}(b(x)) = \overline{h}(q(x)a(x)).$$

But, as $\overline{h}$ is a homomorphism, that is equivalent to $\overline{h}(b(x)) = \overline{h}(q(x))\overline{h}(a(x))$, i.e. $\overline{h}(a(x))$ is a factor of $\overline{h}(b(x))$.

□

Proposition. Let $m \in \mathbb{Z}^+$. If $h : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is the projective homomorphism, let $\overline{h} : \mathbb{Z}[x] \to \mathbb{Z}/m\mathbb{Z}[x]$ be the homomorphism induced by h. Then:

1. $\overline{h}(a(x)) = \overline{0}$ if and only if m divides every coefficient of $a(x)$.
2. If $m \in P$ and $a(x)b(x) \in \ker\left(\overline{h}\right)$, then $a(x) \in \ker\left(\overline{h}\right)$ or $b(x) \in \ker\left(\overline{h}\right)$.

Proof. *Ad* 1. Let $a(x) \in \mathbb{Z}[x]$ so that $a(x) = a_m x^m + \cdots + a_1 x + a_0$, for some $m \in \mathbb{Z}_0^+$ and $a_i \in \mathbb{Z}$, for all $i \in \{0, \ldots, m\}$. *Necessity.* Assume $\overline{h}(a(x)) = \overline{0}$. Then, $\overline{h}(a(x)) = h(a_m)x^m + \cdots + h(a_1)x + h(a_0)$. But, as h is a projective homomorphism, and as $\overline{h}(a(x)) = \overline{0}$, we have $\overline{h}(a(x)) = \overline{a_m}x^m + \cdots + \overline{a_1}x + \overline{a_0} = \overline{0}$. That implies, as all corresponding coefficients on both sides must be equal (along with degrees of $\overline{h}(a(x))$ and $\overline{0}$) that $\overline{a_i} = \overline{0}$, for all $i \in \{0, \ldots, m\}$. But, that means that $a_i \equiv 0 \pmod{m}$, i.e. $m|a_i$. *Sufficiency.* Let $m|a_i$ for all $i \in \{0, \ldots, m\}$. Then, $a_i \equiv 0 \pmod{m}$, i.e. $\overline{a_i} = \overline{0}$, for all $i \in \{0, \ldots, m\}$. As $\overline{h}(a(x)) = h(a_m)x^m + \cdots + h(a_1)x + h(a_0) = \overline{a_m}x^m + \cdots + \overline{a_1}x + \overline{a_0}$, that implies that $\overline{h}(a(x)) = \overline{0}$.

Ad 2. Let $m \in P$ and $a(x), b(x) \in \mathbb{Z}[x]$ such that $a(x)b(x) \in \ker\left(\overline{h}\right)$. As $m \in P$, then $\mathbb{Z}/m\mathbb{Z}$ is a field, by a previous proposition. Also, it is an integral domain, so $\mathbb{Z}/m\mathbb{Z}[x]$ is an integral domain. By a previous proposition, as h is surjective (projective homomorphism is always surjective) $\overline{h} : \mathbb{Z}[x] \to \mathbb{Z}/m\mathbb{Z}[x]$ is surjective. Then, by FHT, $\mathbb{Z}[x]/\ker\left(\overline{h}\right) \cong \mathbb{Z}/m\mathbb{Z}[x]$ and it follows that $\mathbb{Z}[x]/\ker\left(\overline{h}\right)$ is an integral domain (as it is isomorphic to integral domain $\mathbb{Z}/m\mathbb{Z}[x]$. By a previous proposition, $\ker\left(\overline{h}\right)$ is a prime ideal of $\mathbb{Z}[x]$, which implies that $a(x) \in \ker\left(\overline{h}\right)$ or $b(x) \in \ker\left(\overline{h}\right)$.

□

Remark. Notice that, as $A[x]$ is an integral domain (if A is integral domain), then we can construct a field of quotients denoted by $A(x, y)$. Then, $A(x, y)$ consists of all the fractions $\frac{a(x)}{b(x)}$, where $b(x) \neq 0$, and $a(x), b(x) \in A[x]$.

Proposition. Let A be an integral domain. Then, $\operatorname{char}(A(x)) = \operatorname{char}(A)$.

Proof. Let $\operatorname{char}(A) = p$. That implies $p \cdot 1 = 0$. But, also $1 \in A(x)$, so $p \cdot 1 = 0$. As $p \in P$, then $\operatorname{char}(A(x)) = p$.

□

Remark. Notice that previous proposition implies that for every $p \in P$, there is an infinite field of characteristic p.

Proposition. If A and B are integral domains and $h : A \to B$ is an isomorphism, then $\overline{h} : A(x) \to B(x)$ is an isomorphism defined as:

$$\tilde{h}\left(\frac{a_m x^m + \cdots + a_1 x + a_0}{b_n x^n + \cdots + b_1 x + b_0}\right) = \frac{h(a_m)x^m + \cdots + h(a_1)x + h(a_0)}{h(b_n)x^n + \cdots + h(b_1)x + h(b_0)} = \frac{\overline{h}(a(x))}{\overline{h}(b(x))}.$$

Proof. Assume h is an isomorphism and that $\tilde{h}$ is defined as above. Then, if we

take $\frac{a(x)}{b(x)} \in A(x)$, as h is well-defined, there exists $\frac{a'(x)}{b'(x)}$ in $B(x)$ (whose coefficients are $h(a_i)$ and $h(b_i)$) such that $\tilde{h}\left(\frac{a(x)}{b(x)}\right) = \frac{a'(x)}{b'(x)}$. If $\frac{a(x)}{b(x)} = \frac{a'(x)}{b'(x)}$, then, by definition, $a(x)b'(x) = a'(x)b(x)$. As $a(x)b'(x), a'(x)b(x) \in A[x]$, then, as $\overline{h}$ is well-defined, $\overline{h}(a(x)b'(x)) = \overline{h}(a'(x)b(x))$. As $\overline{h}$ is a homomorphism, then $\overline{h}(a(x))\overline{h}(b'(x)) = \overline{h}(a'(x))\overline{h}(b(x))$. That implies $\frac{\overline{h}(a(x))}{\overline{h}(b(x))} = \frac{\overline{h}(a'(x))}{\overline{h}(b'(x))}$, i.e. $\tilde{h}\left(\frac{a(x)}{b(x)}\right) = \tilde{h}\left(\frac{a'(x)}{b'(x)}\right)$, so $\tilde{h}$ is well-defined. Then, take $\frac{a'(x)}{b'(x)} \in B(x)$. It is easy to see, that, as $h(a_i)$ and $h(b_i)$ are coefficients in $a'(x)$ and $'b(x)$, that $\frac{\overline{h}(a(x))}{\overline{h}(b(x))} \in A(x)$, granting coefficients of $a(x)$ and $b(x)$ are $a_i, b_i \in A(x)$, then equals $\frac{a'(x)}{b'(x)}$. Also, if $\tilde{h}\left(\frac{a(x)}{b(x)}\right) = \tilde{h}\left(\frac{(a'(x)}{b(x)}\right)$, then $\frac{\overline{h}(a(x))}{\overline{h}(b(x))} = \frac{\overline{h}(a'(x))}{\overline{h}(b'(x))}$, i.e. $\overline{h}(a(x))\overline{h}(b'(x)) = \overline{h}(a'(x))\overline{h}(b(x))$. That means that the coefficients for $a(x)b'(x) = a'(x)b(x)$ satisfy $\sum_{i+j=k} h(a_i)h(b'_j) = \sum_{i+j=k} h(a'_i)h(b_j)$. As h is an isomorphism, we have $h\left(\sum_{i+j=k} a_i b'_j\right) = h\left(\sum_{i+j=k} a'_i b_j\right)$. As h is injective, that implies $\sum_{i+j=k} a_i b'_j = \sum_{i+j=k} a'_i b_j$, i.e. $a(x)b'(x) = a'(x)b(x)$. That implies $\frac{a(x)}{b(x)} = \frac{a'(x)}{b'(x)}$, so $\tilde{h}$ is also injective. Also,

$$\begin{aligned}
\tilde{h}\left(\frac{a(x)}{b(x)} + \frac{a'(x)}{b'(x)}\right) &= \tilde{h}\left(\frac{a(x)b'(x) + a'(x)b(x)}{b(x)b'(x)}\right) = \frac{\overline{h}(a(x)b'(x) + a'(x)b(x))}{\overline{h}(b(x)b'(x))} \\
&= \frac{\overline{h}(a(x))\overline{h}(b'(x)) + \overline{h}(a'(x))\overline{h}(b(x))}{\overline{h}(b(x))\overline{h}(b'(x))} \\
&= \frac{\overline{h}(a(x)}{\overline{h}(b(x))} + \frac{\overline{h}(a'(x))}{\overline{h}(b'(x))} = \tilde{h}\left(\frac{a(x)}{b(x)}\right) + \tilde{h}\left(\frac{a'(x)}{b'(x)}\right).
\end{aligned}$$

Finally,

$$\begin{aligned}
\tilde{h}\left(\frac{a(x)}{b(x)} \cdot \frac{a'(x)}{b'(x)}\right) &= \tilde{h}\left(\frac{a(x)a'(x)}{b(x)b'(x)}\right) = \frac{\overline{h}(a(x)a'(x))}{\overline{h}(b(x)b'(x))} \\
&= \frac{\overline{h}(a(x))\overline{h}(a'(x))}{\overline{h}(b(x))\overline{h}(b'(x))} = \frac{\overline{h}(a(x))}{\overline{h}(b(x))} \cdot \frac{\overline{h}(a'(x))}{\overline{h}(b'(x))} \\
&= \tilde{h}\left(\frac{a(x)}{b(x)}\right)\tilde{h}\left(\frac{a'(x)}{b'(x)}\right).
\end{aligned}$$

In conclusion, $\tilde{h}$ is an isomorphism from $A(x)$ to $B(x)$. In other words, if $A \cong B$, then $A(x) \cong B(x)$.

□

Definition. Let A be a ring. Then we define **multivariate polynomial** inductively. If polynomial ring $A[x_1]$ is denoted by A_1, then $A_1[x_2]$ is a polynomial in two variables

denoted by $A[x_1, x_2]$. If $A[x_1, \ldots, x_i]$, where $i \in \mathbb{Z}^+$, is denoted by A_i, then $A_{i+1}[x_{i+1}]$ is a polynomial ring in $i+1$ letters denoted by $A[x_1, \ldots, x_{i+1}]$. The degree of a multivariate polynomial is the highest sum of powers of individual factors appearing in one of its terms having a non-zero coefficient.

Problem. List all the polynomials of degree less than 3 in $\mathbb{Z}/3\mathbb{Z}[x, y]$.

Solution. We have zero polynomial 0. Then, for zero degree polynomials, there are 1 and 2. For degree one polynomials, we have x, $x+\overline{1}$, $x+\overline{2}$, $\overline{2}x$, $\overline{2}x+\overline{1}$, $\overline{2}x+\overline{2}$, y, $y+\overline{1}$, $y+\overline{2}$, $\overline{2}y$, $\overline{2}y+\overline{1}$, $\overline{2}y+\overline{2}$. For degree 2 polynomials, we have $\overline{a_{2,0}}x^2+\overline{a_{0,2}}y^2+\overline{a_{1,1}}xy+\overline{a_{1,0}}x+\overline{a_{0,1}}y+\overline{a_{0,0}}$, where at least one of $a_{2,0}$, $a_{0,2}$ and $a_{1,1}$ is not equal to zero. Then, for degree 3 we have $\overline{a_{3,0}}x^3+\overline{a_{0,3}}y^3+\overline{a_{2,1}}x^2y+\overline{a_{1,2}}xy^2+\overline{a_{2,0}}x^2+\overline{a_{0,2}}y^2+\overline{a_{1,1}}xy+\overline{a_{1,0}}x+\overline{a_{0,1}}y+\overline{a_{0,0}}$, where at least one of $a_{3,0}$, $a_{0,3}$, $a_{2,1}$ and $a_{1,2}$ is not equal to zero. Of course, all $a_{i,j} \in \mathbb{Z}$, so $\overline{a_{i,j}} \in \mathbb{Z}/3\mathbb{Z}$.

Proposition. If A is an integral domain, then $A[x_1, \ldots, x_m]$ is an integral domain, for all $m \in \mathbb{Z}^+$.

Proof. Proof by induction. We have already proved the case for $m = 1$ in a previous proposition. Then, assume that if A is an integral domain, then $A[x_1, \ldots, x_m]$ is an integral domain. We will prove that it is true for $m+1$. We know that $A[x_1, \ldots, x_{m+1}]$ actually equals $(A[x_1, \ldots, x_m])[x_{m+1}]$ by definition. But, as A is an integral domain, then, so is $A[x_1, \ldots, x_m]$, by assumption. Then, as $A[x_1, \ldots, x_m]$ is an integral domain, also $(A[x_1, \ldots, x_m])[x_{m+1}]$ is an integral domain.

□

Remark. We will denote an arbitrary polynomial $a(x, y) \in A[x, y]$ by $\sum_{i,j \in \mathbb{Z}_0^+} a_{ij}x^iy^j$. Then, if $a(x, y), b(x, y) \in A[x, y]$ such that $a(x, y) = \sum_{i,j \in \mathbb{Z}_0^+} a_{ij}x^iy^j$ and $b(x, y) = \sum_{i,j \in \mathbb{Z}_0^+} b_{ij}x^iy^j$. We define addition as $a(x, y) + b(x, y) = \sum_{i,j \in \mathbb{Z}_0^+} (a_{ij} + b_{ij})x^iy^j$. Let us observe the two polynomials:

$$\begin{aligned} a(x, y) &= a_{0,0} + a_{1,0}x + a_{0,1}y + a_{1,1}xy + a_{2,0}x^2 + a_{0,2}y^2 + a_{2,1}x^2y, \\ b(x, y) &= b_{0,0} + b_{1,0}x + b_{0,1}y + b_{1,1}xy + b_{2,0}x^2 + b_{2,1}x^2y + b_{2,2}x^2y^2. \end{aligned}$$

Then, their product is:

$$\begin{aligned} a(x,y)b(x,y) &= (a_{0,0}b_{0,0}) + (b_{0,0}a_{1,0} + b_{1,0}a_{0,0})\,x + (b_{0,0}a_{0,1} + b_{0,1}a_{0,0})\,y \\ &+ (b_{0,0}a_{1,1} + a_{0,0}b_{1,1} + a_{0,1}b_{1,0} + b_{0,1}a_{1,0})\,xy \\ &+ (a_{2,0}b_{0,0} + a_{0,0}b_{2,0} + a_{1,0}b_{1,0})\,x^2 + (a_{0,2}b_{0,0} + a_{0,1}b_{0,1})\,y^2 \\ &+ (a_{2,1}b_{0,0} + b_{2,1}a_{0,0} + a_{1,1}b_{1,0} + b_{1,1} + a_{1,0} + b_{2,0}a_{0,1} + a_{2,0}b_{0,1})\,x^2y \\ &+ (a_{0,0}b_{2,2} + a_{2,1}b_{0,1} + b_{2,1}a_{0,1} + b_{2,0}a_{0,2} + a_{1,1}b_{1,1})\,x^2y^2. \end{aligned}$$

Then, the sum of indices of a and b, observed as vectors, corresponds to the exponents of x and y, observed as vectors, respectively. Therefore, we can write the formula for the product of two polynomials in two letters as:

$$a(x,y)b(x,y) = \sum_{\substack{i+k=u \\ j+l=v}} a_{ij}b_{kl}x^u y^v$$

Proposition. If A is an integral domain, then $\deg a(x,y)b(x,y) = \deg a(x,y) + \deg b(x,y)$.

Proof. Assume A is an integral domain. Then, let $\deg a(x,y) = m$ and $\deg b(x,y) = n$. That means that the largest sum of exponents (in some term) is m in $a(x,y)$ and n in $b(x,y)$. So, there exist terms $a_{i,j}x^iy^j$, where $a_{i,j} \in A$, and $b_{k,l}x^ky^l$, where $b_{k,l} \in A$, such that $a_{i,j}, b_{k,l} \neq 0$ and $i + j = m$ and $k + l = n$. Then, the largest sum of exponents in $a(x,y)b(x,y)$ is $m + n$ appearing in $a_{i,j}b_{k,l}x^{i+k}y^{j+l}$. As A is an integral domain and $a_{i,j}, b_{k,l} \neq 0$, then also $a_{i,j}b_{k,l} \neq 0$, so the degree of $a(x,y)b(x,y)$ is $m + n$.

□

Factoring polynomials

Theorem. Let F be a field. Then, every ideal of $F[x]$ is principal.

Proof. Let $J \trianglelefteq F[x]$. We know that at least $0 \in J$. Assume $J = \{0\}$. Then, $J = \langle 0 \rangle$, so J is principal. Assume $|J| > 1$, i.e. there exists $a(x) \in J$ such that $a(x) \neq 0$. Let $D = \{\deg b(x) : \ b(x) \in J - \{0\}\}$. Notice that we put $\deg 0 \notin D$, as 0 has an undefined degree. Well, at least $a(x) \in J$, then we have $\deg a(x) \in D$. So, $D \neq \emptyset$ and as $D \subseteq \mathbb{Z}_0^+$, by well-ordering principle, there exists $\deg a(x) \in D$ such that $\deg a(x) \leq \deg b(x)$, for all $b(x) \in J$. Let $b(x) \in J$. Then, by division with remainder for polynomials, there exist $q(x), r(x) \in J$ (we know that they are in J because J is itself a field and both $a(x), b(x) \in J$) such that $0 \leq \deg r(x) < \deg a(x)$ and $b(x) = a(x)q(x) + r(x)$. But, $\deg r(x) < \deg a(x)$ is in contradiction with $\deg a(x) \leq \deg c(x)$, for all $c(x) \in J$. Therefore, it can only be that $r(x) = 0$, i.e. its degree is undefined (and it can be as $0 \in J$). Therefore, $b(x) = a(x)q(x)$ implies that every $b(x) \in J$ can be written as a polynomial multiple of $a(x)$, i.e. $J = \langle a(x) \rangle$.

□

Definition. Let F be a field and let $a(x), b(x) \in F[x]$ such that $a(x), b(x) \neq 0$. We say that $a(x)$ and $b(x)$ are **associates** if $a(x)|b(x)$ and $b(x)|a(x)$.

Proposition. Let F be a field and $a(x), b(x) \in F[x] - \{0\}$. Then, $a(x)$ and $b(x)$ are associates if and only if there exist $c, d \in F - \{0\}$, such that $a(x) = cb(x)$ and $b(x) = da(x)$.

Proof. *Necessity.* Let $a(x)$ and $b(x)$ be associates. That implies there exist $p(x), q(x) \in A[x]$ such that $a(x) = b(x)p(x)$ and $b(x) = a(x)q(x)$. That means that $a(x) = b(x)p(x) = (a(x)q(x))p(x)$, i.e. $a(x) \cdot 1 = a(x)(q(x)p(x))$. As $a(x) \neq 0$ and $A[x]$ is an integral domain, that implies $1 = q(x)p(x)$. But, that is possible only if $\deg p(x) = \deg q(x) = 0$, so $p(x) = c$ and $q(x) = d$, where $c, d \in F$ and $c, d \neq 0$. That means $a(x) = cb(x)$ and $b(x) = da(x)$.

Sufficiency. Let there exist $c, d \in F - \{0\}$ such that $a(x) = cb(x)$ and $b(x) = da(x)$. That means that, as $c, d \in F[x]$ also, that $b(x)|a(x)$ and $a(x)|b(x)$, i.e. $a(x)$ and $b(x)$ are associates.

□

Definition. Let F be a field. Then, $a(x) \in F[x] - \{0\}$ is called **monic** if its leading coefficient is equal to 1, i.e. it is of the form $a(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, where $m \in \mathbb{Z}_0^+$ and $a_{m-1}, \ldots, a_1, a_0 \in F[x]$. Monic polynomial $a(x) \in F[x] - \{0\}$ is

called a **monic associate** of a polynomial $b(x) \in F[x] - \{0\}$ if there exists $c \in F - \{0\}$ such that $b(x) = ca(x)$.

Proposition. Let F be a field. Then, every $a(x) \in F[x] - \{0\}$ has a unique monic associate.

Proof. *Existence.* Let $a(x) \in F[x] - \{0\}$ such that $a(x) = a_m x^m + \cdots + a_1 x + a_0$. Then, as F is a field, there exists a_m^{-1} such that $a_m a_m^{-1} = a_m^{-1} a_m = 1$. Therefore, $a_m^{-1} a(x) = a_m^{-1} a_m x^m + \cdots + a_m^{-1} a_1 x + a_m^{-1} a_0 = x^m + \cdots + (a_m^{-1} a_1)x + (a_m^{-1} a_0)$ is a monic associate of $a(x)$. *Uniqueness.* Let $a(x) \in F[x] - \{0\}$ and assume $b(x), c(x) \in F[x] - \{0\}$ are both monic associates of $a(x)$. That means that there exist $b', c' \in F - \{0\}$ such that $a(x) = b'b(x)$ and $a(x) = c'c(x)$ and that $b(x)$ and $c(x)$ are monic. We have $a(x) = b'b(x) = c'c(x)$. But, from $b'b(x) = c'c(x)$, we may conclude that they have equal degrees and that all their coefficients are equal. Therefore, if b_m and c_m are the leading coefficients of $b(x)$ and $c(x)$, respectively, we have $b'b_m = c'c_m$. But, as they are monic, that means that $b_m = c_m = 1$, so we have $b'1 = c'1$, i.e. $b' = c'$. Therefore, all other coefficients of $b'b(x)$ and $c'c(x)$ are $b'b_i$ and $c'c_i$ and we have $b'b_i = c'c_i$. As $b' = c'$, we have $b'b_i = b'c_i$. Multiplying that by $[b']^{-1}$ (which we can as F is a field), we have $[b']^{-1}b'b_i = [b']^{-1}b'c_i$, i.e. $1b_i = 1c_i$, which means $b_i = c_i$. Thus, $b(x) = c(x)$.

□

Definition. Let F be a field and let $a(x), b(x) \in F[x]$. We say that $d(x) \in F[x]$ is a **greatest common divisor** of $a(x)$ and $b(x)$ if:

1. $d(x)|a(x)$ and $d(x)|b(x)$;
2. $d(x)$ is monic;
3. $c(x)|a(x)$ and $c(x)|b(x)$ implies $c(x)|d(x)$, for all $c(x) \in F[x]$.

We then write $\gcd(a(x), b(x)) = d(x)$.

Proposition. Let F be a field and $a(x), b(x) \in F[x]$. Then there exists a unique $\gcd(a(x), b(x)) \in F[x]$ such that $\gcd(a(x), b(x)) = a(x)p(x) + b(x)q(x)$, for some $p(x), q(x) \in F[x]$.

Proof. *Existence.* Let $J = \{a(x)p(x) + b(x)q(x) : \ p(x), q(x) \in F[x]\}$. Obviously $J \subseteq F[x]$, by its definition. Take $a(x)p_1(x) + b(x)q_1(x), a(x)p_2(x) + b(x)q_2(x) \in J$. It's easy to see that $a(x)p_1(x) + b(x)q_1(x) + a(x)p_2(x) + b(x)q_2(x) = a(x)[p_1(x) + p_2(x)] + b(x)[q_1(x) + q_2(x)] \in J$. Also, $[a(x)p_1(x) + b(x)q_1(x)][a(x)p_2(x) + b(x)q_2(x)] = a(x)p_1(x)a(x)p_2(x) + a(x)p_1(x)b(x)q_2(x) + b(x)q_1(x)a(x)p_2(x) + b(x)q_1(x)b(x)q_2(x) =$

$a(x)[a(x)p_1(x)p_2(x) + p_1(x)b(x)q_2(x)] + b(x)[q_1(x)a(x)p_2(x) + q_1(x)b(x)q_2(x)] \in F[x]$. Finally, if $c(x) \in F[x]$, then $[a(x)p(x) + b(x)q(x)]c(x) = c(x)[a(x)p(x) + b(x)q(x)] = c(x)a(x)p(x) + c(x)b(x)q(x) = a(x)[c(x)p(x)] + b(x)[c(x)q(x)] \in F[x]$. That implies that $J \trianglelefteq F[x]$ and by previous proposition J is a principal ideal generated by some $d'(x) \in F[x]$. If $d'(x)$ is not monic, then we can take $d(x) \in F[x]$ as $d(x) = d_L^{-1}d'(x)$, where $d_L \in F$ is the leading coefficient of $d'(x)$. Then, J is also generated by $d(x)$, because $a(x) \in J$ implies $a(x) = d'(x)r(x)$, for some $r(x) \in J$, but also $a(x) = d_L^{-1}d(x)r(x)$, i.e. $a(x) = d(x)[d_L^{-1}r(x)]$. Now, as we have $d(x) \in J$, then $d(x) = a(x)p(x) + b(x)q(x)$, for some $p(x), q(x) \in F[x]$. Also, as $a(x)1 + b(x)0 \in J$, i.e. $a(x) \in J$, then $a(x) = d(x)r_a(x)$, for some $r_a(x) \in F[x]$ and we have $d(x)|a(x)$. Similarly, $a(x)0 + b(x)1 \in J$, that is $b(x) \in J$, so $b(x) = d(x)r_b(x)$ for some $r_b(x) \in F[x]$ and that means $d(x)|b(x)$. Now, let $c(x)|a(x)$ and $c(x)|b(x)$. Then there exist $p_1(x), q_1(x) \in F[x]$ such that $a(x) = c(x)p_1(x)$ and $b(x) = c(x)q_1(x)$. That means that $a(x)p(x) + b(x)q(x) = d(x)$ is equivalent to $c(x)p_1(x)p(x) + c(x)q_1(x)q(x) = d(x)$, i.e. $c(x)[p_1(x)p(x) + q_1(x)q(x)] = d(x)$. That implies that $c(x)|d(x)$. Therefore, by definition, $d(x) = \gcd(a(x), b(x))$. *Uniqueness.* Assume $c(x) = \gcd(a(x), b(x))$ and $d(x) = \gcd(a(x), b(x))$. Then, $c(x)|a(x)$ and $c(x)|b(x)$. But, as $d(x)|a(x)$ and $d(x)|b(x)$ also, then $d(x)|c(x)$. But, at the same time, $c(x)|a(x)$ and $c(x)|b(x)$ implies $c(x)|d(x)$. Therefore, $c(x) = d(x)$.

□

Definition. Let F be a field and $p(x) \in F[x]$ a non-constant polynomial. If there do not exist $q(x), r(x) \in F[x]$ such that $\deg q(x) \neq 0$ and $\deg r(x) \neq 0$ and $p(x) = q(x)r(x)$, we say that $p(x)$ is **irreducible** over F.

Lemma. Let F be a field and $p(x) \in F[x]$. Then, the only divisors of $p(x)$ are c and $dp(x)$, where $c, d \in F$.

Proof. It is obvious that $c|p(x)$ as $p(x) = (c)(c^{-1}p(x))$. Also, $dp(x)|p(x)$ because $p(x) = (dp(x))(d^{-1})$. Both polynomials satisfy the conditions for irreducibility because $\deg c = 0$ and $\deg d = 0$. If we assumed that some other $a(x) \in F[x]$, $0 < \deg a(x) < \deg p(x)$, divides $p(x)$, there would have to exist $q(x) \in F[x]$ such that $p(x) = a(x)q(x)$. But, as $F[x]$ is an integral domain, we have $\deg p(x) = \deg a(x) + \deg q(x)$, i.e. $\deg p(x) - \deg a(x) = \deg q(x)$. As $\deg a(x) > 0$, we have $\deg q(x) = \deg p(x) - \deg a(x) < \deg p(x)$ and $0 < \deg p(x) - \deg a(x) = \deg q(x)$ because $\deg a(x) < \deg p(x)$. Then it is impossible as $q(x)$ cannot be equal to a constant polynomial, i.e. both $a(x)$ and $q(x)$ would be non-constant polynomials.

□

Theorem (Euclid's lemma for polynomials). Let F be a field and $p(x) \in F[x]$ a polynomial irreducible over F. If $p(x)|a(x)b(x)$, where $a(x), b(x) \in F[x]$, then $p(x)|a(x)$ or $p(x)|b(x)$.

Proof. If $p(x)|a(x)$, we are done. Now, assume that $p(x) \nmid a(x)$. By previous lemma, the only divisors of $p(x)$ are c and $dp(x)$, where $c, d \in F$. Therefore, as for greatest common divisor we only consider monic polynomials, we have $\gcd(a(x), p(x)) \in \{1, p(x)\}$. If it were that $\gcd(a(x), p(x)) = p(x)$, we would have that $p(x)|a(x)$. The only possibility is that $\gcd(a(x), p(x)) = 1$. That means that there exist $c(x), d(x) \in F[x]$ such that $a(x)c(x) + p(x)d(x) = 1$. As $p(x)|a(x)b(x)$, there exists $q(x) \in F[x]$ such that $a(x)b(x) = p(x)q(x)$. From $a(x)c(x) + p(x)d(x) = 1$ we get $a(x)c(x) = 1 - p(x)d(x)$. So, we multiply $a(x)b(x) = p(x)q(x)$ with $c(x)$ to get $a(x)c(x)b(x) = p(x)q(x)c(x)$. Then, we substitute expression for $a(x)c(x)$ and get $[1 - p(x)d(x)]b(x) = p(x)q(x)c(x)$. That gives us $b(x) - p(x)d(x)b(x) = p(x)q(x)c(x)$, i.e. $b(x) = p(x)q(x)c(x) + p(x)d(x)b(x)$. Extracting a common factor gives us $b(x) = p(x)[q(x)c(x) + d(x)b(x)]$. That implies that $p(x)|b(x)$.

□

Corollary. Let F be a field and $p(x) \in F[x]$ a polynomial irreducible over F. Let $a_1(x), \ldots, a_m(x) \in F[x]$, where $m \in \mathbb{Z}^+$, such that $p(x)|a_1(x) \cdots a_m(x)$, then $p(x)|a_i(x)$, for some $i \in \{1, \ldots, m\}$.

Proof. Proof by induction. Assume $m = 1$. Then, $p(x)|a_1(x)$ implies $p(x)|a_1(x)$. Assume that $p(x)|a_1(x) \cdots a_m(x)$, for some $m \in \mathbb{Z}^+$, implies $p(x)|a_i(x)$, for some $i \in \{1, \ldots, m\}$. If $p(x)|a_1(x) \cdots a_{m+1}(x)$, then $p(x)|\,(a_1(x) \cdots a_m(x))\,(a_{m+1}(x))$. By previous theorem, $p(x)|a_1(x) \cdots a_m(x)$ or $p(x)|a_{m+1}(x)$. If it is the first case, by assumption of induction, we have that $p(x)|a_i(x)$, for some $i \in \{1, \ldots, m\}$. If it is the second case, we already have $p(x)|a_{m+1}(x)$. In conclusion, $p(x)|a_i(x)$, where $i \in \{1, \ldots, m\} \cup \{m+1\} = \{1, \ldots, m+1\}$, proving the corollary is true for all $m \in \mathbb{Z}^+$.

□

Corollary. Let F be a field and $p(x) \in F[x]$ a polynomial irreducible over F. Let $q_1(x), \ldots, q_m(x)$, for some $m \in \mathbb{Z}^+$, be monic irreducible polynomials. If it is the case that $p(x)|q_1(x) \cdots q_m(x)$, then $p(x) = q_i(x)$, for some $i \in \{1, \ldots, m\}$.

Proof. By previous corollary we have that $p(x)|q_i(x)$, for some $i \in \{1, \ldots, m\}$. As $q_i(x)$ is irreducible, it's only divisors are c and $dq_i(x)$, where $c \in F[x]$. But, as $q_i(x)$ is monic, it means that $c = d = 1$. So, as $p(x)$ is a divisor of $q_i(x)$ it has to be

$p(x) \in \{1, q_i(x)\}$. If it were that $p(x) = 1$, by definition, it would not be irreducible[84]. Therefore, it must be that $p(x) = q_i(x)$.

□

Lemma. Let F be a field and $p(x) \in F[x]$ a polynomial such that $\deg p(x) = 1$. Then, $p(x)$ is irreducible over F.

Proof. Assume $p(x)$ is not irreducible over F, i.e. there exist polynomials $a(x), b(x) \in F[x]$ such that $\deg a(x) \neq 0$, $\deg b(x) \neq 0$ and $p(x) = a(x)b(x)$. That implies $\deg p(x) = \deg a(x) + \deg b(x)$, i.e. $1 = \deg a(x) + \deg b(x)$. But then, if $\deg a(x) = 1$ it must be that $\deg b(x) = 0$, which cannot be. Similarly, if $\deg b(x) = 1$, it must be $\deg a(x) = 0$, again a contradiction. Therefore there do not exist such polynomials and it must be that $p(x)$ is irreducible over F.

□

Theorem (Unique factorization of polynomials). Every polynomial $a(x)$ of positive degree in $F[x]$ can be uniquely written as a product $a(x) = kp_1(x) \cdots p_m(x)$, where $k \in F$ and $p_1(x), \ldots, p_m(x) \in F[x]$ are monic irreducible polynomials.

Proof. *Factorization.* Let $m = \deg a(x)$. If $m = 1$, by previous lemma we have $a(x) = a(x)$. If $a(x) = a_1 x + a_0$ it can be made monic by $a(x) = a_1 \left(x + a_0 a_1^{-1}\right)$. Assume that for all $n \in \mathbb{Z}^+$, $n < m$ the polynomial $a(x)$ can be written as $a(x) = kp_1(x) \cdots p_n(x)$, where $p_i(x)$ are monic irreducible polynomials. Now, we will prove that the statement is true for m. If $a(x)$ of degree m is irreducible, we are done because $a(x) = a_m \left(a_m^{-1} a(x)\right)$ (where a_m is the leading coefficient of $a(x)$). Assume $a(x)$ is not irreducible. Then, by definition, it can be written as a product $a(x) = p(x)q(x)$, where $p(x), q(x) \in F[x]$ such that $\deg p(x) \neq 0$ and $\deg q(x) \neq 0$. That means that $\deg p(x), \deg q(x) < \deg a(x) = m$, so by assumption of induction, $p(x)$ and $q(x)$ can be written as a products of irreducible monic polynomials, i.e. $p(x) = kp_1(x) \cdots p_{m_1}(x)$ and $q(x) = lq_1(x) \cdots q_{m_2}(x)$, where $m_1, m_2 \in \mathbb{Z}^+$. Therefore, $a(x) = (kl)p_1(x) \cdots p_{m_1}(x)q_1(x) \cdots q_{m_2}(x)$, meaning it can be written as a product of irreducible monic polynomials with a constant factor.

Uniqueness. Assume that $a(x) = kp_1(x) \cdots p_{m_1}(x)$ and $a(x) = lq_1(x) \cdots q_{m_2}(x)$ with $m_1 \leq m_2$. That implies $kp_1(x) \cdots p_{m_1}(x) = lq_1(x) \cdots q_{m_2}(x)$. By multiplying that expression with $l^{-1} \in F$, we have $(kl^{-1})p_1(x) \cdots p_{m_1}(x) = q_1(x) \cdots q_{m_2}(x)$. As all q_i are not constant polynomials, then it must be that $kl^{-1} = 1$, i.e. $k = l$. By Euclid's lemma (and its corollaries), from $p_i | q_1(x) \cdots q_{m_2}(x)$ it follows that, as q_j are monic and irreducible, that $p_i = q_j$ for some j. In that fashion we get $p_i = q_{f(i)}$, where f :

[84]The definition demands that it is a non-constant polynomial - in a similar fashion definition of a prime number demands that a prime number is not equal to 1.

$\{1,\ldots,m_1\} \to \{1,\ldots,m_2\}$ is a function. Now, let $S = \{1,\ldots,m_2\} - f(\{1,\ldots,m_1\})$. That implies that $\prod_{i\in S} q_i(x) = 1$, meaning all other $q_i(x)$ can be disregarded as they are equal to 1. Therefore factorization of $a(x)$ is unique.

□

Definition. Let A be an integral domain and $a \in A$. If there exist $p_1,\ldots,p_m \in A$ such that $a = p_1\cdots p_m$ and if $p_1\cdots p_m = q_1\cdots q_n$, for some $q_1\cdots q_n \in A$, implies that $m = n$ and that there exists a bijection $f : \{1,\ldots,m\} \to \{1,\ldots,m\}$ such that $p_i = q_{f(i)}$, for all $i \in \{1,\ldots,m\}$, then we say that A is a **unique factorization domain** (or **UFD** for short).

Problem. Factor $x^4 - 4$ into irreducible factors over $\mathbb{Q}$, over $\mathbb{R}$ and over $\mathbb{C}$.

Solution. We have $x^4 - 4 = (x^2-2)(x^2+2)$ and $x^2 \pm 2$ is irreducible over $\mathbb{Q}$, but $x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2})$, which cannot be further reduced in $\mathbb{R}$, so $x^4 - 4 = (x-\sqrt{2})(x+\sqrt{2})(x^2+2)$. Finally, over $\mathbb{C}$, we have $x^2+2 = (x-i\sqrt{2})(x+i\sqrt{2})$, so $x^4-4 = (x-\sqrt{2})(x+\sqrt{2})(x-i\sqrt{2})(x+i\sqrt{2})$.

Problem. Factor $x^2 - 16$ into irreducible factors over $\mathbb{Q}$, over $\mathbb{R}$ and over $\mathbb{C}$.

Solution. Trivially, $x^2 - 16 = (x-4)(x+4)$ over $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Problem. Find all the irreducible polynomials of degree ≤ 4 in $\mathbb{Z}/2\mathbb{Z}[x]$.

Solution. Let $a(x) = \overline{a_4}x^4 + \overline{a_3}x^3 + \overline{a_2}x^2 + \overline{a_1}x + \overline{a_0}$. We know that, if $\overline{a_0} = \overline{0}$, then $a(x)$ is reducible in $\mathbb{Z}/2\mathbb{Z}[x]$ because then we would have $a(x) = \overline{a_4}x^4 + \overline{a_3}x^3 + \overline{a_2}x^2 + \overline{a_1}x = x\left(\overline{a_4}x^3 + \overline{a_3}x^2 + \overline{a_2}x + \overline{a_1}\right)$. Therefore, we can restrict ourselves to polynomials with $\overline{a_0} = \overline{1}$. For first degree polynomials, all are irreducible, so we have x (an exception to our observation) and $x + \overline{1}$. For degree 2, we observe $x^2 + x + \overline{1}$ and $x^2 + \overline{1}$. As those are second degree polynomials, their factorization must be that of two first degree polynomials (x and $x+\overline{1}$). Of all the trivial cases, we can only observe $(x+\overline{1})(x+\overline{1}) = x^2 + \overline{1}x + \overline{1}x + \overline{1} = x^2 + 2\cdot\overline{1}x + \overline{1} = x^2 + \overline{1}$. So, $x^2 + \overline{1}$ is reducible and we are only left with $x^2 + x + \overline{1}$ as the only irreducible polynomial of second degree in $\mathbb{Z}/2\mathbb{Z}[x]$. For third degree polynomials, we have $x^3 + x^2 + x + \overline{1}$, $x^3 + x^2 + \overline{1}$, $x^3 + x + \overline{1}$ and $x^3 + \overline{1}$. If a third degree polynomial can be factored, then it has to contain a polynomial of a first degree (because $3 = 2+1 = 1+1+1$). Therefore, we can observe only $\overline{a_3}x^3 + \overline{a_2}x^2 + \overline{a_1}x + \overline{1} = \left(\overline{b_1}x + \overline{b_0}\right)\left(\overline{c_2}x^2 + \overline{c_1}x + \overline{c_0}\right)$. It definitely must be that $\overline{b_0c_0} = \overline{1}$ which further implies $\overline{b_0} = \overline{c_0} = \overline{1}$. Then, it is also obvious that it must be $\overline{b_1} = \overline{c_2} = \overline{1}$. So, we have only two cases for $\overline{c_1} \in \{\overline{0},\overline{1}\}$. If $\overline{c_1} = \overline{0}$, then we have $(x+\overline{1})(x^2+\overline{1}) = x^3+\overline{1}x+\overline{1}x^2+\overline{1} = x^2+x^2+x+\overline{1}$. If $\overline{c_1} = \overline{1}$, then $(x+\overline{1})(x^2+x+\overline{1}) =$

$x^3+x^2+\overline{1}x+\overline{1}x^2+\overline{1}x+\overline{1}=x^3+\overline{1}$. Therefore, the only irreducible polynomials of degree 3 are $x^3+x^2+\overline{1}$ and $x^3+x+\overline{1}$. Finally, for degree 4, we have $x^4+x^3+x^2+x+\overline{1}$, $x^4+x^3+x+\overline{1}$, $x^4+x^2+x+\overline{1}$, $x^4+x^3+x^2+\overline{1}$, $x^4+x^3+\overline{1}$, $x^4+x^2+\overline{1}$, $x^4+x+\overline{1}$ and $x^4+\overline{1}$. In this way, we will observe if we can factor $a(x)$ as $(x+\overline{1})(x^3+\overline{c_2}x^2+\overline{c_1}x+\overline{1})$ or $(x^2+\overline{b_1}x+\overline{1})(x^2+\overline{c_1}x+\overline{1})$. It is obvious that leading and constant terms have to be $\overline{1}$. In the first case, if $\overline{c_2}=\overline{c_1}=\overline{0}$, we have $(x+\overline{1})(x^3+\overline{1})=x^4+x^3+x+\overline{1}$. If $\overline{c_2}=\overline{c_1}=\overline{1}$, we have $(x+\overline{1})(x^3+x^2+x+\overline{1})=x^4+x^3+x^2+x+x^3+x^2+x+\overline{1}=x^4+\overline{1}$. If $\overline{c_2}=\overline{0}$ and $\overline{c_1}=\overline{1}$, we have $(x+\overline{1})(x^3+x+\overline{1})=x^4+x^2+x+x^3+x+\overline{1}=x^4+x^3+x^2+\overline{1}$. If $\overline{c_2}=\overline{1}$ and $\overline{c_1}=\overline{0}$, then $(x+\overline{1})(x^3+x^2+\overline{1})=x^4+x^3+x+x^3+x^2+\overline{1}=x^4+x^2+x+\overline{1}$. Finally, in the second case, we observe $(x^2+\overline{b_1}x+\overline{1})(x^2+\overline{c_1}x+\overline{1})$. Let $\overline{b_1}=\overline{c_1}=\overline{0}$. Then, $(x^2+1)^2=x^4+2x^2+\overline{1}^2=x^4+\overline{1}$. Let $\overline{b_1}=\overline{c_1}=\overline{1}$. Then, $(x^2+x+\overline{1})^2=(x^2+x)^2+2(x^2+x)+\overline{1}^2=x^4+2x^3+x^2+\overline{1}=x^4+x^2+\overline{1}$. If $\overline{b_1}=\overline{0}$ and $\overline{c_1}=\overline{1}$, we have $(x^2+\overline{1})(x^2+x+\overline{1})=x^4+x^3+x^2+x^2+x+\overline{1}=x^4+x^3+x+\overline{1}$. So, the only irreducible polynomials of degree 4 in $\mathbb{Z}/2\mathbb{Z}[x]$ are $x^4+x^3+x^2+x+\overline{1}$, $x^4+x^3+\overline{1}$ and $x^4+x+\overline{1}$. Notice that we could have made things much simplier by using the theorems from the next chapter. But, here we illustrated some methods for checking irreducibility. Also, notice the fine example that $x^4+x^2+\overline{1}=(x^2+x+\overline{1})^2$, while $\overline{1}^4+\overline{1}^2+\overline{1}=\overline{1}$, so by the theorem in the next chapter, and as $x-\overline{1}=x+\overline{1}$, we have that $x+\overline{1}\nmid x^4+x^2+\overline{1}$, but it is reducible.

Problem. Show that $x^2+\overline{2}$ is irreducible in $\mathbb{Z}/5\mathbb{Z}[x]$. Then factor $x^4-\overline{4}$ into irreducible factors in $\mathbb{Z}/5\mathbb{Z}[x]$.

Solution. The only possibility, as $x^2+\overline{2}$ is of degree 1 is that $x^2+\overline{2}=\overline{k}(x+\overline{a})(x+\overline{b})=\overline{k}(x^2+\overline{b}x+\overline{a}x+\overline{ab})$. It follows that $\overline{k}=\overline{1}$, so we are left with $x^2+\overline{2}=x^2+\overline{a+b}x+\overline{ab}$. From that we have $\overline{2}=\overline{ab}$, i.e. $\overline{2}=\overline{a}\overline{b}$. We also have $\overline{a+b}=\overline{0}$, i.e. $\overline{a}+\overline{b}=\overline{0}$. That implies $\overline{a}=-\overline{b}$. So, from $\overline{2}=\overline{a}\overline{b}$, we have $\overline{2}=-\overline{a}^2$. That is equivalent to $\overline{a}^2=-\overline{2}$, that is $\overline{a}^2=\overline{3}$. From $\overline{1}^2=\overline{4}^2=\overline{1}$ and $\overline{3}^2=\overline{2}^2=\overline{4}$, we conclude that there does not exist such $\overline{a}$ that $\overline{a}^2=\overline{3}$ and our assumption that $x^2+\overline{2}$ is reducible does not hold.

In $\mathbb{Z}/5\mathbb{Z}[x]$, we have $x^4-\overline{4}=(x^2-\overline{2})(x^2+\overline{2})=(x^2+\overline{3})(x^2+\overline{2})$. Both $x^2+\overline{3}$ and $x^2+\overline{2}$ are irreducible.

Problem. Factor $\overline{2}x^3+\overline{4}x+\overline{1}$ in $\mathbb{Z}/5\mathbb{Z}[x]$.

Solution. As the polynomial in the problem is of degree three, then, if it can be factored, it has to have at least one polynomial of degree one as a factor. Therefore, $\overline{2}x^3+\overline{4}x+\overline{1}=\overline{k}(x+\overline{a_0})(x^2+\overline{b_1}x+\overline{b_0})=\overline{k}x^3+\overline{k(a_0+b_1)}x^2+\overline{k(b_0+a_0b_1)}x+\overline{ka_0b_0}$. From that we have $\overline{k}=\overline{2}$ and then:

$$\begin{aligned}\overline{2a_0+2b_1} &= \overline{0},\\ \overline{2b_0+2a_0b_1} &= \overline{4},\\ \overline{2a_0b_0} &= \overline{1}.\end{aligned}$$

After multiplying all equalities by $\overline{2}^{-1}=\overline{3}$ we get:

$$\begin{aligned}\overline{a_0+b_1} &= \overline{0},\\ \overline{b_0+a_0b_1} &= \overline{2},\\ \overline{a_0b_0} &= \overline{3}.\end{aligned}$$

From first equality we have $\overline{b_1}=-\overline{a_0}$. From the last equality, we get $\overline{b_0}=\overline{3a_0^{-1}}$. Substituting those two expressions into second equality, we get $\overline{3a_0^{-1}-a_0^2}=\overline{2}$. Multiplying by $\overline{a_0}$, we get $\overline{3}=\overline{a_0}^3+\overline{2}\overline{a_0}$, i.e. $\overline{3}=\overline{a_0}\left(\overline{a_0}^2+\overline{2}\right)$. The only two possibilities are $\overline{a_0}\in\{\overline{1},\overline{3}\}$. If $\overline{a_0}=\overline{1}$, then $\overline{b_0}=\overline{3}$ and $\overline{3+b_1}=\overline{2}$, so $\overline{b_1}=\overline{4}$. That complies with $\overline{a_0+b_1}=\overline{0}=\overline{5}$. We can check that by multiplying the expressions in brackets: $(x+\overline{1})(x^2+\overline{4}x+\overline{3})=x^3+\overline{4}x^2+\overline{3}x+x^2+\overline{4}x+\overline{3}=x^3+\overline{5}x^2+\overline{2}x+\overline{3}$. Finally $\overline{2}(x+\overline{1})(x^2+\overline{4}x+\overline{3})=\overline{2}x^3+\overline{4}x+\overline{1}$, exactly the polynomial we wanted to factor. We can write:

$$\overline{2}x^3+\overline{4}x+\overline{1}=\overline{2}(x+\overline{1})(x^2+\overline{4}x+\overline{3}).$$

Let us check the case for $\overline{a_0}=\overline{3}$. We would have $\overline{b_0}=\overline{1}$ and $\overline{b_1}=-\overline{a_0}=\overline{2}$. Also, from $\overline{1+3\cdot 2}=\overline{7}=\overline{2}$, we have a guarantee that these solutions will work. Let us check: $\overline{2}(x+\overline{3})(x^2+\overline{2}x+\overline{1})=\overline{2}x^3+\overline{4}x^2+\overline{2}x+\overline{6}x^2+\overline{12}x+\overline{6}=\overline{2}x^3+\overline{10}x^2+\overline{14}x+\overline{6}=\overline{2}x^3+\overline{4}x+\overline{1}$, proving that this factorization is correct. Now, from these two factorizations we have (disregarding the factor of $\overline{2}$, which gets cancelled out):

$$(x+\overline{1})(x^2+\overline{4}x+\overline{3})=(x+\overline{3})(x^2+\overline{2}x+\overline{1}).$$

It is obvious that $\gcd(x+\overline{1},x+\overline{3})=1$, so by Euclid's lemma for polynomials, we have that $x+\overline{1}|x^2+\overline{2}x+\overline{1}$. Therefore, $x^2+\overline{2}x+\overline{1}=(x+\overline{1})(x+\overline{c_0})=x^2+\overline{c_0+1}+\overline{c_0}$. That implies $\overline{c_0}=1$, which is in accordance with $\overline{c_0+1}=\overline{1+1}=\overline{2}$. So, we have $x^2+\overline{2}x+\overline{1}=(x+\overline{1})^2$ and then:

$$(x+\overline{1})(x^2+\overline{4}x+\overline{3})=(x+\overline{3})(x+\overline{1})^2.$$

Last check, $(x+\overline{3})(x+\overline{1}) = x^2+\overline{4}x+\overline{3}$. In conclusion:

$$\overline{2}x^3+\overline{4}x+\overline{1} = \overline{2}\left(x+\overline{3}\right)\left(x+\overline{1}\right)^2.$$

Remark. We could have solved the problem more efficiently using the theorem from the following chapter, but we wanted do display some techniques without using the fact that $(x-c)|p(x)$ iff $p(x)=0$.

Problem. In $\mathbb{Z}/6\mathbb{Z}[x]$, factor each of the following into two polynomials of degree 1: x, $x+\overline{2}$, $x+\overline{3}$. Why is this possible?

Solution. We have $x = (\overline{3}x+\overline{2})(\overline{2}x+\overline{3})$, $x+\overline{2} = (\overline{3}x+\overline{2})(\overline{2}x+\overline{1})$ and $x+\overline{3} = (\overline{3}x+\overline{5})(\overline{2}x+\overline{3})$. That is possible because $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain and so is not $\mathbb{Z}/6\mathbb{Z}[x]$. Therefore, there exist elements that produce zero when multiplied which makes it possible for the leading term to become zero.

Proposition. Let F be a field and $a(x), b(x) \in F[x]$. Then,

1. If $a(x)$ and $b(x)$ are distinct monic polynomials, they cannot be associates.
2. Any two distinct irreducible polynomials are relatively prime.
3. If $a(x)$ is irreducible, any associate of $a(x)$ is irreducible.
4. If $a(x) \neq 0$, $a(x)$ cannot be an associate of 0.

Proof. *Ad* 1. Let $a(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ and $b(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$. Assume that $a(x) = kb(x)$, for some $k \in F$. If $m \neq n$, then also $a(x) \neq kb(x)$, i.e. they cannot be associates. Then assume that $m = n$ and we have $a(x) = kx^n + (kb_{n-1})x^{n-1} + (kb_1)x + (kb_0)$. Then, we would have the coefficients of leading terms correspond, i.e. $k = 1$. But, then $a(x) = b(x)$ which is a contradiction. *Ad* 2. If they were not relatively prime, their greatest common divisor would be some polynomial $p(x)$, which would mean $a(x) = p(x)a_1(x)$ and $b(x) = p(x)b_1(x)$, which is a contradiction to the fact that they are irreducible. *Ad* 3. Let $a(x)$ be irreducible and $b(x)$ an associate of $a(x)$. That means that $a(x) = kb(x)$, for some $k \in F$. If $b(x)$ were not irreducible, there would exist $p(x), q(x) \in F[x]$ such that $b(x) = p(x)q(x)$, but that would mean that $a(x) = kp(x)q(x)$, a contradiction to the condition of irreducibility of $a(x)$. *Ad* 4. Let $a(x) \neq 0$. Assume $a(x)$ is an associate of 0. Then, $a(x) = k0$, for some $k \in F$. But then $a(x) = k0 = 0$, a contradiction to assumption that $a(x) \neq 0$.

□

Proposition. Let $p \in P$. In $\mathbb{Z}/p\mathbb{Z}[x]$, every nonzero polynomial has exactly $p-1$ associates.

Proof. Let $a(X) \in \mathbb{Z}/p\mathbb{Z}[x]$ be a non-zero polynomial. As $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$, the number of associates of $a(x)$ is $|S|$, where $S = \{\overline{k}a(x) : \overline{k} \in \mathbb{Z}/p\mathbb{Z} - \{0\}\}$. We have excluded zero, as it can never be an associate of $a(x)$ (nor any of its multiples, which are actually, again, zeros). It is obvious that $|S| \leq p-1$, because $|\mathbb{Z}/p\mathbb{Z} - \{0\}| = p-1$. Assume $\overline{k_1}a(x) = \overline{k_2}a(x)$, for some $\overline{k_1}, \overline{k_2} \in \mathbb{Z}/p\mathbb{Z}[x]$ such that $\overline{k_1} \neq \overline{k_2}$. From $\overline{k_1}a(x) = \overline{k_2}a(x)$, as $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain (because $\mathbb{Z}/p\mathbb{Z}$ is a field), by cancellation law (as $a(x) \neq 0$) we have $\overline{k_1} = \overline{k_2}$, a contradiction to our assumption. Therefore, all $\overline{k}a(x) \in S$, for $\overline{k} \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ are mutually different for different $\overline{k} \in \mathbb{Z}/p\mathbb{Z} - \{0\}$. So, there are as many elements in S as there are in $\mathbb{Z}/p\mathbb{Z} - \{0\}$, and that implies $|S| = p - 1$.

□

Proposition. $x^2 + \overline{1}$ is reducible in $\mathbb{Z}/p\mathbb{Z}[x]$ if and only if there exist $a, b \in \mathbb{Z}^+$ such that $p = a + b$ and $ab \equiv 1 \pmod{p}$.

Proof. *Necessity.* Assume $x^2 + \overline{1}$ is reducible in $\mathbb{Z}/p\mathbb{Z}[x]$. Then we can write $x^2 + 1 = \overline{k}(x + \overline{a_0})(x + \overline{b_0})$, for some $\overline{k}, \overline{a_0}, \overline{b_0} \in \mathbb{Z}/p\mathbb{Z}$. We can assume $0 \leq k, a_0, b_0 < p$. Then, $\overline{k} = \overline{1}$ and it must be that $\overline{a_0} + \overline{b_0} = \overline{0}$ and $\overline{a_0} \cdot \overline{b_0} = \overline{1}$. From the latter condition, we have $a_0 b_0 \equiv 1 \pmod{p}$ and from the former, $a_0 + b_0 \equiv 0 \pmod{p}$. That implies $a_0 + b_0 = qp$, for some $q \in \mathbb{Z}$. But, as $a_0, b_0 < p$, we have $a_0 + b_0 < 2p$, so it must be that $q = 1$, i.e. $a_0 + b_0 = p$. *Sufficiency.* Let $p \in P$ and $a, b \in \mathbb{Z}^+$ such that $p = a + b$ (from which we get $\overline{a + b} = \overline{0}$, due to $a + b - 0 = p$) and $ab \equiv 1 \mod p$. Then, $(x + \overline{a})(x + \overline{b}) = x^2 + \overline{a + b}x + \overline{ab} = x^2 + \overline{1}$, so $x^2 + \overline{1}$ is reducible.

□

Proposition. Let $p \in P$. The number of irreducible quadratics in $\mathbb{Z}/p\mathbb{Z}[x]$ is:

$$(p-1)\left(p^2 - \left[\binom{p}{1} + \binom{p}{2}\right]\right).$$

Proof. Let $m \in \mathbb{Z}^+$. Then, $P_m = \{q(x) \in \mathbb{Z}/p\mathbb{Z}[x] : \deg q(x) = m\}$. Then, as for each $\overline{q_i}$ in $q(x) = \overline{q_m}x^m + \cdots + \overline{q_1}x + \overline{q_0}$ we can choose p elements (except for $\overline{q_m}$ which cannot be zero), we have that $|P_m| = (p-1)p^m$. That is the number of all polynomials of degree m with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Thus, $|P_2| = (p-1)p^2$. Let $I_m = \{q(x) \in P_m : (\forall a(x), b(x) \in \mathbb{Z}/p\mathbb{Z}[x])(q(x) \neq a(x)b(x))\}$. We know that all degree 1 polynomials are irreducible and they are of the form $q(x) = \overline{q_1}x + \overline{q_0}$, where $\overline{q_0}, \overline{q_1} \in \mathbb{Z}/p\mathbb{Z}$ and $\overline{q_1} \neq \overline{0}$. It is obvious that then $I_1 = P_1$ and $|I_1| = |P_1| = (p-1)p$.

Now, if a polynomial is reducible in P_2, then it can be written as a product of two polynomials in $I_1 = P_1$. Then, the number of ways in which we can choose two polynomials from I_1 (with the possibility of repeating the same, i.e. $(x+\overline{1})^2$) is equal to the number of ways in which we can distribute 2 balls in $|I_1|$ boxes[85]. Considering only monic polynomials as the "building blocks", which we can put in I_m^M (representing irreducible monic polynomials of degree m), the number of ways in which we can choose 2 polynomials in I_1^M (with repetition) is:

$$\binom{|I_1^M|+2-1}{2} = \binom{|I_1^M|+1}{2}.$$

The only thing left to do is to determine $|I_1^M|$. But, that is quite easy, as we only observe $x+\overline{q_0}$, and for that we have p choices. So, finally, the number of reducible polynomials in P_2, as we can put all coefficients except for zero to get non-monic polynomials (explaining $p-1$ as a coefficient of the binomial coefficient), is:

$$\begin{aligned} |I_2| &= |P_2| - (p-1)\binom{|I_1^M|+1}{2} \\ &= (p-1)p^2 - (p-1)\binom{p+1}{2}. \end{aligned}$$

That can be simplified as:

$$\begin{aligned} |I_2| &= (p-1)p^2 - (p-1)\binom{p+1}{1+1} \\ &= (p-1)p^2 - (p-1)\left[\binom{p}{1} + \binom{p}{2}\right]. \end{aligned}$$

The formula above actually gives us quite good combinatorial glimpse at how this works. We can either choose 1 polynomial from I_1 and then raise it to the second power or choose two different polynomials from I_1.

□

Remark. Reasoning the same as above, we can conclude that the number of irreducible cubics in $\mathbb{Z}/p\mathbb{Z}[x]$ is:

[85] Consider that each box represents a polynomial and that underline is the ball. Then, for example in $\mathbb{Z}/3\mathbb{Z}[x]$, we could have $x, x+\overline{1}, \underline{x+\overline{2}}, \overline{2}x, \underline{\overline{2}x+\overline{1}}, \overline{2}x+\overline{2}$ which would represent $(x+\overline{2})(\overline{2}x+\overline{1}) = \overline{2}x^2+\overline{2}x+\overline{2}$.

$$|I_3| = |P_3| - (p-1)\left[|I_2^M| \cdot |I_1^M| + \left(\binom{|I_1^M|}{3}\right)\right].$$

Proposition. Let F be a field and $J \trianglelefteq F[x]$. Then,

1. Any two generators of J are associates.
2. J has a unique monic generator $m(x) \in F[x]$.
3. Let $a(x) \in F[x]$. Then, $a(x) \in \langle m(x)\rangle$ if and only if $m(x)|a(x)$.
4. If $p(x) \in F[x]$ is irreducible, then $\langle p(x)\rangle$ is a maximal ideal of $F[x]$.

Proof. *Ad* 1. Let $a(x), b(x) \in J - \{0\}$ such that $J = \langle a(x)\rangle = \langle b(x)\rangle$. As $b(x) \in J = \langle a(x)\rangle$, then there exists $p(x) \in F[x]$ such that $b(x) = a(x)p(x)$. As $a(x) \in J = \langle b(x)\rangle$, then there exists $q(x) \in F[x]$ such that $a(x) = b(x)q(x)$. Multiplying that by $p(x)$ we get $a(x)p(x) = b(x)p(x)q(x)$ and that is equivalent to $b(x) = b(x)p(x)q(x)$. As $F[x]$ is an integral domain (because F is a field) and $b(x) \neq 0$, then $b(x) = b(x)p(x)q(x)$ implies $1 = p(x)q(x)$. From that follows that $p(x) = p_0$ and $q(x) = q_0$, where $p_0, q_0 \in F$. That means that $a(x) = q_0 b(x)$ and $b(x) = p_0 a(x)$ (with $q_0^{-1} = p_0$). To conclude, $a(x)$ and $b(x)$ are associates. *Ad* 2. Assume that $J = \langle m(x)\rangle$ where $m(x)$ is monic. Assume that also $J = \langle p(x)\rangle$ where $p(x)$ is monic and assume that they are distinct. Then, by previous result, $p(x)$ and $m(x)$ are associates. From a previous problem, there do not exist distinct monic associates, so it must be that $m(x) = p(x)$. *Ad* 3. Let $a(x) \in F[x]$. *Necessity.* Assume $a(x) \in \langle m(x)\rangle$. Then, there exists $p(x) \in F[x]$ such that $a(x) = m(x)p(x)$. From that we conclude that $m(x)|a(x)$. *Sufficiency.* Let $m(x)|a(x)$. Then by definition there exists $q(x) \in F[x]$ such that $a(x) = q(x)m(x)$. But, as $q(x) \in F[x]$, then $q(x)m(x) \in \langle m(x)\rangle$, i.e. $a(x) \in \langle m(x)\rangle$. *Ad* 4. Let $p(x) \in F[x]$ be irreducible. We have that $\langle p(x)\rangle \trianglelefteq F[x]$. Assume that there exists $J \trianglelefteq F[x]$ such that $\langle p(x)\rangle \subset J \subseteq F[x]$. Such J exists because $p(x) \neq 0$ and $F[x]$ is an integral domain, so it cannot be a trivial ring. Also, $F[x] - \langle p(x)\rangle \neq \emptyset$ (i.e. $F[x] \neq \langle p(x)\rangle$), because, i.e. $p(x)q(x) + 1 \in F[x]$, but $p(x) \notin \langle p(x)\rangle$. If the latter were the case we would have $p(x)q(x) + 1 = p(x)r(x)$, for some $r(x) \in F[x]$, which would imply $1 = p(x)[r(x) - q(x)]$, i.e. that $p(x)$ is a constant polynomial, a contradiction to the assumption that it is irreducible. So, $\langle p(x)\rangle \subset J \subseteq F[x]$ is possible and let $a(x) \in J - \langle p(x)\rangle$ such that $a(x) \neq 0$. As $a(x) \notin \langle p(x)\rangle$, then there does not exist $b(x)$ such that $a(x) = p(x)b(x)$, i.e. $p(x) \nmid a(x)$. That implies that, as $p(x)$ is irreducible, $\gcd(a(x), p(x)) = 1$. By Bezout's lemma for polynomials, there exist $q(x), r(x) \in J$ such that $a(x)q(x) + p(x)r(x) = 1$. As $a(x), q(x) \in J$ then $a(x)q(x) \in J$. Also, $p(x)r(x) \in \langle p(x)\rangle \subset J$, so $a(x)q(x) + p(x)r(x) = 1 \in J$. But, if we take $a(x) \in F[x]$, where $a(x) \neq 0$, then $a(x)1 \in J$, i.e. $a(x) \in J$ (because $J \trianglelefteq F[x]$). That implies

$F[x] \subseteq J$, and with $J \subseteq F[x]$, we have $J = F[x]$, meaning $\langle p(x) \rangle$ is maximal ideal of $F[x]$.

□

Proposition. Let S be the set of all polynomials $a_0 + a_1x + \cdots + a_mx^m \in F[x]$, such that $a_0 + a_1 + \cdots + a_m = 0$. Then, $x - 1 \in S$ and $S = \langle x - 1 \rangle$. Also, $F[x]/\langle x - 1 \rangle \cong F$.

Proof. It is obvious that $1x - 1 = x - 1 \in S$ because $1 + (-1) = 0$. Let $S' = \langle x - 1 \rangle$. Let $(x - 1)q(x) \in \langle x - 1 \rangle$. Then, if we take $q(x) = q_mx^m + \cdots + q_1x + q_0$, we have $(x-1)(q_mx^m+\cdots+q_1x+q_0) = q_mx^{m+1}+(q_{m-1}-q_m)x^m+\cdots+(q_1-q_2)x^2+(q_0-q_1)x-q_0$. Then, obviously $q_m + (q_{m-1} - q_m) + \cdots + (q_1 - q_2) + (q_0 - q_1) - q_0 = (q_m - q_m) + (q_{m-1} - q_{m-1}) + \cdots + (q_2 - q_2) + (q_1 - q_1) + (q_0 - q_0) = 0$. Therefore $(x - 1)q(x) \in S$, i.e. $S' \subseteq S$. Let $q(x) \in S$. Then, $q_m + \cdots + q_1 + q_0 = 0$. We will show that $x - 1|q(x)$, for all degrees $m \in \mathbb{Z}^+ - \{1\}$ (note that $0 \in S$ and $0 \in \langle x - 1 \rangle$, so we will exclude that case; also note that there are no constant polynomials in $\langle x - 1 \rangle$). Then, let $q(x) = q_mx^m + \cdots + q_1x + q_0 \in S$. We have $q_m + \cdots + q_1 + q_0 = 0$. Then, $q_0 = -(q_m + \cdots + q_1)$ and we have $q_m(x^m - 1) + q_{m-1}(x^{m-1} - 1) + \cdots + q_1(x - 1)$. From a previous proposition (for all rings with unity, at the beginning of the ring theory), we know that $x - 1|x^n - 1$, for all $n \in \mathbb{Z}^+$. Therefore, we can write $q(x) = q_mx^m + \cdots + q_1x + q_0 = (x - 1)[q_ma_m(x) + \cdots + q_1a_1(x)]$, where $a_n(x) \in F[x]$, for all $0 < n \leq m$, such that $(x^n - 1) = (x - 1)a_n(x)$. From that we have $x - 1|q(x)$ and it must be that $x - 1 \in \langle x - 1 \rangle$, i.e. $S \subseteq \langle x - 1 \rangle$. That implies $S = \langle x - 1 \rangle$.

Now, define $f : F[x] \to F$ such that $f(q_mx^m + \cdots + q_1x + q_0) = q_m + \cdots + q_1 + q_0$. It is obvious that f is a well defined function, as it is defined for all $q(x) \in F[x]$ and if $q(x) = p(x)$, it follows that $q_i = p_i$, for all $0 \leq i \leq \deg q(x) = \deg p(x)$, so $q_{\deg q(x)} + \cdots + q_1 + q_0 = p_{\deg q(x)} + \cdots + p_1 + p_0$. If we take $a \in F$, then, $ax - a \in F[x]$ and $a + (-a) = 0$, so there exists $ax - a$ such that $f(ax - a) = a$. However, f is not injective as also $ax^m - a \in F[x]$, for all $m \in \mathbb{Z}^+$, and $a + (-a) = 0$. But, as it is surjective, as we have proved, by fundamental homomorphism theorem for rings, we have $F \cong F[x]/\ker(f)$. It is obvious that $\ker(f) = \{q_mx^m + \cdots + q_1x + q_0 \in F[x] : q_m + \cdots + q_1 + q_0 = 0\} = \langle x - 1 \rangle$, so $F \cong F[x]/\langle x - 1 \rangle$.

□

Proposition. Let F be a field. Then, $F[x, y]$ is not a principal ideal domain.

Proof. Let $J \trianglelefteq F[x, y]$ such that J contains all polynomials in $F[x, y]$ whose constant coefficient is zero (it is obvious that J is an ideal, as the sum and product of two polynomials with zero constant coefficients will give a polynomial with a zero constant coefficient; also the product of a polynomial with a zero coefficient and a

polynomial with a non-zero coefficient will again yield a polynomial with a zero constant coefficient). Assume that $\langle q(x,y)\rangle = J$. But, then $x+y \in J$ and it must be $x+y = q(x,y)p(x,y)$, where $p(x,y) \in F[x,y]$. But, it is obvious that $x+y$ cannot split in $F[x,y]$. It's degree is 1 and it would have to be $q(x,y)=1$ and $p(x,y)=0$ or $p(x,y)=1$ and $q(x,y)=0$; the latter is not possible at all, but the former would only imply that $q(x,y) = x+y$, meaning that $x+y$ is irreducible. It is obvious that, for example, $x+y \nmid x$, although $x \in J$, so J cannot be a principal ideal domain.

□

Problem. In $\mathbb{Q}$, using the Euclidean algorithm find the greatest common divisor of: (a) x^3+1 and $x^4+x^3+2x^2+x-1$; (b) $x^{24}-1$ and $x^{15}-1$. Express the greatest common divisors as the linear combinations of those two pairs of polynomials.

Solution. (a) Using the algorithm for polynomial division, we have:

$$\begin{array}{rl} & (x^4+x^3+2x^2+x-1) : (x^3+1) = x+1 \\ - & \underline{(x^4+x)} \\ & x^3+2x^2-1 \\ - & \underline{(x^3+1)} \\ & 2x^2-2. \end{array}$$

Thus, $x^4+x^3+2x^2+x-1 = (x^3+1)(x+1)+(2x^2-2)$ and we then divide x^3+1 by $2x^2-2$ to get:

$$\begin{array}{rl} & (x^3+1) : (2x^2-2) = \dfrac{1}{2}x \\ - & \underline{(x^3-x)} \\ & x+1. \end{array}$$

From that we have $x^3+1 = \frac{x}{2}(2x^2-2)+(x+1)$. Then, we divide $2x^2-2$ by $x+1$. That is easy to do because $2x^2-2 = 2(x^2-1) = 2(x+1)(x-1)$, so $2x^2-2 = (2x-2)(x+1)$. As here remainder is zero, the last residue is $x+1$, and that means that:

$$\gcd(x^4+x^3+2x^2+x-1, x^3+1) = x+1.$$

In order to express the greatest common divisor as the linear combination of these two polynomials, we need to roll back the following process:

$$\begin{aligned} x^4+x^3+2x^2+x-1 &= (x^3+1)(x+1)+(2x^2-2), \\ x^3+1 &= \frac{x}{2}\left(2x^2-2\right)+(x+1), \\ 2x^2-2 &= (2x-2)(x+1). \end{aligned}$$

From the first row, we have $2x^2-2=(x^4+x^3+2x^2+x-1)-(x^3+1)(x+1)$. Substituting that for $2x^2-2$ obtained from the second row as $x+1=(x^3+1)-\frac{x}{2}(2x^2-2)$, we finally get $x+1=(x^3+1)-\frac{x}{2}\left[(x^4+x^3+2x^2+x-1)-(x+1)(x^3+1)\right]$. That is equivalent to:

$$x+1=\left(\frac{x^2}{2}+\frac{x}{2}+1\right)\left(x^3+1\right)+\left(-\frac{x}{2}\right)\left(x^4+x^3+2x^2+x-1\right).$$

Notice that this would not be possible to find in $\mathbb{Z}[x]$ as we have rational coefficients in some terms. (b) We will divide $x^{24}-1$ by $x^{15}-1$ first:

$$\begin{array}{rl} & \left(x^{24}-1\right):\left(x^{15}-1\right)=x^9 \\ - & \underline{\left(x^{24}-x^9\right)} \\ & x^9-1. \end{array}$$

Therefore, $x^{24}-1=x^9\left(x^{15}-1\right)+\left(x^9-1\right)$. Now, we divide $x^{15}-1$ by x^9-1. We have:

$$\begin{array}{rl} & \left(x^{15}-1\right):\left(x^9-1\right)=x^6 \\ - & \underline{\left(x^{15}-x^6\right)} \\ & x^6-1. \end{array}$$

So, as $x^{15}-1=x^6\left(x^9-1\right)+\left(x^6-1\right)$, we divide x^9-1 by x^6-1 and:

$$\begin{array}{rl} & \left(x^9-1\right):\left(x^6-1\right)=x^3 \\ - & \underline{\left(x^9-x^3\right)} \\ & x^3-1. \end{array}$$

Then, $x^9-1=x^3\left(x^6-1\right)+\left(x^3-1\right)$ and we must divide x^6-1 by x^3-1. That is easy

to do because $x^6 - 1 = (x^3 + 1)(x^3 - 1)$. We now know, as the last residue is $x^3 - 1$, that

$$\gcd\left(x^{24} - 1, x^{15} - 1\right) = x^3 - 1.$$

In order to express the greatest common divisor as the linear combination of $x^{24} - 1$ and $x^{15} - 1$, we need to roll back the whole process:

$$\begin{aligned} x^{24} - 1 &= x^9\left(x^{15} - 1\right) + \left(x^9 - 1\right), \\ x^{15} - 1 &= x^6\left(x^9 - 1\right) + \left(x^6 - 1\right), \\ x^9 - 1 &= x^3\left(x^6 - 1\right) + \left(x^3 - 1\right), \\ x^6 - 1 &= \left(x^3 + 1\right)\left(x^3 - 1\right). \end{aligned}$$

First, $x^3 - 1 = (x^9 - 1) - x^3(x^6 - 1)$ (from the third row). Then, from the second row, $x^6 - 1 = (x^{15} - 1) - x^6(x^9 - 1)$ and substituting that in the third row we have $x^3 - 1 = (x^9 - 1) - x^3\left[(x^{15} - 1) - x^6(x^9 - 1)\right]$. That can be written more neatly as $x^3 - 1 = (x^9 - 1)(x^9 + 1) - x^3(x^{15} - 1)$. From the first row we have $x^9 - 1 = (x^{24} - 1) - x^9(x^{15} - 1)$, and substituting that in the former expression, we get $x^3 - 1 = (x^9 + 1)\left[(x^{24} - 1) - x^9(x^{15} - 1)\right] - x^3(x^{15} - 1)$. Finally, that is equivalent to:

$$x^3 - 1 = \left(x^9 + 1\right)\left(x^{24} - 1\right) + \left(-x^{18} - x^9 - x^3\right)\left(x^{15} - 1\right).$$

Problem. In $\mathbb{Z}/3\mathbb{Z}$, using the Euclidean algorithm find the greatest common divisor of $x^3 + \overline{1}$ and $x^4 + x^3 + \overline{2}x^2 + x - \overline{1}$. Express the greatest common divisor as the linear combination of those two polynomials.

Solution. Using the algorithm for polynomial division to divide $x^4 + x^3 + \overline{2}x^2 + x - \overline{1}$ by $x^3 + \overline{1}$ we have:

$$\begin{array}{rl} & \left(x^4 + x^3 + \overline{2}x^2 + x - \overline{1}\right) : \left(x^3 + \overline{1}\right) = x + \overline{1} \\ - & \underline{(x^4 + x)} \\ & x^3 + \overline{2}x^2 - \overline{1} \\ - & \underline{(x^3 + \overline{1})} \\ & \overline{2}x^2 - \overline{2}. \end{array}$$

That means that $x^4 + x^3 + \overline{2}x^2 + x - \overline{1} = \left(x + \overline{1}\right)\left(x^3 + \overline{1}\right) + \left(\overline{2}x^2 - \overline{2}\right)$. Then we divide $x^3 + \overline{1}$ by $\overline{2}x^2 - \overline{2}$ and we have:

$$\begin{array}{rl} & \left(x^3+\overline{1}\right) : \left(\overline{2}x^2-\overline{2}\right) = \overline{2}x \\ - & \underline{(x^3-x)} \\ & x+\overline{1}. \end{array}$$

From that we have $x^3+\overline{1} = \overline{2}x\left(\overline{2}x^2-\overline{2}\right)+\left(x+\overline{1}\right)$. We divide $\overline{2}x^2-\overline{2}$ by $x+\overline{1}$ easily as $\overline{2}x^2-\overline{2} = \overline{2}\left(x^2-\overline{1}\right) = \overline{2}\left(x+\overline{1}\right)\left(x-\overline{1}\right)$. We have $\overline{2}x^2-\overline{2} = \left(\overline{2}x-\overline{2}\right)\left(x+\overline{1}\right)$. That implies:

$$\gcd\left(x^4+x^3+\overline{2}x^2+x-\overline{1}, x^3+\overline{1}\right) = x+\overline{1}.$$

Unrolling the following process will give us the greatest common divisor as the linear combination of those two polynomials:

$$\begin{aligned} x^4+x^3+\overline{2}x^2+x-\overline{1} &= \left(x+\overline{1}\right)\left(x^3+\overline{1}\right)+\left(\overline{2}x^2-\overline{2}\right), \\ x^3+\overline{1} &= \overline{2}x\left(\overline{2}x^2-\overline{2}\right)+\left(x+\overline{1}\right), \\ \overline{2}x^2-\overline{2} &= \left(\overline{2}x-\overline{2}\right)\left(x+\overline{1}\right). \end{aligned}$$

From the second row we have $x+\overline{1} = \left(x^3+\overline{1}\right)-\overline{2}x\left(\overline{2}x^2-\overline{2}\right)$ and from the first row $\overline{2}x^2-\overline{2} = \left(x^4+x^3+\overline{2}x^2+x-\overline{1}\right)-\left(x+\overline{1}\right)\left(x^3+\overline{1}\right)$. Substituting latter expression into the former expression we finally obtain the equality for the greatest common divisor, $x+\overline{1} = \left(x^3+\overline{1}\right)-\overline{2}x\left[\left(x^4+x^3+\overline{2}x^2+x-\overline{1}\right)-\left(x+\overline{1}\right)\left(x^3+\overline{1}\right)\right]$. That is equivalent to:

$$x+\overline{1} = x\left(x^4+x^3+\overline{2}x^2+x+\overline{2}\right)+\left(\overline{2}x^2+\overline{2}x+\overline{1}\right)\left(x^3+\overline{1}\right).$$

Proposition. Let F be a field, $G \subseteq F[x]$ such that $a(x) \in G$ if and only if constant term of $a(x)$ is non-zero. Let $h : G \to G$ be a mapping defined by:

$$h(a_0+a_1x+\cdots+a_mx^m) = a_m+a_{m-1}x+\cdots+a_0x^m.$$

Then:

1. h is a function and, for all $a(x), b(x) \in G$, $h(a(x)b(x)) = h(a(x))h(b(x))$;
2. h is injective, surjective and $h \circ h = \epsilon$;

3. $a(x)$ is irreducible if and only if $h(a(x))$ is irreducible;

4. If $c \in F$, $a(c) = 0$ if and only if $[h\,(a(x))]\,(c^{-1}) = 0$.

Proof. *Ad* 1. It is obvious that h is defined for all $a(x)$. Assume $a(x) = b(x)$. Then, $\deg a(x) = \deg b(x)$ and they have equal corresponding coefficients. It's easy to see that then $h(a(x)) = h(b(x))$, so h is a function. Let $a(x), b(x) \in G$. As the constant term of $a(x), b(x)$ is non-zero, then $\deg a(x) = \deg h(a(x))$ and $\deg b(x) = \deg h(b(x))$. So, $\deg h(a(x)b(x)) = \deg a(x)b(x) = \deg a(x) + \deg b(x) = \deg h(a(x)) + \deg h(b(x))$. Then, the k-th term of $h(a(x)b(x))$ is equal to $c_{\deg c-k}$ and k-th term of $h(a(x))h(b(x))$ is equal to:

$$c_k = \sum_{i+j=k} a_{\deg a(x)-i} b_{\deg b(x)-j} = \sum_{\deg a(x)-i+\deg b(x)-j=k} a_i b_j = \sum_{i+j=\deg a(x)b(x)-k} a_i b_j.$$

That is equal to the k-th coefficient of $h(a(x)b(x))$. Therefore, $h(a(x))h(b(x)) = h(a(x)b(x))$.

Ad 2. Let $h(a(x)) = h(b(x))$. Then, $\deg h(a(x)) = \deg h(b(x)) = m$ and their coefficients correspond. But then, also their $(m-i)$-th coefficients correspond, so $a(x) = b(x)$. If $a(x) \in G$, then it is obvious that there exists $b(x) \in G$ such that $h(b(x)) = a(x)$. Finally, h carries i-th coefficient to $(m-i)$-th and applying it again, it will carry $(m-i)$-th coefficient to $m-(m-i) = i$, so $h(h(a(x))) = a(x)$.

Ad 3. *Necessity.* Assume that $a(x)$ is irreducible and that $h(a(x))$ is not irreducible. Then, $h(a(x)) = p(x)q(x)$, for some $p(x), q(x) \in F[x]$. Applying h again gives us $h(h(a(x))) = h(p(x)q(x))$, i.e. $a(x) = h(p(x))h(q(x))$, meaning that $a(x)$ is not irreducible, which is a contradiction. *Sufficiency.* Follows the same line of reasoning as necessity.

Ad 4. Let $c \in F$. *Necessity.* Assume $a(c) = 0$. Then, $a(x) = (x-c)q(x)$, for some $q(x) \in G$ and we have $h(a(x)) = h((x-c)q(x))$, which implies $h(a(x)) = h(x-c)h(q(x))$. But, $h(x-c) = -cx+1$, so $h(a(x)) = (1-cx)h(q(x))$. Now, from $-cx+1 = 0$ we have $-cx = -1$, and after multiplying by $-c^{-1} \in F$, $x = c^{-1}$. Thus, if $b(x) = h(a(x))$, we have $b(c^{-1}) = (1-cc^{-1})h(q(x)) = 0h(q(x)) = 0$. So, $b(c^{-1}) = [h(a(x))](c^{-1}) = 0$. *Sufficiency.* The line of reasoning is the same as for necessity.

□

Problem. Let $a_0 + a_1x + \cdots + a_mx^m = (b_0 + \cdots + b_px^p)(c_0 + \cdots + c_qx^q)$. Factor $h(a(x))$ (where h is the function from the theorem above).

Solution. Let $b(x) = h(a(x))$. Then, $b(x) = h((b_0 + \cdots + b_px^p)(c_0 + \cdots + c_qx^q)) = h(b_0 + \cdots + b_px^p)h(c_0 + \cdots + c_qx^q) = (b_0x^p + \cdots + b_{p-1}x + b_p)(c_0x^p + \cdots + c_{q-1}x + c_q)$.

Substitution in polynomials

Definition. Let A be a ring, $p(x) \in A[x]$ and $c \in A$. If $p(x) = p_m x^m + \cdots + p_1 x + p_0$, we define $p(c) = p_m c^m + \cdots + p_1 c + p_0$. Furthermore, if $p(c) = 0$, then we say that c is a **root** of $p(x)$ in A.

Remark. Notice that if $c \in A$, then also $p(c) \in A$ (it is closed with respect to powers with non-negative exponents, multiplication and addition). Also, in this light we can say that p is a function from A to A, i.e. $p : A \to A$. But, then notion of equality of polynomials and equality of polynomial functions do not necessarily coincide; polynomial functions $p : A \to A$ and $q : A \to A$ are equal if $p(x) = q(x)$ for all $x \in A$.

Lemma. Let A be an integral domain. Then, $x - c | x^k - c^k$ in $A[x]$, for all $k \in \mathbb{Z}^+$ and $c \in A$.

Proof. Let $c \in A$. Let $k = 1$. Trivial, $x^1 - c^1 = x - c = 1(x - c)$ (as $1 \in A$), so $x - c | x - c$. Assume that the statement is true for some $k \in \mathbb{Z}^+$, i.e. $x^k - c^k = (x - c)q(x)$, for some $q(x) \in A[x]$. We will show it is true for $k + 1$. We have $x^{k+1} - c^{k+1} = x^k x + c^k x - c^k c - c^k x = x(x^k - c^k) + c^k x - c^k c = x(x^k - c^k) + c^k(x - c)$. By assumption of induction, that is equivalent to $x^{k+1} - c^{k+1} = x(x - c)q(x) + c^k(x - c) = (x - c)(xq(x) + c^k)$, so $x - c | x^{k+1} - c^{k+1}$. Thus, $x - c | x^k - c^k$, for all $k \in \mathbb{Z}^+$.

□

Theorem. Let A be an integral domain, $p(x) \in A[x]$ and $c \in A$. Then, c is a root of $p(x)$ in A if and only if $x - c | p(x)$.

Proof. *Necessity*[86]. Let $c \in A$ be a root of $p(x)$, i.e. $p(c) = 0$. Then, $p(x) = p(x) - 0 = p(x) - p(c)$. From that, if $p(x) = p_m x^m + \cdots + p_1 x + p_0$, we have $p(x) - p(c) = (p_m x^k + \cdots + p_1 x + p_0) - (p_m c^k + \cdots + p_1 c + p_0) = p_m \cdot (x^k - c^k) + \cdots + p - 1(x - c)$. By previous lemma $x - c | x^k - c^k$, for all $k \in \mathbb{Z}^+$, so there exist $q_m, \cdots, q_1 \in A[x]$ such that $p(x) - p(c) = p_m \cdot (x - c)q_m(x) + \cdots + p_1(x - c)q_1(x) = (x - c)(p_m q_m(x) + \cdots + p_1 q_1(x))$. Therefore, $x - c | p(x) - p(c)$, and as $p(x) - p(c) = p(x) - 0 = p(x)$, we have $x - c | p(x)$.

Sufficiency. Let $c \in A$ and $x - c | p(x)$. That means that there exists $q(x) \in A[x]$ such that $p(x) = (x - c)q(x)$. Substituting c in place of x gives us $p(c) = (c - c)q(c)$, i.e. $p(c) = 0q(c)$. That implies $p(c) = 0$, i.e. c is a root of $p(x)$ in A.

[86] Proven for fields easier as follows. Assume that $c \in F$ is a root of $p(x)$ and that $x - c \nmid p(x)$. That would mean that there exist $q(x), r(x) \in F[x]$ such that $p(x) = (x - c)q(x) + r(x)$, where $0 \leq \deg r(x) < \deg (x - c) = 1$. That implies that $\deg r(x) = 0$, i.e. $r(x) = r_0$, where $r_0 \in F$. Now, from $p(c) = 0$ we have $p(c) = (c - c)q(c) + r_0$, i.e. $0 = 0q(c) + r_0$. That would imply $r_0 = 0$, which is a contradiction to the fact that the degree of $r(x)$ is defined. Therefore, it must be that $x - c | p(x)$.

□

Corollary. Let A be an integral domain and $p(x) \in A[x]$. If $c_1, \ldots, c_m \in A$, where $m \in \mathbb{Z}^+$, are distinct roots of $p(x)$ in A, then $(x - c_1) \cdots (x - c_m) | p(x)$.

Proof. Let $m = 1$. Then, $c_1 \in A$ is a root of $p(x)$ so, by previous theorem, $x - c_1 | p(x)$. Assume the statement is true for some m. Then, assume $c_1, \ldots, c_m, c_{m+1}$ are roots of $p(x)$. Then, as $c_1, \ldots, c_m$ are distinct roots of $p(x)$, we have that $(x-c_1) \cdots (x-c_m) | p(x)$, i.e. there exists $q(x) \in A[x]$ such that $p(x) = q(x)(x - c_1) \cdots (x - c_m)$. As c_{m+1} is a root of $p(x)$, then $0 = p(c_{m+1}) = q(c_{m+1})(c_{m+1} - c_1) \cdots (c_{m+1} - c_m)$. As A is an integral domain, then so $A[x]$ is an integral domaina and either $q(c_{m+1}) = 0$ or $c_{m+1} - c_i = 0$, for some $i \in \{1, \ldots, m\}$. If $q(c_{m+1}) = 0$, then c_{m+1} is a root of $q(x)$ and we have that $x - c_{m+1} | q(x)$, by previous theorem. In other words, there exists $q_1(x) \in A[x]$ such that $q(x) = q_1(x)(x - c_{m+1})$. That implies $p(x) = q_1(x)(x - c_{m+1})(x - c_1) \cdots (x - c_m)$, i.e. $(x - c_1) \cdots (x - c_{m+1}) | p(x)$. If $q(c_{m+1}) \neq 0$, then $c_{m+1} - c_i = 0$ implies $c_{m+1} = c_i$, which is a contradiction to the fact that $c_1, \ldots, c_{m+1}$ are distinct.

□

Corollary. Let A be an integral domain and $p(x) \in A[x]$. If $\deg p(x) = m$, for some $m \in \mathbb{Z}^+$, then $p(x)$ has at most m distinct roots.

Proof. Assume that $p(x)$ has more than m roots, i.e. $c_1, \ldots, c_{m+k}$, where $k \in \mathbb{Z}^+$. Then, by previous corollary, $(x - c_1) \cdots (x - c_{m+k}) | p(x)$. So, there exists $q(x) \in A[x]$ such that $p(x) = q(x)(x - c_1) \cdots (x - c_{m+k})$. But that means, because $\deg (x - c_i) = 1$, for all $i \in \{1, \ldots, m + k\}$, that $m = \deg p(x) = \deg q(x) + (m + k)$, i.e. $\deg q(x) = -k$, which is impossible.

□

Corollary. Let $q(x) \in \mathbb{Q}[x]$ and let $r_1, \ldots, r_m \in \mathbb{Q}$ be roots of $q(x)$. Then, there exists $p(x) \in \mathbb{Z}[x]$ with same roots as $q(x)$.

Proof. By previous corollary, $q(x) = q_1(x)(x - r_1) \cdots (x - r_m)$. Let $f : \mathbb{Q} \to \mathbb{Z}^+$ be a function defined with $f\left(\frac{a}{b}\right) = b$. Then, it is easy to see that $f(r_1 \cdots r_m)(x - r_1) \cdots (x - r_m)$ is a polynomial with integer coefficients and that its roots are $r_1, \ldots, r_m$. Then, let $g : \mathbb{Q}[x] \to \mathbb{Z}^+$ be a function defined with $g\left(\frac{a_m}{b_m} x^m + \cdots + \frac{a_1}{b_1} x + \frac{a_0}{b_0}\right) = b_m \cdots b_1 b_0$. Then, $g(q_1(x))q_1(x)$ is obviously a polynomial with integer coefficients. So,

$$\begin{aligned} p(x) &= g(q_1(x)) f(r_1 \cdots r_m) q(x) \\ &= g(q_1(x)) q_1(x) f(r_1 \cdots r_m)(x - r_1) \cdots (x - r_m) \end{aligned}$$

is a polynomial with integer coefficients and with roots $r_1, \ldots, r_m$.

□

Theorem. Let $q(x) \in \mathbb{Z}[x]$ such that $q(x) = q_m x^m + \cdots + q_1 x + q_0$ and $m \in \mathbb{Z}^+$. If there exists $\frac{a}{b} \in \mathbb{Q}$ such that $q\left(\frac{a}{b}\right) = 0$ and $\gcd(a, b) = 1$, then $a|q_0$ and $b|q_m$.

Proof. For $m = 1$, it is easy to see that, if $q_1 \frac{a}{b} + q_0 = 0$, then $q_1 a = (-q_0)b$, so as $\gcd(a, b) = 1$, by Euclid's lemma, we have $a|q_0$ and $b|q_1$. Let $m = 2$. Assume there exists $\frac{a}{b} \in \mathbb{Q}$ such that $q_m \left(\frac{a}{b}\right)^m + \cdots + q_1 \left(\frac{a}{b}\right) + q_0 = 0$. If we multiply that equality with b^m, we get $q_m a^m + q_{m-1} a^{m-1} b + \cdots + q_1 a b^{m-1} + q_0 b^m = 0$. That is equivalent to $(-q_m)a^m + (-q_{m-1})a^{m-1}b + \cdots + (-q_1)ab^{m-1} = q_0 b^m$. If we factor out a on the left-hand side, we get $ac = q_0 b^m$, where $c = (-q_m)a^{m-1}b + (-q_{m-1})a^{m-2}b^{m-1} + \cdots + (-q_2)ab^{m-2} + (-q_1)b^{m-1}$. As $q_i, a^i, b^i \in \mathbb{Z}$, for all $i \in \mathbb{Z}_0^+$, then also $c \in \mathbb{Z}$. So, from $ac = q_0 b^m$, because $\gcd(a, b) = 1$, by Euclid's lemma, we get that $a|q_0$. Similarly, from $q_m a^m + q_{m-1} a^{m-1} b + \cdots + q_1 a b^{m-1} + q_0 b^m = 0$ we get $q_m a^m = (-q_{m-1})a^{m-1}b + \cdots + (-q_1)ab^{m-1} + (-q_0)b^m = 0$. When we factor out b on the right-hand side we get $q_m a^m = bd$, where $d = (-q_{m-1})a^{m-2} + \cdots + (-q_1)ab^{m-2} + (-q_0)b^{m-1}$. Again, it is obvious that $d \in \mathbb{Z}$, because $q_i, a^i, b^i \in \mathbb{Z}$ for all $i \in \mathbb{Z}_0^+$. So, by Euclid's lemma, from $q_m a^m = bd$ and $\gcd(a, b) = 1$, we have that $b|q_m$.

□

Corollary. Let $q(x) \in \mathbb{Z}[x]$ such that $q(x) = x^m + q_{m-1} x^{m-1} + \cdots + q_1 x + q_0$ (it is monic) and $m \in \mathbb{Z}^+$. If $q(a) \neq 0$, for all $a \in \mathbb{Z}$ such that $a|q_0$, then $q(x)$ has no roots in $\mathbb{Q}$.

Proof. Assume that there exists $\frac{a}{b} \in \mathbb{Q}$ such that $q\left(\frac{a}{b}\right) = 0$. Then, by previous proposition, it must be that $a|q_0$ and $b|q_m$. But, as $q(x)$ is monic, we have $q_m = 1$, so $b = \pm 1$. That implies that $\frac{a}{b} = \frac{\pm a}{1} \in \mathbb{Z}$ and we can denote $c = \frac{\pm a}{1} = \pm a$. As $a|q_0$, then also $\pm a|q_0$, i.e. $c|q_0$. But, assumption of proposition implies that, as $c \in \mathbb{Z}$ and as $c|q_0$ that $q(c) \neq 0$, which is a contradiction to our assumption.

□

Lemma (Gauss). Let $a(x), b(x), c(x) \in \mathbb{Z}[x]$ such that $a(x) = b(x)c(x)$. Let $p \in P$. If p divides every coefficient of $a(x)$, then p divides every coefficient of $b(x)$ or $c(x)$.

Proof. As p divides all coefficients of $a(x)$, then we can write $a(x) = pa_1(x)$. But then $pa_1(x) = b(x)c(x)$. That implies that $p|b(x)c(x)$. If $p|b(x)$ then p divides every coefficient of $b(x)$ and we are done. If $p \nmid b(x)$, then, as the only divisors of p are ± 1 and

$\pm p$, it must be that $\gcd(p, b(x)) = 1$. That implies that there exist $q(x), r(x) \in \mathbb{Z}[x]$ such that $pq(x)+b(x)r(x) = 1$. From that we have $b(x)r(x) = 1-pq(x)$. From $pa_1(x) = b(x)c(x)$ we have $pa_1(x)r(x) = b(x)c(x)r(x)$ and then $pa_1(x)r(x) = c(x)[1 - pq(x)]$. That is equivalent to $pa_1(x)r(x)+c(x)pq(x) = c(x)$, i.e. $p[a_1(x)r(x)+c(x)q(x)] = c(x)$. From that follows that $p|c(x)$, i.e. p divides every coefficient of $c(x)$.

□

Lemma (Gauss). Let $a(x) \in \mathbb{Z}[x]$ and $b(x), c(x) \in \mathbb{Q}[x]$ such that $a(x) = b(x)c(x)$. Then, there exist $b_1(x), c_1(x) \in \mathbb{Z}[x]$ such that $a(x) = b_1(x)c_1(x)$, where $b_1(x) = kb(x)$ and $c_1(x) = lc(x)$ for some $k, l \in \mathbb{Z}$.

Proof. Let $f : \mathbb{Q} \to \mathbb{Z}^+$ be a function defined with $f\left(\frac{m}{n}\right) = n$. Also, let $g : \mathbb{Q}[x] \to \mathbb{Z}^+$ be defined with $g\left(a_m x^m + \cdots + a_1 x + a_0\right) = f(a_0)f(a_1)\cdots f(a_m)$. Then, as in a previous corollary, we have that $g(b(x))b(x) \in \mathbb{Z}[x]$ and $g(c(x))c(x) \in \mathbb{Z}[x]$. We define $k = g(b(x))$ and $l = g(c(x))$. Also, we define $b_2(x) = kb(x)$ and $c_2(x) = lc(x)$. Then, $b_2(x)c_2(x) = klb(x)c(x) = kla(x)$. By using fundamental theorem of arithmetic, $k = p_1 \cdots p_s$ and $l = q_1 \cdots q_t$, where $p_i, q_j \in P$, for all $i \in \{1, \ldots, s\}$, where $s \in \mathbb{Z}^+$, and for all $j \in \{1, \ldots, t\}$, where $t \in \mathbb{Z}^+$. Then, by previous lemma, from $b_2(x)c_2(x) = kla(x)$, which is equivalent to $b_2(x)c_2(x) = (p_1 \cdots p_s)(q_1 \cdots q_t)a(x)$, we have that p_i and p_j divide all coefficients of $b_2(x)$ or $c_2(x)$. Thus, after dividing coefficients of $b_2(x)$ and $c_2(x)$ with p_i and q_j, we obtain $b_1(x), c_1(x) \in \mathbb{Z}[x]$ such that $a(x) = b_1(x)c_1(x)$.

□

Remark. Let $a(x) = (3x - 2)\left(4x + \frac{3}{5}\right)$. Then, from the proof of Gauss' lemma, we have $k = g(3x - 2) = f(3)f(-2) = 1$ and $l = g\left(4x + \frac{3}{5}\right) = f(4)f\left(\frac{3}{5}\right) = 5$. Then, $b_2 = 3x - 2$ and $c_2 = 5\left(4x + \frac{3}{5}\right) = 20x + 3$. We have $kla(x) = klb_2(x)c_2(x)$, i.e. $5a(x) = (3x-2)(20x+3)$. We see that Gauss' lemma doesn't apply here. Why is that? Because we have $a(x)$ has to be in $\mathbb{Z}[x]$, and here, implicitly, $(3x - 2)(4x + \frac{3}{5}) \notin \mathbb{Z}[x]$.

Theorem (Eisenstein's Criterion) Let $a(x) \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}^+$ such that $a(x) = a_m x^m + \cdots + a_1 x + a_0$ and $a_m \neq 0$. If there exists $p \in P$ such that $p \nmid a_m$, $p^2 \nmid a_0$ and $p \mid a_i$, for all $i \in \{0, \ldots, m - 1\}$, then $a(x)$ is irreducible over $\mathbb{Q}$.

Proof. Assume that $a(x)$ is reducible over $\mathbb{Q}$. Then, there exist $q_1(x), r_1(x) \in \mathbb{Q}[x]$ such that $a(x) = q_1(x)r_1(x)$. But, as $a(x) \in \mathbb{Z}[x]$ and $q_1(x), r_1(x) \in \mathbb{Q}[x]$, we can apply the previous lemma to obtain $q(x), r(x) \in \mathbb{Z}[x]$ such that $a(x) = q(x)r(x)$. Let $m, n(q(x)), n(r(x)) \in \mathbb{Z}_0^+$ (here we consider a function $n : \mathbb{Z}[x] \to \mathbb{Z}_0^+$) so that $a(x) = a_m x^m + \cdots + a_1 x + a_0$, $q(x) = q_{n(q(x))} x^{n(q(x))} + \cdots + q_1 x + q_0$ and $r(x) = r_{n(r(x))} x^{n(r(x))} + \cdots + r_1 x + r_0$. Let $f : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ be a function defined with

$f(a_m x^m + \cdots + a_1 x + a_0) = \overline{a_m} x^m + \cdots + \overline{a_1} x + \overline{a_0}$. Thus, f is a homomorphism (we have already proved it before). If we take $a(x) = q(x)r(x)$, as f is a function on $\mathbb{Z}[x]$, we have $f(a(x)) = f(q(x)r(x))$. As f is a homomorphism, that is equivalent to $f(a(x)) = f(q(x))f(r(x))$. Now, as p divides $a_0, a_1, \ldots, a_{m-1}$, we have $f(a(x)) = \overline{a_m} x^m$. From that we have $\overline{a_m} x^m = \left(\overline{q_{n(q(x))}} x^{n(q(x))} + \cdots + \overline{q_1} x + \overline{q_0}\right)\left(\overline{r_{n(r(x))}} x^{n(r(x))} + \cdots + \overline{r_1} x + \overline{r_0}\right)$. It is obvious that $\overline{q_{n(q(x))}} \cdot \overline{r_{n(r(x))}} = \overline{a_m}$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, then $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain and it has to be that $\overline{q_{n(q(x))}}, \overline{r_{n(r(x))}} \neq 0$. But, also $\overline{0} = \overline{q_0} \cdot \overline{r_0}$ implies that $\overline{q_0} = 0$ or $\overline{r_0} = 0$. Assume that $\overline{q_0} = 0$. Let $n = \min\{i \in \{1, \ldots, n(q(x))\} : p \nmid q_i\}$. If $n > n(r(x))$, then we can assume $\overline{r_j} = \overline{0}$ for all $j \in \{n(r(x)), \ldots, n\}$. We have $\overline{a_n} = \sum_{i+j=n} \overline{q_i r_j} = \overline{q_0 r_n} + \overline{q_1 r_{n-1}} + \cdots + \overline{q_{n-1} r_1} + \overline{q_n r_0}$. But, by assumption all q_i such that $0 < i < n$ are divisible by p so they are equal to $\overline{0}$ and we only have $\overline{a_n} = \overline{q_n r_0}$. Also, $\overline{a_n} = 0$, as it is divisible by p (we of course assumed that $q(x)$ and $p(x)$ are non-constant so it cannot be that $n = m$) and we have $\overline{0} = \overline{q_n r_0}$. But, as $(\mathbb{Z}/p\mathbb{Z})[x]$ is an integral domain we have either $\overline{q_n} = \overline{0}$ or $\overline{r_0} = \overline{0}$. If $\overline{q_n} = \overline{0}$, then it is a contradiction to well-ordering property because we assumed that n is a minimal index such that $p \nmid q_n$ (and $\overline{q_n} = \overline{0}$ implies $p | q_n$). The only thing we are left with is $\overline{r_0} = \overline{0}$, so $p | r_0$. But, we also assumed that $p | q_0$ (from $\overline{q_0} = \overline{0}$) and that would mean that $r_0 = p r_0'$ and $q_0 = p q_0'$. Then, $a_0 = r_0 q_0 = p r_0' p q_0' = p^2 r_0' q_0'$, which is a contradiction to $p^2 \nmid a_0$. Therefore, it must be that $a(x)$ is irreducible over $\mathbb{Q}$.

□

Proposition. Let F be a field, $p(x) \in F[x]$ and $c \in F$. Then, $\deg p(x) = \deg p(x - c)$.

Proof. Let $m \in \mathbb{Z}^+$, $\deg p(x) = m$ and $p(x) = p_m x^m + \cdots + p_1 x + p_0$. Then, $p(x - c) = p_m (x - c)^m + \cdots + p_1 (x - c) + p_0$. By binomial formula, the largest power of $(x - c)^m$ is x^m, so the largest power in $p(x - c)$ is again $p_m x^m$.

□

Proposition. Let F be a field, $p(x) \in F[x]$ and $c \in F$. If $p(x - c)$ is irreducible over F, then $p(x)$ is irreducible over F.

Proof. Assume that $p(x - c)$ is irreducible over F, but that $p(x)$ is not irreducible over F, i.e. there exist $q(x), r(x) \in F[x]$ such that $p(x) = q(x)r(x)$ with $\deg q(x), \deg r(x) \neq 0$. Then, $p(x - c) = q(x - c)r(x - c)$, but by previous proposition $\deg q(x - c) = \deg q(x) \neq 0$ and $\deg r(x - c) = \deg r(x) \neq 0$ meaning that $p(x - c)$ is not irreducible, a contradiction. Therefore, $p(x)$ is also irreducible.

□

Definition. A polynomial of the form $\frac{x^m-1}{x-1}$, where $m \in \mathbb{Z}^+$, is called **cyclotomic polynomial**.

Proposition. Let $p(x) = x^m - 1$, where $m \in \mathbb{Z}^+$. Then, $x - 1 | x^m - 1$, for all $m \in \mathbb{Z}^+$ and $\frac{x^m-1}{x-1} = x^{m-1} + \cdots + x + 1$.

Proof. Let $m = 1$. Then, $x - 1 | x - 1$. Assume the statement is true for m. Then, $x^{m+1} - 1 = x^m x - 1 + x - x = x(x^m - 1) + (x - 1)$. As $(x - 1)|(x^m - 1)$, there exist $q(x) \in \mathbb{Q}[x]$ such that $x^m - 1 = q(x)(x - 1)$. So we have $x^{m+1} - 1 = xq(x)(x - 1) + (x - 1) = (x - 1)(xq(x) + 1)$, i.e. $(x - 1)|x^{m+1}$, therefore the statement is true for all $m \in \mathbb{Z}^+$. Let $m = 1$. Then, $\frac{x-1}{x-1} = 1$. Assume the statement is true for some $m \in \mathbb{Z}^+$. Then, $\frac{x^{m+1}-1}{x-1} = \frac{x^m x-1+x-x}{x-1} = \frac{x(x^m-1)+x-1}{x-1} = \frac{x(x^m-1)}{x-1} + \frac{x-1}{x-1} = x(x^{m-1}+\cdots+x+1)+1 = x^m + \cdots + x + 1$, so the statement is true for all $m \in \mathbb{Z}^+$.

□

Proposition. Let $p \in P$. Then, $x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.

Proof. From previous proposition, $x^{p-1} + \cdots + x + 1 = \frac{x^p-1}{x-1}$. Let $q(x) = \frac{x^p-1}{x-1}$. Then, $q(x + 1) = \frac{(x+1)^p-1}{(x+1)-1}$. That is equivalent to:

$$\begin{aligned} q(x+1) &= \frac{\left(\binom{p}{p}x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{1}x + \binom{p}{0}\right) - 1}{x} \\ &= \frac{x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{1}x + 1 - 1}{x} = \frac{x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{1}x}{x} \\ &= x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1} = x^{p-1} + px^{p-2} + \cdots + \binom{p}{2}x + p. \end{aligned}$$

From a previous proposition, we know that $p|\binom{p}{k}$, for all $0 < k < p$. Therefore, as $p \nmid 1$ (the leading coefficient), as $p|\binom{p}{k}$, where $0 < k < p$, which are coefficients of x^k, and as $p|p$, but $p^2 \nmid p$ (the constant term of $q(x + 1)$), we can apply Eisenstein's criterion and conclude that $q(x + 1)$ is irreducible over $\mathbb{Q}$. From the previous proposition, we conclude that, as $q(x+1)$ is irreducible over $\mathbb{Q}$, then $q(x) = \frac{x^p-1}{x-1}$ is irreducible over $\mathbb{Q}$.

□

Proposition. If a polynomial $p(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$.

Proof. Assume that there exist $q(x), r(x) \in \mathbb{Q}[x]$ such that $p(x) = q(x)r(x)$. Then, by

previous corollary, as $p(x) \in \mathbb{Z}[x]$ and $q(x), r(x) \in \mathbb{Q}[x]$, there exist $q_1(x), r_1(x) \in \mathbb{Z}[x]$ such that $p(x) = q_1(x)r_1(x)$. But, that would mean that $p(x)$ is not irreducible, which is a contradiction.

□

Remark. For the following problems we will deal with $\mathbb{Z}/7\mathbb{Z}$ field, so we will write out the addition and multiplication table (the squares are bold):

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{\mathbf{0}}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{\mathbf{1}}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{\mathbf{4}}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{\mathbf{2}}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{\mathbf{2}}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{\mathbf{4}}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{\mathbf{1}}$

Problem. Find all the roots of the following polynomials in $\mathbb{Z}/7\mathbb{Z}[x]$, and factor the polynomials: (a) $x^3 + x^2 + x + \overline{1}$; (b) $\overline{3}x^4 + x^2 + \overline{1}$; (c) $x^5 + \overline{1}$; (d) $x^4 + \overline{1}$; (e) $x^4 + \overline{4}$.

Solution. First, we will note that all squares in $\mathbb{Z}/7\mathbb{Z}$ are $\overline{0}$, $\overline{1}$, $\overline{2}$ and $\overline{4}\}$. That is easily checked by $\overline{1^2} = \overline{6^2} = \overline{1}$, $\overline{2^2} = \overline{5^2} = \overline{4}$ and $\overline{3^2} = \overline{4^2} = \overline{2}$. Also, $\overline{0^2} = \overline{0}$.

(a) We can group the factors to have $x^3 + x^2 + x + \overline{1} = x(x^2 + \overline{1}) + (x^2 + \overline{1}) = (x^2+\overline{1})(x+\overline{1})$. Therefore, one of the roots is $\overline{-1} = \overline{6}$. Now, we can easily see that $x^2+\overline{1}$ cannot be factored further because, by checking all the squares in $\mathbb{Z}/7\mathbb{Z}[x]$, $\overline{1} + \overline{1} = \overline{2}$, $\overline{2} + \overline{1} = \overline{3}$ and $\overline{4} + \overline{1} = \overline{5}$. Obviously, also, $\overline{0} + \overline{1} = \overline{1}$. As $x^2 + \overline{1}$ can only be factored as two polynomials of degree one, if it doesn't have a root, it is irreducible. Therefore, $x^3 + x^2 + x + \overline{1} = (x^2 + \overline{1})(x - \overline{6})$.

(b) We have $p(x) = \overline{3}x^4+x^2+\overline{1}$. To see if the polynomial is divisible by $x-\overline{a}$, where $\overline{a} \in \mathbb{Z}/7\mathbb{Z}$, and as we only have x^2 in $p(x)$, we can substitute the squares only. So, we can take $t = x^2$ and then have $p(t) = \overline{3}t^2 + t + \overline{1}$. Now, we can only have $t \to \overline{0}, \overline{1}, \overline{2}, \overline{4}$. So, $\overline{0}$ is obviously not a root, then $p(\overline{1}) = \overline{3} + \overline{2} = \overline{5}$, $p(\overline{2}) = \overline{34} + \overline{3} = \overline{15} = \overline{1}$ and $p(\overline{4}) = \overline{32} + \overline{5} = \overline{11} = \overline{4}$. So, $\overline{3}t^2 + t + \overline{1}$ cannot be expressed as a product of two polynomials of degree one, and so cannot $\overline{3}x^4 + x^2 + \overline{1}$, as the only difference is in replacing t in the factorisation with x^2. From this is also obvious that $p(x)$ is then not divisible by any $x - \overline{a}$.

(c) It is obvious that $\overline{-1}^5 + \overline{1} = \overline{-1} + \overline{1} = \overline{0}$, so $x + \overline{1} | x^5 + \overline{1}$. Also, note that $x + \overline{1} = x - \overline{6}$. We have:

$$
\begin{array}{ll}
 & (x^5+\overline{1}) : (x-\overline{6}) = x^4+\overline{6}x^3+x^2+\overline{6}x+\overline{1} \\
- & \underline{(x^5-\overline{6}x^4)} \\
 & \overline{6}x^4+\overline{1} \\
- & \underline{(\overline{6}x^4-x^3)} \\
 & x^3+\overline{1} \\
- & \underline{(x^3-\overline{6}x^2)} \\
 & \overline{6}x^2+\overline{1} \\
- & \underline{(\overline{6}x^2-x)} \\
 & x+\overline{1} \\
- & \underline{(x-\overline{6})} \\
 & \overline{0}
\end{array}
$$

Thus, $x^5+\overline{1} = (x-\overline{6})(x^4+\overline{6}x^3+x^2+\overline{6}x+\overline{1})$. Now, $x^4+\overline{6}x^3+x^2+\overline{6}x+\overline{1} = x^4-x^3+x^2-x+\overline{1} = x^2(x^2+1)-x(x^2+\overline{1})+\overline{1} = (x^2+\overline{1})(x^2-x)+\overline{1} = x(x^2+\overline{1})(x-\overline{1})+\overline{1}$. Obviously, $\overline{0}$ and $\overline{1}$ are not roots. Now, $\overline{2}\cdot\overline{5}\cdot\overline{1}+\overline{1} = \overline{11}$, so $\overline{2}$ is not a root. Furthermore, $\overline{3}\cdot\overline{10}\cdot\overline{2}+\overline{1} = \overline{5}$, so $\overline{3}$ is not a root. Also, $\overline{4}\cdot\overline{17}\cdot\overline{3}+\overline{1} = \overline{5}\cdot\overline{3}+\overline{1} = \overline{15}+\overline{1} = \overline{2}$, so $\overline{4}$ is not a root. Then, for $\overline{5} = \overline{-2}$, we have $-\overline{2}\cdot\overline{5}\cdot\overline{-3}+\overline{1} = \overline{31} = \overline{3}$, so $\overline{5}$ is not a root. Finally, $\overline{6} = \overline{-1}$ gives us $-\overline{1}\cdot\overline{2}\cdot\overline{-2}+\overline{1} = \overline{5}$, so $\overline{6}$ is not a root. Thus, $x^4-x^3+x^2-x+\overline{1}$ is not divisible by any $x-\overline{a}$, where $\overline{a}\in\mathbb{Z}/7\mathbb{Z}$. Thus, for factorization, we need only check if we can write $x^4-x^3+x^2-x+\overline{1} = (x^2+\overline{a_1}x+\overline{a_0})(x^2+\overline{b_1}x+\overline{b_0})$, but that is a lot of work which we will leave for later.

(d) Let us observe $x^4+\overline{1}$. It is obvious that $x^4+\overline{1} = (x^2)^2+\overline{1}$ has no roots as $\overline{0}^2+\overline{1} = \overline{1}$, $\overline{1}^2+\overline{1} = \overline{2}$, $\overline{2}^2+\overline{1} = \overline{5}$ and $\overline{4}^2+\overline{1} = \overline{17} = \overline{3}$.

(e) Similarly, $x^6+\overline{1} = (x^2)^3+\overline{1}$ has no roots. We have $\overline{0}^3+\overline{1} = \overline{1}$, $\overline{1}^3+\overline{1} = \overline{2}$, $\overline{2}^3+\overline{1} = \overline{9} = \overline{2}$ and $\overline{4}^3+\overline{1} = \overline{65} = \overline{2}$.

Problem. Use Fermat's theorem to find all the roots of the following polynomials in $\mathbb{Z}/7\mathbb{Z}[x]$: (a) $x^{100}-\overline{1}$; (b) $\overline{3}x^{98}+x^{19}+\overline{3}$; (c) $\overline{2}x^{74}-x^{55}+\overline{2}x+\overline{6}$.

Solution. (a) We know that $\overline{a}^6 = \overline{1}$, for all $\overline{a}\in\mathbb{Z}/7\mathbb{Z}-\{\overline{0}\}$. We have $100 = 6\cdot 16+4$, so $(\overline{a}^6)^{16} = \overline{1}$. So we are looking for $\overline{a}$ which satisfies $\overline{a}^{96}\cdot\overline{a}^4 = \overline{1}$, i.e. $\overline{a}^4 = \overline{1}$. From that we have $(\overline{a}^2)^2 = \overline{1}$. So, obviously we have $\overline{1}^2 = \overline{1}$. Then, $\overline{2}^2 = \overline{4}$, $\overline{4}^2 = \overline{2}$. Thus, it is only possible that $\overline{a}\in\{\overline{1},\overline{6}\}$, i.e. $x_1 = \overline{1}$ and $x_2 = \overline{6}$.

(b) We have $\overline{3}x^{98}+x^{19}+\overline{3} = \overline{3}\left(x^{98}+\overline{5}x^{19}+\overline{1}\right)$. If there exists a root $\overline{a}\in\mathbb{Z}/7\mathbb{Z}$, then $\overline{3}\left(\overline{a}^{98}+\overline{5}\cdot\overline{a}^{19}+\overline{1}\right) = \overline{0}$, and after multiplying that by $\overline{3}^{-1}$ we have $\overline{a}^{98}+\overline{5}\cdot\overline{a}^{19}+\overline{1} = \overline{0}$. We also know that $98 = 6\cdot 16+2$ and $19 = 6\cdot 3+1$. So, $\overline{a}^{98}+\overline{5}\cdot\overline{a}^{19}+\overline{1} = (\overline{a}^6)^{16}\,\overline{a}^2+$

$\overline{5}\cdot(\overline{a}^6)^3\,\overline{a}+\overline{1}$. By Fermat's theorem, $\overline{a}^6=\overline{1}$ and we have $(\overline{a}^6)^{16}\,\overline{a}^2+\overline{5}\cdot(\overline{a}^6)^3\,\overline{a}+\overline{1}=\overline{a}^2+\overline{5}\cdot\overline{a}+\overline{1}$. We have to find $\overline{a}\in\mathbb{Z}/7\mathbb{Z}$ such that $\overline{a}^2+\overline{5}\cdot\overline{a}+\overline{1}=\overline{0}$. Here we have $\overline{t}^2=(\overline{5}^2-\overline{4})\overline{4}^{-1}=\overline{21}\cdot\overline{2}=\overline{42}=\overline{0}$. Then, $\overline{t}=\overline{0}$ and we have $\overline{a}=\overline{0}-\overline{5}\cdot\overline{2}^{-1}=\overline{2}\cdot\overline{2}^{-1}=\overline{1}$. We see that $\overline{1}^2+\overline{5}\cdot\overline{1}+\overline{1}=\overline{7}=\overline{0}$. Furthermore, as $\overline{t}=\overline{0}$, this solution must be the only solution in $\mathbb{Z}/7\mathbb{Z}$, which we can check by $\left(\overline{a}-\overline{1}\right)^2=\overline{a}^2-\overline{2}\cdot\overline{a}+\overline{1}=\overline{a}^2+\overline{5}\cdot\overline{a}+\overline{1}$.

(c) Let us observe $\overline{2}x^{74}-x^{55}+\overline{2}x+\overline{6}=\overline{2}x^{74}+\overline{6}x^{55}+\overline{2}x+\overline{6}=\overline{2}\left(x^{74}+\overline{3}x^{55}+x+\overline{3}\right)$. It is sufficient to observe $x^{74}+\overline{3}x^{55}+x+\overline{3}$. If there exists a root $\overline{a}\in\mathbb{Z}/7\mathbb{Z}$, then it must be that $\overline{a}^{74}+\overline{3}\cdot\overline{a}^{55}+\overline{a}+\overline{3}=\overline{0}$. We find out that $74=12\cdot6+2$ and $55=9\cdot6+1$. So, by Fermat's theorem, we have $\overline{a}^6=\overline{1}$ and it follows that $\overline{a}^{74}+\overline{3}\cdot\overline{a}^{55}+\overline{a}+\overline{3}=(\overline{a}^6)^{12}\,\overline{a}^2+\overline{3}\,(\overline{a}^6)^9\,\overline{a}+\overline{a}+\overline{3}=\overline{a}^2+\overline{3}\cdot\overline{a}+\overline{a}+\overline{3}=\overline{a}^2+\overline{4}\cdot\overline{a}+\overline{3}$. We need to solve $\overline{a}^2+\overline{4}\cdot\overline{a}+\overline{3}=\overline{0}$. We have $\overline{t}^2=(\overline{16}-\overline{12})\overline{4}^{-1}=\overline{1}$. That implies that there are two possibilities, $\overline{t_1}=\overline{1}$ and $\overline{t_2}=\overline{6}$. We will calculate $\overline{s}=-\overline{4}\cdot\overline{2}^{-1}=-\overline{44}=-\overline{16}=\overline{5}$, so that $\overline{a_{1,2}}=\overline{t_{1,2}}+\overline{s}$. For $\overline{t_1}=\overline{1}$ we have $\overline{a_1}=\overline{1}+\overline{5}=\overline{6}$. For $\overline{t_2}=\overline{6}$, we have $\overline{a_2}=\overline{6}+\overline{5}=\overline{11}=\overline{4}$. That can be checked by $(\overline{a}-\overline{6})(\overline{a}-\overline{4})=\overline{a}^2-\overline{10}\cdot\overline{a}+\overline{24}=\overline{a}^2+\overline{4}\cdot\overline{a}+\overline{3}$. So, the only two solutions in $\mathbb{Z}/7\mathbb{Z}$ are $\overline{a_1}=\overline{6}$ and $\overline{a_2}=\overline{4}$.

Problem. Using Fermat's theorem, find polynomials of degree ≤ 6 which determine the same functions as the following polynomials in $\mathbb{Z}/7\mathbb{Z}[x]$: (a) $\overline{3}x^{75}-\overline{5}x^{54}+\overline{2}x^{13}-x^2$; (b) $\overline{4}x^{108}+\overline{6}x^{101}-\overline{2}x^{81}$; (c) $\overline{3}x^{103}-x^{73}+\overline{3}x^{55}-x^{25}$.

Solution. (a) Let $p(x)=\overline{3}x^{75}-\overline{5}x^{54}+\overline{2}x^{13}-x^2$. It is obvious that, for all $\overline{a}\in\mathbb{Z}/7\mathbb{Z}-\{\overline{0}\}$, we have $p(\overline{a})=\overline{3}\,(\overline{a}^6)^{12}\,\overline{a}^3-\overline{5}\,(\overline{a}^6)^9+\overline{2}\,(\overline{a}^6)^2\,\overline{a}-\overline{a}^2$. Now, using Fermat's theorem, we have $\overline{a}^6=\overline{1}$, for all $\overline{a}\in\mathbb{Z}/7\mathbb{Z}-\{\overline{0}\}$. So, $p(\overline{a})=\overline{3}\cdot\overline{a}^3-\overline{5}+\overline{2}\cdot\overline{a}-\overline{a}^2$, and that can be written more neatly as a new polynomial $q_1(x)=\overline{3}x^3+\overline{6}x^2+\overline{2}x+\overline{2}$. It is obvious that now, $p(\overline{a})=q_1(\overline{a})$, for all $\overline{a}\in\mathbb{Z}/7\mathbb{Z}-\{0\}$. But notice that $p(\overline{0})=\overline{0}$ and $q_1(\overline{0})=\overline{2}$. That can be fixed by defining a new polynomial $q(x)=\overline{2}x^6+\overline{3}x^3+\overline{6}x^2+\overline{2}x$. Now, $q(\overline{0})=\overline{0}$, and due to Fermat's theorem, function values for other elements remain the same.

(b) Let $p(x)=\overline{4}x^{108}+\overline{6}x^{101}-\overline{2}x^{81}$. Then, for all $\overline{a}\in\mathbb{Z}/7\mathbb{Z}[x]$ we have $p(\overline{a})=\overline{4}\,(\overline{a}^6)^{18}+\overline{6}\,(\overline{a}^6)^{96}\,\overline{a}^5-\overline{2}\,(\overline{a}^6)^{13}\,\overline{a}^3$. Using Fermat's theorem, and due to the need for $p(\overline{0})=q(\overline{0})$, as argued in the previos case, we will define new polynomial $q(x)=\overline{4}x^6+\overline{6}x^5+\overline{5}x^3$. It is easy to see that now $p(\overline{a})=q(\overline{a})$, for all $\overline{a}\in\mathbb{Z}/7\mathbb{Z}$.

(c) Let $p(x)=\overline{3}x^{103}-x^{73}+\overline{3}x^{55}-x^{25}$. Arguing as in the previos cases, we define $q(x)=\overline{3}x-x+\overline{3}x-x=\overline{6}x-\overline{2}x=\overline{4}x$. Now, due to Fermat's theorem, $p(\overline{a})=q(\overline{a})$, for all $\overline{a}\in\mathbb{Z}/7\mathbb{Z}$.

Remark. Notice that, due to Fermat's theorem, every polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$ has the same roots as a polynomial of degree $<p$, which can be obtained by dividing exponents of different terms with $p-1$ and disregarding x^{p-1}, thus leaving only the residue, whose degree is, due to the division with remainder theorem, less than $p-1$, and by that

less than p. Also, the only problem is the zero element for which we need to set the constant term to include x^{p-1}.

Problem. Find all the rational roots of the following polynomials, and factor them into irreducible polynomials in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$: (a) $9x^3 + 18x^2 - 4x - 8$; (b) $4x^3 - 3x^2 - 8x + 6$; (c) $2x^4 + 3x^3 - 8x - 12$; (d) $6x^4 - 7x^3 + 8x^2 - 7x + 2$.

Solution. (a) If there is a root $\frac{a}{b} \in \mathbb{Q}$, then $a \in \pm\{1, 2, 4, 8\}$ and $b \in \pm\{1, 3, 9\}$. So we don't search through all, we will just show (discovered by a lucky guess) that $9\left(\frac{2}{3}\right)^3 + 18\left(\frac{2}{3}\right)^2 - 4 \cdot \frac{2}{3} - 8 = 9 \cdot \frac{8}{27} + 18 \cdot \frac{4}{9} - \frac{8}{3} - 8 = \frac{8}{3} + 8 - \frac{8}{3} + 8 = 0$. So, we can divide $9x^3 + 18x^2 - 4x - 8$ by $x - \frac{2}{3}$:

$$
\begin{array}{ll}
 & (9x^3 + 18x^2 - 4x - 8) : \left(x - \dfrac{2}{3}\right) = 9x^2 + 24x + 12 \\
- & \underline{\left(9x^3 - 6x^2\right)} \\
 & 24x^2 - 4x - 8 \\
- & \underline{(24x^2 - 16x)} \\
 & 12x - 8 \\
- & \underline{(12x - 8)} \\
 & 0
\end{array}
$$

So, $9x^3 + 18x^2 - 4x - 8 = \left(x - \frac{2}{3}\right)(9x^2 + 24x + 12) = (3x - 2)(3x^2 + 8x + 4)$. From that we have $x_1 = \frac{2}{3}$ and:

$$x_{2,3} = \frac{-8 \pm \sqrt{64 - 48}}{6} = \frac{-8 \pm 4}{6}.$$

Therefore, $x_2 = -2$ and $x_3 = -\frac{2}{3}$. So, we can write $9x^3 + 18x^2 - 4x - 8 = (3x - 2) \cdot 3(x + 2)\left(x + \frac{2}{3}\right)$, i.e. $9x^3 + 18x^2 - 4x - 8 = (3x - 2)(3x + 2)(x + 2)$.

(b) We have $4x^3 - 3x^2 - 8x + 6$. We check for rational roots in $\frac{a}{b} \in \mathbb{Q}$ by searching through $a \in \pm\{1, 2, 3, 6\}$ and $b \in \pm\{1, 2, 4\}$. After some calculations we can see that $4\left(\frac{3}{4}\right)^3 - 3\left(\frac{3}{4}\right)^2 - 8 \cdot \frac{3}{4} + 6 = \frac{3^3}{4^2} - \frac{3^3}{4^2} - 6 + 6 = 0$. Now we use the division algorithm:

$$
\begin{array}{ll}
 & (4x^3 - 3x^2 - 8x + 6) : \left(x - \dfrac{3}{4}\right) = 4x^2 - 8 \\
- & \underline{(4x^3 - 3x^2)} \\
 & -8x + 6 \\
- & \underline{(-8x + 6)} \\
 & 0
\end{array}
$$

Thus, $4x^3-3x^2-8x+6=\left(x-\frac{3}{4}\right)(4x^2-8)=4\left(x-\frac{3}{4}\right)(x^2-2)=(4x-2)(x^2-2)$. Polynomial x^2-2 does not split over $\mathbb{Q}$, as there does not exist a rational number such that $x^2=2$. But we know that $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$, so $4x^3-3x^2-8x+6=(4x-2)(x-\sqrt{2})(x+\sqrt{2})$ over $\mathbb{R}$. The three solutions, therefore, are $x_1=\frac{3}{4}$, $x_2=\sqrt{2}$ and $x_3=-\sqrt{2}$.

(c) For rational roots $\frac{a}{b}\in\mathbb{Q}$ of $2x^4+3x^3-8x-12$ we search in $a\in\pm\{1,2,3,4,6,12\}$ and $b\in\pm\{1,2\}$. It is easy to see that 1 and -1 are not roots, so we search roots that are not integers and see that $2\left(-\frac{3}{2}\right)^4+3\left(-\frac{3}{2}\right)^3+8\cdot\frac{3}{2}-12=\frac{3^4}{2^3}-\frac{3^4}{2^3}+12-12=0$. By usind division algorithm,

$$\begin{array}{ll} & (2x^4+3x^3-8x-12):\left(x+\dfrac{3}{2}\right)=2x^3-8 \\ - & \underline{(2x^4+3x^3)} \\ & -8x-12 \\ - & \underline{(-8x-12)} \\ & 0 \end{array}$$

So, $x_1=\frac{3}{2}$ and $2x^4+3x^3-8x-12=(2x^3-8)\left(x+\frac{3}{2}\right)=(x^3-4)(2x+3)$. The polynomial cannot split any further in $\mathbb{Q}[x]$. Now we solve $x^3-4=0$, i.e. $x^3=4$. That means that at least one of the roots is $x_2=\sqrt[3]{4}$. Using the division algorithm again we have:

$$\begin{array}{ll} & \left(x^3-4\right):\left(x-\sqrt[3]{4}\right)=x^2+x\sqrt[3]{4}+2\sqrt[3]{2} \\ - & \underline{\left(x^3-x^2\sqrt[3]{4}\right)} \\ & x^2\sqrt[3]{4}-4 \\ - & \underline{\left(x^2\sqrt[3]{4}-2x\sqrt[3]{2}\right)} \\ & 2x\sqrt[3]{2}-4 \\ - & \underline{\left(2x\sqrt[3]{2}-4\right)} \\ & 0 \end{array}$$

Thus, over $\mathbb{R}$, we have $2x^4+3x^3-8x-12=(2x+3)\left(x-\sqrt[3]{4}\right)(x^2+x\sqrt[3]{4}+2\sqrt[3]{2})$. Using the quadratic equation formula:

$$x_{3,4}=\frac{-\sqrt[3]{4}\pm\sqrt{2\sqrt[3]{2}-8\sqrt[3]{2}}}{2}=-\frac{\sqrt[3]{4}}{2}\pm i\frac{\sqrt{6\sqrt[3]{2}}}{2}.$$

That can be elaborated further:

$$x_{3,4} = -\sqrt[3]{\frac{4}{8}} \pm i\frac{\sqrt{3\sqrt[3]{16}}}{2} = -\sqrt[3]{\frac{1}{2}} \pm i\sqrt{3}\sqrt[6]{\frac{2^4}{2^6}}.$$

Finally,

$$x_{3,4} = -\sqrt[3]{\frac{1}{2}} \pm i\sqrt[6]{\frac{27}{4}}$$

Therefore, the polynomial splits over $\mathbb{C}$ as:

$$2x^4 + 3x^3 - 8x - 12 = (2x+3)\left(x - \sqrt[3]{4}\right)\left(x + \sqrt[3]{\frac{1}{2}} + i\sqrt[6]{\frac{27}{4}}\right)\left(x + \sqrt[3]{\frac{1}{2}} - i\sqrt[6]{\frac{27}{4}}\right).$$

(d) We need to find roots of $6x^4 - 7x^3 + 8x^2 - 7x + 2$. We look for rational roots $\frac{a}{b} \in \mathbb{Q}$ by looking at $a \in \pm\{1,2\}$ and $b \in \pm\{1,2,3,6\}$. We can easily eliminate 1 and -1 in the beginning by looking at the sum $6 - 7 + 8 - 7 + 2 = 2$ for 1 and $6+7+8+7+2 = 30$ for -1. By going through all possibilities, i.e. $\pm 2, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{1}{6}$ (we already eliminated 1 and -1), or by a lucky guess (as in the author's case), we see that $6\left(\frac{2}{3}\right)^4 - 7\left(\frac{2}{3}\right)^3 + 8\left(\frac{2}{3}\right)^2 - 7\cdot\frac{2}{3} + 2 = 2\cdot 3\cdot\frac{2^4}{3^4} - 7\cdot\frac{2^3}{3^3} + 2^3\cdot\frac{2^2}{3^2} - \frac{2\cdot 7}{3} + \frac{2\cdot 3}{3} = \frac{2^5}{3^3} - \frac{7\cdot 2^3}{3^3} + \frac{3\cdot 2^5}{3^3} - \frac{2\cdot 7\cdot 3^2}{3^3} + \frac{2\cdot 3^3}{3^3} = \frac{2^5 - 7\cdot 2^3 + 3\cdot 2^5 - 2\cdot 7\cdot 3^2 + 2\cdot 3^3}{3^3} = \frac{2^3(4-7+12) + 3^2(6-14)}{3^3} = \frac{2^3\cdot 9 + 3^2\cdot(-8)}{3^3} = \frac{8\cdot 9 - 9\cdot 8}{3^3} = \frac{0}{3^3} = 0$. We use division algorithm like so:

$$\begin{array}{ll} & (6x^4 - 7x^3 + 8x^2 - 7x + 2) : \left(x - \frac{2}{3}\right) = 6x^3 - 3x^2 + 6x - 3 \\ - & \underline{(6x^4 - 4x^3)} \\ & -3x^3 + 8x^2 - 7x + 2 \\ - & \underline{(-3x^3 + 2x^2)} \\ & 6x^2 - 7x + 2 \\ - & \underline{(6x^2 - 4x)} \\ & -3x + 2 \\ - & \underline{-3x + 2} \\ & 0 \end{array}$$

Thus we have $6x^4 - 7x^3 + 8x^2 - 7x + 2 = \left(x - \frac{2}{3}\right)(6x^3 - 3x^2 + 6x - 3) = (3x-2)(2x^3 - x^2 + 2x - 1)$. To factor $2x^3 - x^2 + 2x - 1$ we look for rational roots $\frac{a}{b} \in \mathbb{Q}$ such that $a \in \{1, -1\}$ and $b \in \pm\{1,2\}$. At a glance we see that we can eliminate 1 and -1. So,

we are left with $\pm\frac{1}{2}$ and see that $2\left(\frac{1}{2}\right)^3-\left(\frac{1}{2}\right)^2+2\cdot\frac{1}{2}-1=2\cdot\frac{1}{2^3}-\frac{1}{2^2}+1-1=\frac{1}{2^2}-\frac{1}{2^2}=0$. So, we use the division algorithm once more:

$$\begin{array}{rl} & (2x^3-x^2+2x-1):\left(x-\dfrac{1}{2}\right)=2x^2+2 \\ - & \underline{(2x^3-x^2)} \\ & (2x-1) \\ - & \underline{(2x-1)} \\ & 0 \end{array}$$

So, $6x^4-7x^3+8x^2-7x+2=(3x-2)(2x^3-x^2+2x-1)=(3x-2)(2x^2+2)\left(x-\frac{1}{2}\right)$, i.e. $6x^4-7x^3+8x^2-7x+2=(3x-2)(2x-1)(x^2+1)$ over $\mathbb{Q}$. Now, x^2+1 cannot be factored over $\mathbb{R}$, but it can be factored over $\mathbb{C}$ as $x^2+1=(x-i)(x+i)=x^2-i^2=x^2+1$. Therefore, the roots are $x_1=\frac{2}{3}$, $x_2=\frac{1}{2}$, $x_{3,4}=\pm i$ and we have $6x^4-7x^3+8x^2-7x+2=(3x-2)(2x-1)(x-i)(x+i)$.

Problem. Find associates with integer coefficients and rational roots for each of the following polynomials: (a) $x^3+\frac{3}{2}x^2-\frac{4}{9}x-\frac{2}{3}$; (b) $\frac{1}{2}x^3-\frac{1}{4}x^2-\frac{1}{2}x+\frac{1}{4}$; (c) $x^3\sqrt{3}+\frac{1}{\sqrt{3}}x^2-x\sqrt{3}-\frac{1}{\sqrt{3}}$. Then, factor them over $\mathbb{R}$.

Solution. (a) We have $18\left(x^3+\frac{3}{2}x^2-\frac{4}{9}x-\frac{2}{3}\right)=18x^3+27x^2-8x-12$. For rational roots of the form $\frac{a}{b}\in\mathbb{Q}$ we look in $a\in\pm\{1,2,3,4,6,12\}$ and $b\in\pm\{1,2,3,4,6,9,18\}$. Well, how did the author get to the first root? Let us denote $p(x)=18x^3+27x^2-8x-12$. We calculated $p(1)$ and got $p(1)=25$. Then we calculated $p\left(\frac{1}{6}\right)=-\frac{25}{2}$. As the change of sign happened, our root has to be somewhere between 1 and $\frac{1}{6}$. That includes $\frac{2}{6}=\frac{1}{3}$, $\frac{3}{6}=\frac{1}{2}$, $\frac{4}{6}=\frac{2}{3}$ and $\frac{5}{6}$. For $\frac{1}{3}$ we have $p\left(\frac{1}{3}\right)=-11$, so actually, we got closer to our root, or so we may assume (if the values of the polynomial don't fluctuate too much), so looking further we get $p\left(\frac{1}{2}\right)=-7$. For the next one, $p\left(\frac{2}{3}\right)=0$, and that's our root! Also, our assumption that we were getting closer to the root was correct (by what ways, we may only wonder, but later we will see that actually we were just sliding down the polynomial; it will turn out it has two more rational roots, but below zero, a place we never even touched). We use the division algorithm now (notice that due to Gauss' lemma we could divide the polynomial by $3x-2$ instead of $x-\frac{2}{3}$):

$$
\begin{array}{ll}
 & (18x^3+27x^2-8x-12):(3x-2)=6x^2+13x+6 \\
- & \underline{(18x^3-12x^2)} \\
 & 39x^2-8x-12 \\
- & \underline{(39x^2-26x)} \\
 & 18x-12 \\
- & \underline{(18x-12)} \\
 & 0
\end{array}
$$

So, $18x^3+27x^2-8x-12=(3x-2)\,(6x^2+13x+6)$. By using the formula for the quadratic equation we obtain:

$$x_{2,3}=\frac{-13\pm\sqrt{169-144}}{12}=\frac{-13\pm 5}{12}.$$

From that we have $x_2=-\frac{2}{3}$ and $x_3=-\frac{3}{2}$ (and our poor old root $x_1=\frac{2}{3}$). Thus, $18x^3+27x^2-8x-12=(3x-2)\cdot 6\left(x+\frac{3}{2}\right)\left(x+\frac{2}{3}\right)$. By using Gauss' lema we can simplify that from $18x^3+27x^2-8x-12=(3x-2)\cdot 6\cdot\frac{1}{2}\,(2x+3)\cdot\frac{1}{3}\,(3x+2)$ to:

$$18x^3+27x^2-8x-12=6(3x-2)(2x+3)(3x+2).$$

Of course, the factorization of the original polynomial is:

$$x^3+\frac{3}{2}x^2-\frac{4}{9}x-\frac{2}{3}=\frac{1}{3}(3x-2)(2x+3)(3x+2).$$

(b) We can take the associate $4\left(\frac{1}{2}x^3-\frac{1}{4}x^2-\frac{1}{2}x+\frac{1}{4}\right)=2x^3-x^2-2x+1$. Now, we can easily factor that as $2x^3-x^2-2x+1=(2x^3-2x)-(x^2-1)=2x(x^2-1)-(x^2-1)=(x^2-1)(2x-1)=(x-1)(x+1)(2x-1)$, so our roots are $x_1=\frac{1}{2}$ and $x_{2,3}=\pm 1$. Also, the factorization of the original polynomial is:

$$\frac{1}{2}x^3-\frac{1}{4}x^2-\frac{1}{2}x+\frac{1}{4}=\frac{1}{4}(x-1)(x+1)(2x-1).$$

(c) We have $\sqrt{3}\left(x^3\sqrt{3}+\frac{1}{\sqrt{3}}x^2-x\sqrt{3}-\frac{1}{\sqrt{3}}\right)=3x^3+x^2-3x-1$. Again, this polynomial can be easily factored as $3x^3+x^2-3x-1=(3x^3-3x)+(x^2-1)=3x(x^2-1)+(x^2-1)=(x^2-1)(3x+1)=(x+1)(x-1)(3x+1)$. So the roots are $x_1=-\frac{1}{3}$ and $x_{2,3}=\pm 1$. The factorization of the original is:

$$x^3\sqrt{3}+\frac{1}{\sqrt{3}}x^2-x\sqrt{3}-\frac{1}{\sqrt{3}}=\frac{1}{\sqrt{3}}(x+1)(x-1)(3x+1).$$

Problem. Does $2x^4 + 3x^2 - 2$ have any rational roots? Can it be factored into two polynomials of lower degree in $\mathbb{Q}[x]$?

Solution. We look for rational roots $\frac{a}{b} \in \mathbb{Q}$ by looking at $a \in \pm\{1, 2\}$ and $b \in \pm\{1, 2\}$. Thus, we will check all the roots, noting that their signs don't change the value, as all the exponents of the terms in the polynomial are even: $p(-2) = p(2) = 42$, $p(-1) = p(1) = 3$, $p\left(-\frac{1}{2}\right) = p\left(\frac{1}{2}\right) = -\frac{9}{8}$. Therefore, there are no rational roots. But, taking $t = x^2$, we can try to solve $2t^2 + 3t - 2 = 0$. By quadratic formula we have:

$$t_{1,2} = \frac{-3 \pm \sqrt{9 + 16}}{4} = \frac{-3 \pm 5}{4}.$$

So, we have $t_1 = -2$ and $t_2 = \frac{1}{2}$ and that implies $2t^2 + 3t - 2 = 2(t + 2)\left(t - \frac{1}{2}\right) = (t + 2)(2t - 1)$. Now, taking the substitution back, we have:

$$2x^4 + 3x^2 - 2 = (x^2 + 2)(2x^2 - 1).$$

Thus, the polynomial can be factored into two polynomials of lower degree over $\mathbb{Q}$, but it has no rational roots (a nice counterexample for the theorem).

Proposition. Let F be a field, $c \in F$ and $p(x) \in F[x]$. Then,

1. The remainder of $p(x)$, when divides by $x - c$, is $p(c)$;
2. $x - c | p(x) - p(c)$.

Proof. *Ad* 1. Let $p(x) \in F[x]$. By division with remainder theorem, there exist $q(x), r(x) \in F[x]$ such that $p(x) = q(x)(x-c)+r(x)$, where $0 \leq \deg r(x) < \deg(x - c)$. But, $\deg(x - c) = 1$, so $r(x) = a$, where $a \in F$. That implies $p(x) = q(x)(x - c) + a$. Now, $p(c) = q(c)(c-c)+a$, i.e. $p(c) = 0+a$. Indeed, $p(c) = a$, which is the remainder.

Ad 2. Let $p(x) \in F[x]$ and $c \in F$. Then, there exist $q(x), r(x) \in F[x]$ such that $p(x) - p(c) = q(x)(x - c) + r(x)$, where $0 \leq \deg r(x) < \deg(x - c) = 1$, which implies $r(x) = a$, for some $a \in F$. By taking $x = c$ we have $p(c) - p(c) = q(c)(c - c) + a$ and that means $0 = 0 + a$, i.e. $a = 0$. From that we have $r(x) = 0$ meaning that $x - c | p(x) - p(c)$.

□

Proposition. Every polynomial over some field F has the same roots as any of its associates.

Proof. Let F be a field, $a \in F$ and $p(x), q(x) \in F[x]$ such that $p(x) = aq(x)$. If $c \in F$ is a root of $p(x)$, then $p(c) = 0$. That implies $p(c) = aq(c)$, i.e. $0 = aq(c)$. By multiplying the equality with $a^{-1} \in F$, we have $0 = q(c)$, meaning that c is also a root of $q(x)$.

□

Problem. If $a(x), b(x) \in F[x]$ have the same roots in a field F, are they necessarily associates?

Solution. For example, $(x-3)(x^2+1)$ and $(x-3)(2x^2+1)$ have the same roots in $\mathbb{R}$ (that is $x_1 = 3$), but they are not associates.

Proposition. Let F be a field. If $a(x) \in F[x]$ is a monic polynomial of degree $m \in \mathbb{Z}^+$, and $a(x)$ has m distinct roots $c_1, \ldots, c_m \in F$, then $a(x) = (x - c_1) \cdots (x - c_m)$.

Proof. Let $m = 1$. Then, $a(x)$ is of degree 1 and has 1 root c_1. As $a(x)$ is of degree 1, it is of the form $a(x) = x + a_0$ (by assumption monic). As $c_1 \in F$ is a root, then $x - c_1$ divides $x + a_0$, i.e. there exists $q(x) \in F[x]$ such that $x + a_0 = (x - c_1)q(x)$. As $1 = \deg(x + a_0) = \deg((x - c_1)q(x)) = \deg(x - c_1) + \deg q(x) = 1 + \deg q(x)$, it must be that $\deg q(x) = 0$, i.e. $q(x) = q_0$, for some $q_0 \in F$. Thus, $x + a_0 = q_0 x - q_0 c_1$. But, that implies $q_0 = 1$, i.e. $a(x) = x - c_1$. Assume that the statement holds for all monic polynomials of degree $m \in \mathbb{Z}^+$ with m roots. Let $a(x)$ be a monic polynomial of $(m+1)$-st degree with roots $c_1, \ldots, c_{m+1}$. Then, $x - c_{m+1} | a(x)$ and we have $a(x) = q(x)(x - c_{m+1})$. That implies that $q(x)$ is monic (as $a(x)$ is monic and $x - c_{m+1}$ is monic). As $x - c_{m+1} \neq x - c_i$, for all $i \in \{1, \ldots, m\}$ and as $x - c_i | a(x)$, it must be that $x - c_i | q(x)$. As $q(x)$ is of m-th degree and is divisible by m polynomials of the form $x - c_i$, it has m roots $c_1, \ldots, c_m$, so by assumption $q(x) = (x - c_1) \cdots (x - c_m)$. That implies $a(x) = (x - c_1) \cdots (x - c_{m+1})$.

□

Proposition. Let F be a field. Assume $a(x), b(x) \in F[x]$ have degree $< m$, for some $m \in \mathbb{Z}^+ - \{1\}$. If $a(c_i) = b(c_i)$ for all $c_1, \ldots, c_m \in F$ (all distinct), then $a(x) = b(x)$.

Proof. Let $p(x) = a(x) - b(x)$. Then, if $a(x) \neq b(x)$, we have $0 \leq \deg p(x) \leq \max\{\deg a(x), \deg b(x)\} = n < m$. But, $p(c_i) = a(c_i) - b(c_i) = 0$, so $x - c_i | p(x)$, for all $i \in \{1, \ldots, m\}$. Thus, we have $(x - c_1) \ldots (x - c_m) q(x) = p(x)$. But, on the left hand side we have degree of at least m and on the right hand side n, i.e. $m + k = n$, i.e. $m \leq n$. That is in contradiction with $n < m$ so it must be $a(x) = b(x)$. Thus, $\deg p(x)$ is undefined and $p(x) = 0$. Also, $x - c_i | 0$, for all $c_i \in F$, where $i \in \{1, \ldots, m\}$.

□

Proposition. There are infinitely many irreducible polynomials over any field F.

Proof. Let $I \subseteq F[x]$ such that $p(x) \in I$ if and only if $p(x)$ is irreducible. That means that $a_1x + a_0 \in I$, for all $a_1, a_0 \in F - \{0\}$, by definition. So, if F is infinite, then I is certainly infinite. But if F is finite, then the number of $a_1x + a_0 \in I$ is finite. So, let us assume that I itself is finite, i.e. $I = \{p_1(x), \ldots, p_m(x)\}$, where $m \in \mathbb{Z}^+$. Take $q(x) = p_1(x) \cdots p_m(x) + 1$. As $F[x]$ is a unique factorization domain, $q(x)$ can be written down as a product of irreducible polynomials, i.e. it is divisible by at least one irreducible polynomial. Then, as I contains all irreducible polynomials, $q(x)$ is either one of them, or divisible by one of them (both cases come down to the latter). So, assume, without loss of generalty, $p_1(x)|q(x)$. We have $q(x) = p_1(x)r(x)$, where $r(x) \in F[x]$. So, $p_1(x)r(x) = p_1(x) \cdots p_m + 1$. Then, $p_1(x)(r(x) - p_2(x) \cdots p_m(x)) = 1$, but that is impossible as $p_1(x)$ would divide 1. So, there has to be some irreducible polynomial outside of I that divides $q(x)$ (or is $q(x)$ itself). The process can be repeated infinitely, meaning that I is infinite.

□

Problem. How many roots does $x^2 - x$ have in $\mathbb{Z}/10\mathbb{Z}$? In $\mathbb{Z}/11\mathbb{Z}$?

Solution. In $\mathbb{Z}/10\mathbb{Z}$, $x^2 - x$ has four roots: $\overline{0}^2 - \overline{0} = \overline{0}$, $\overline{1}^2 - \overline{1} = \overline{0}$, $\overline{5}^2 - \overline{5} = \overline{20} = \overline{0}$ and $\overline{6}^2 - \overline{6} = \overline{30} = \overline{0}$. In $\mathbb{Z}/11\mathbb{Z}$, it has two roots, $\overline{0}$ and $\overline{1}$. That happens because $\mathbb{Z}/10\mathbb{Z}$ is not a field (and the theorem that states that polynomial of degree m has at most m roots depends on the division alorithm for polynomials, which in turn can be proved only over a field).

□

Problem. Show that each of the following polynomials is irreducible over $\mathbb{Q}$: (a) $3x^4 - 8x^3 + 6x^2 - 4x + 6$; (b) $\frac{2}{3}x^5 + \frac{1}{2}x^4 - 2x^2 + \frac{1}{2}$; (c) $\frac{1}{5}x^4 - \frac{1}{3}x^3 - \frac{2}{3}x + 1$; (d) $\frac{1}{2}x^4 + \frac{4}{3}x^3 - \frac{2}{3}x^2 + 1$.

Solution. (a) We have $2 \nmid 3$, $2| - 8$, $2|6$, $2| - 4$, $2|6$ and $2^2 = 4 \nmid 6$, so by Eisenstein, the polynomial $3x^4 - 8x^3 + 6x^2 - 4x + 6$ is irreducible over $\mathbb{Q}$. (b) We can take $6\left(\frac{2}{3}x^5 + \frac{1}{2}x^4 - 2x^2 + \frac{1}{2}\right) = 4x^5 + 3x^4 - 12x^2 + 3$, thus $3 \nmid 4$, $3|3$, $3| - 12$, $3|3$ and $3^2 = 9 \nmid 3$. By Eisenstein's criterion, $4x^5 + 3x^4 - 12x^2 + 3$ is irreducible and, by a previous proposition, it's associate $\frac{2}{3}x^5 + \frac{1}{2}x^4 - 2x^2 + \frac{1}{2}$ is also irreducible. (c) Take $15\left(\frac{1}{5}x^4 - \frac{1}{3}x^3 - \frac{2}{3}x + 1\right) = 3x^4 - 5x^3 - 10x + 15$. Then, $5 \nmid 3$, $5| - 5$, $5| - 10$, $5|15$ and $5^2 = 25 \nmid 15$. Therefore, by Eisenstein, the polynomial, along with its associate, is irreducible. (d) Let $6\left(\frac{1}{2}x^4 + \frac{4}{3}x^3 - \frac{2}{3}x^2 + 1\right) = 3x^4 + 8x^3 - 4x^2 + 6$. So, $2 \nmid 3$, $2|8$,

$2|-4$, $2|6$ and $2^2 = 4 \nmid 6$. By Eisenstein's criterion, the polynomial is irreducible, and by a previous proposition, so are all of its associates.

Proposition. Let F be a field, $a \in F$ and $p(x) \in F[x]$. Then, $p(x)$ is irreducible if and only if $p(x+a)$ is irreducible.

Proof. Notice that $\deg p(x) = \deg p(x+a)$. *Necessity.* Assume $p(x)$ is irreducible and that $p(x+a)$ is reducible. Then there exist $s(x), t(x) \in F[x]$ such that $p(x+a) = s(x)t(x)$. But, then, $p(x+a-a) = s(x-a)t(x-a)$, i.e. $p(x) = s(x-a)t(x-a)$. Therefore, $p(x)$ is reducible, which is a contradiction. *Sufficiency.* Follows the same reasoning as necessity.

□

Problem. Show that $x^4 + 4x + 1$ is irreducible over $\mathbb{Q}$ by using the change of variable $x \to x + 1$ and Eisenstein's criterion.

Solution. Let $p(x) = x^4 + 4x + 1$. Then, $p(x+1) = (x+1)^4 + 4(x+1) + 1 = x^4 + 4x^3 + 6x^2 + 4x + 1 + 4x + 4 + 1 = x^4 + 4x^3 + 6x^2 + 8x + 6$. As $2 \nmid 1$, $2|4$, $2|6$, $2|8$, $2|6$ and $2^2 = 4 \nmid 6$, then by Eisenstein, $p(x+1)$ is irreducible, and so is $p(x)$, by previous proposition.

Problem. Find an appropriate change of variable to prove that the following are irreducible in $\mathbb{Q}[x]$: (a) $x^4 + 2x^2 - 1$; (b) $x^3 - 3x + 1$; (c) $x^4 + 1$; (d) $x^4 - 10x^2 + 1$.

Solution. (a) Let $p(x) = x^4 + 2x^2 - 1$. Then, $p(x+k) = (x+k)^4 + 2(x+k)^2 - 1 = x^4 + 4x^3k + 6x^2k^2 + 4xk^3 + k^4 + 2x^2 + 4xk + 2k^2 - 1 = x^4 + 4x^3k + 2(3k^2+2)x^2 + 4k(k^2+1)x + (k^4 + 2k^2 - 1)$. For $k = 1$ we have the constant term to be $1^4 + 2 \cdot 1^2 - 1 = 2$, and the others are obviously divisible by 2 (except for the leading coefficient). Also, constant term is then not divisible by $2^2 = 4$. So, by Eisenstein, $p(x+1)$ is irreducible and so is $p(x)$. (b) Let $p(x) = x^3 - 3x + 1$. Then, $p(x+k) = (x+k)^3 - 3(x+k) + 1 = x^3 + 3x^2k + 3xk^2 + k^3 - 3x + 3k + 1 = x^3 + 3kx^2 + 3(k^2-1)x + (k^3 + 3k + 1)$. For $k = -1$ we have $(-1)^3 + 3 \cdot -1 + 1 = -1 - 3 + 1 = -3$, which is divisible by 3 but not by $3^2 = 9$. Other coefficients, except the leading coefficient, are visibly divisible by 3, so by Eisenstein's criterion, $p(x-1)$ is irreducible and, by a previous proposition, so is $p(x)$. (c) Let $p(x) = x^4 + 1$. Then, $p(x+k) = x^4 + 4x^3k + 6x^2k^2 + 4xk^3 + k^4 + 1$ and taking $k = 1$ gives us $k^4 + 1 = 2$, again divisible by 2 and not divisible by $2^2 = 4$, while other coefficients, except the leading one, are divisible by 2. So, by Eisenstein, $p(x+1)$ is irreducible, and so is $p(x)$.

(d) Let $q(x) = x^4 - 10x^2 + 1$. Let $k \in \mathbb{Z}$. Then, $q(x+k) = (x+k)^4 - 10(x+k)^2 + 1 = x^4 + 4x^3k + 6x^2k^2 + 4xk^3 + k^4 - 10x^2 - 20xk - 10k^2 + 1 = x^4 + (4k)x^3 + (6k^2 - 10)x^2 +$

$(4k^3-20k)x+(k^4-10k^2+1)$. Assume that there exists $p \in P$ that satisfies Eisenstein's criterion. Then, $p|4k$. If $p|4$, then it must be that $p=2$. If k is even then it cannot be proven by Eisenstein's criterion, as k^4-10k^2 is then even and k^4-10k^2+1 is odd, so $2 \nmid k^4-10k^2+1$. Yet, if k is odd, then $k=2k'+1$ and we would have the constant term to be $(2l+1)^4-10(2l+1)^2+1 = 16l^4+32l^3-16l^2-32l-8 = 4(4l^4+8l^3-4l^2-8l-2)$, which is divisible by 2^2. Thus, it is also not provable by Eisenstein's criterion. Next, assume that from $p|4k$ we have $p|k$, i.e. $k=pl$ for some $l \in \mathbb{Z}^+$. Then, $q(x+pl) = x^4+(4pl)x^3+(6p^2l^2-10)x^2+(4p^3l^3-20pl)x+(p^4l^4-10p^2l^2+1)$. Now, it also must be that $p|6p^2l^2-10$. Assume that is the case. Then, there exists $t \in \mathbb{Z}$ such that $6p^2l^2-10 = pt$. From that we have $10 = p(6pl^2-t)$, and it is either $p=2$ or $p=5$. The case $p=2$ is out of consideration because we already tested for even k, which proved to be impossible. So, we have $q(x+5l)$ and the constant term would be $5^4l^4-5^2\cdot 10l^2+1$. If that were divisible by 5, there would exist $s \in \mathbb{Z}$ such that $5^4l^4-5^2\cdot 10l^2+1 = 5s$. That would imply $1 = -5(5^3l^4-5^2\cdot 2l^2-s)$. As $-5 \nmid 1$, it must be that $125l^4-50l^2-s = \frac{1}{5}$. That is impossible since $l, s \in \mathbb{Z}$ and so $125l^4-50l^2-s \in \mathbb{Z}$ while $\frac{1}{5} \notin \mathbb{Z}$. Therefore, the irreducibility of x^4-10x^2+1 cannot be proved by Eisenstein's criterion along with an affine transformation.

Remark. Dual version of Eisenstein's criterion can be stated by using the fact that $h(a_0+a_1x+\cdots+a_mx^m) = a_m+a_{m-1}x+\cdots+a_0x^m$ matches irreducible polynomials with irreducible polynomials.

Problem. Show that each of the following polynomials is irreducible in $\mathbb{Q}[x]$: (a) $6x^4+4x^3-6x^2-8x+5$; (b) $x^4-\frac{1}{2}x^2+\frac{3}{2}x-\frac{4}{3}$; (c) $x^3+\frac{1}{2}x^2-\frac{3}{2}x+\frac{6}{5}$.

Solution. (a) As $2|6$, $2^2 \nmid 6$, $2|4$, $2|-6$, $2|8$ and $2 \nmid 5$, by dual of Eisenstein's criterion, $6x^4+4x^3-6x^2-8x+5$ is irreducible (over $\mathbb{Q}$). (b) We have $6\left(x^4-\frac{1}{2}x^2+\frac{3}{2}x-\frac{4}{3}\right) = 6x^4-3x^2+9x-8$. As $3|6$, $9 \nmid 6$, $3|0$, $3|-3$, $3|9$ and $3 \nmid 8$, then by dual of Eisenstein's criterion, polynomial $6x^4-3x^2+9x-8$ is irreducible over $\mathbb{Q}$, and by a previous proposition, so is its associate $x^4-\frac{1}{2}x^2+\frac{3}{2}x-\frac{4}{3}$. (c) Take $10\left(x^3+\frac{1}{2}x^2-\frac{3}{2}x+\frac{6}{5}\right) = 10x^3+5x^2-15x+12$. Then, $5|10$, $25 \nmid 10$, $5|5$, $5|-15$ and $5 \nmid 12$, so by dual of Eisenstein's criterion, polynomial $10x^3+5x^2-15x+12$ is irreducible over $\mathbb{Q}$, and by a previous proposition, so is its associate $x^3+\frac{1}{2}x^2-\frac{3}{2}x+\frac{6}{5}$.

Proposition. Let F be a field, $m \in \{2,3\}$ and $a(x) \in F[x]$ such that $\deg a(x) = m$. Then, $a(x)$ is irreducible if and only if $a(x)$ has no roots in F.

Proof. *Necessity.* Let $a(x)$ be irreducible. Assume that it has a root $c \in F$. Then, $x-c|a(x)$, i.e. there exists $q(x) \in F[x]$ such that $a(x) = (x-c)q(x)$. Note that, as $\deg a(x) \in \{2,3\}$, then $1 \leq \deg q(x) \leq 2$, depending on the degree of $a(x)$. That is in

contradiction that $a(x)$ is irreducible. *Sufficiency.* Assume that $a(x)$ has no roots in F and that $a(x)$ is reducible. Let $\deg a(x) \in \{2,3\}$. Then, there exist $q(x), p(x) \in F[x]$ such that $a(x) = q(x)p(x)$. But then, if $\deg p(x) = 1$, we have $\deg q(x) \in \{1,2\}$, so $p(x) = p_1x + p_0$. That implies $a(x) = (p_1x + p_0)q(x)$. But, taking $p_1x + p_0 = 0$ gives us $x = -p_0p_1^{-1}$ and it is obvious that $a(-p_0p_1^{-1}) = (-p_1p_0p_1^{-1} + p_0)q(-p_0p_1^{-1}) = (-p_0 + p_o)q(-p_0p_1^{-1}) = 0q(-p_0p_1^{-1}) = 0$, which is in contradiction to our assumption that $a(x)$ has no roots in F.

□

Problem. Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$: (a) $\frac{1}{2}x^3+2x-\frac{3}{2}$; (b) $3x^2 - 2x - 4$; (c) $x^3 + x^2 + \frac{3}{2}x + \frac{1}{2}$; (d) $x^3 + \frac{1}{2}$; (e) $x^2 - \frac{5}{2}x + \frac{3}{2}$.

Solution. (a) We can take $2\left(\frac{1}{2}x^3 + 2x - \frac{3}{2}\right) = x^3 + 4x - 3$. Remember that, if $x^3 + 4x - 3$ has a rational root $\frac{a}{b} \in \mathbb{Q}$, then $a \in \pm\{1,3\}$ and $b \in \{1,-1\}$. So, for 1 we have $1+4-3 = 2$ and for -1 we have $-1-4-3 = -8$. For 3 we have $27+12-3 \neq 0$ and for -3 we have $-27-12-3 \neq 0$. Therefore, $x^3 + 4x - 3$ has no rational roots, and is irreducible (by a previous proposition for $m = 3$) as is its associate $\frac{1}{2}x^3+2x-\frac{3}{2}$. (b) For $3x^2 - 2x - 4$ we have possible roots in $R = \left\{\pm1, \pm2, \pm4, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}\right\}$. Let $p(x) = 3x^2 - 2x - 4$. Then, $p(R) = \left\{-3, 1, \pm4, 12, 36, 52, -\frac{13}{3}, -\frac{4}{3}\right\}$. As $0 \notin p(R)$, then $p(x)$ has no rational roots and is irreducible due to the previous proposition. (c) We can take $p(x) = 2\left(x^3 + x^2 + \frac{3}{2}x + \frac{1}{2}\right) = 2x^3 + 2x^2 + 3x + 1$. The possible rational roots are $R = \left\{\pm1, \pm\frac{1}{2}\right\}$. Then, $p(R) = \left\{8, -12, \frac{13}{4}, -\frac{1}{4}\right\}$. Thus, $0 \notin p(R)$, so $p(x)$ has no rational roots. Thus it is irreducible and so is its associate $x^3 + x^2 + \frac{3}{2}x + \frac{1}{2}$. (d) Let $p(x) = 2\left(x^3 + \frac{1}{2}\right) = 2x^3 + 1$. Then we look for roots in $R = \left\{\pm1, \pm\frac{1}{2}\right\}$. We have $p(R) = \left\{3, -1, \frac{5}{4}, \frac{3}{4}\right\}$ and $0 \notin p(R)$, so $p(x)$ has no rational roots and is irreducible over $\mathbb{Q}$. (e) Take $p(x) = 2\left(x^2 - \frac{5}{2}x + \frac{3}{2}\right) = 2x^2 - 5x + 3$. Then, roots of $p(x)$ are in $R = \left\{\pm1, \pm3, \pm\frac{1}{2}, \pm\frac{3}{2}\right\}$. But, $p(1) = 0$, so $p(x)$ is not irreducible over $\mathbb{Q}$.

Proposition. Suppose a monic polynomial $p(x)$ of degree 4 in $F[x]$ has no roots in F. Then, $p(x)$ is reducible if and only if it is a product of two irreducible quadratics $x^2 + ax + b$ and $x^2 + cx + d$.

Proof. Let $p(x) \in F[x]$ such that $p(x) = x^4+a_3x^3+a_2x^2+a_1x+a_0$. *Necessity.* Assume that $p(x)$ is reducible, has no roots in F and is not a product of two quadratics. Then, the only other option is that $p(x) = (x + a)(x^3 + bx^2 + cx + d)$. But that would mean that $-a \in F$ is a root of $p(x)$, which is a contradiction to assumption that $p(x)$ has no roots in F. Therefore, $p(x)$ is a product of two quadratics. If one of the quadratics $q(x)$ were reducible, that would mean that $x + a|q(x)$ and that would imply $x + a|p(x)$ (as $q(x)|p(x)$ and that relation is transitive) which would again mean that $-a \in F$ is a root and that would be in contradiction to assumption that $p(x)$ has no roots in

F. Sufficiency. Trivial. If $p(x) = (x^2 + ax + b)(x^2 + cx + d)$ then it is by definition reducible.

□

Remark. Note that if $p(x) = (x^2 + ax + b)(x^2 + cx + d)$, then $p(x) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$.

Problem. Prove that the following polynomials are irreducible or reducible in $\mathbb{Q}[x]$: (a) $x^4 - 5x^2 + 1$; (b) $3x^4 - x^2 - 2$; (c) $x^4 + x^3 + 3x + 1$.

Solution. (a) The only possible roots of $p(x) = x^4 - 5x^2 + 1$ are 1 and -1. We have $p(1) = p(-1) = 1 - 5 + 1 = -3$, so $p(x)$ has no roots in $\mathbb{Q}$. Then, the only other possibility is that $p(x)$ is a product of two quadratics. That would mean that (considering the previous remark) $a + c = 0$, $b + ac + d = -5$, $ad + bc = 0$ and $bd = 1$. First we have $c = -a$. That implies $b + ac + d = b - a^2 + d = -5$ and $ad - ab = 0$, i.e. $a(d - b) = 0$. If $a = 0$, then we would have $a = c = 0$, $b + d = -5$ and $bd = 1$. Combining latter and former would give $b^2 + bd = -5b$, i.e. $b^2 + 1 = -5b$. From that we have $b^2 + 5b + 1 = 0$. But, that polynomial is irreducible (as $1 + 5 + 1 = 7$ and $1 - 5 + 1 = -3$), so b cannot be rational, i.e. if $a = 0$, the polynomial $p(x)$ cannot be written as a product of two polynomials in $\mathbb{Q}[x]$. Assume $a \neq 0$. Then, as $\mathbb{Q}$ is an integral domain, $a(d - b) = 0$ implies $d = b$. But, that would give from $bd = 1$ that $b^2 = 1$. So, $b = \pm 1$ and then $\pm 1 \cdot d = 1$, i.e. $\pm d = 1$. That is of course $d = \pm 1$. From $b - a^2 + d = -5$ we would have $\pm 1 - a^2 + \pm 1 = -5$, i.e. $-a^2 + \pm 2 = -5$. First case, $-a^2 + 2 = -5$ gives us $-a^2 + 7 = 0$, i.e. $a^2 - 7 = 0$. That polynomial has no rational roots, so a is not rational. Also, for the second case $-a^2 - 2 = -5$ we would have $-a^2 + 3 = 0$, i.e. $a^2 - 3 = 0$. That polynomial also has no rational roots (the only possible choices are 3 and -3), a is again not rational. Therefore, in any case $p(x)$ cannot be written down as a product of two quadratics in $\mathbb{Q}[x]$.

(b) Let $p(x) = 3x^4 - x^2 - 2$. Then, its roots are in $R = \left\{\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}\right\}$ and we have $p(1) = p(-1) = 3 - 1 - 2 = 0$. Thus, $3x^4 - x^2 - 2 = (x - 1)(x + 1)(x^2 + ax + b)$, for some $a, b \in \mathbb{Q}$. From that we have $3x^4 - x^2 - 2 = (x^2 - 1)(ax^2 + bx + c) = ax^4 + bx^3 + (c - a)x^2 - bx - c$. That implies $a = 3$, $b = -b = 0$, $c - a = -1$ and $-c = -2$, i.e. $c = 2$. So, $2 - a = -1$ and we have $-a = -3$, i.e. $a = 3$, which is in accordance with the polynomial. Thus, $3x^4 - x^2 - 2 = (x^2 - 1)(3x^2 + 2)$. It is obvious that $3x^2 + 2$ is irreducible. Its possible roots are in $R = \left\{\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}\right\}$ leading us to $3R^2 + 2 = \left\{5, 14, \frac{7}{3}, \frac{10}{3}\right\}$. So, as $0 \notin 3R^2 + 2$, $3x^2 + 2$ is irreducible.

(c) Take $p(x) = x^4 + x^3 + 3x + 1$. The only possibilities for roots are 1 and -1 so $p(1) = 1 + 1 + 3 + 1 = 6$ and $p(-1) = 1 - 1 - 3 + 1 = 2 - 4 = -2$. Therefore, $p(x)$ must be a product of two quadratics. So, taking in consideration previous remark, $x^4 + x^3 + 3x + 1 = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$. That implies $a + c = 1$,

$b+ac+d=0$, $ad+bc=3$ and $bd=1$. We have $c=1-a$ and $b+a(1-a)+d=0$. That gives us $b+a-a^2+d=0$. Multiplying that by b gives us $b^2+ab-a^2b+bd=0$, i.e. $b^2+b(a-a^2)+1=0$. Now, the only two options are that $b\in\{1,-1\}$. If $b=1$, then $d=1$ and $a-a^2+2=0$. We can see that $-1-1+2=0$ so $a=-1$ is one possibility. Then we would have $c=2$. Also, $ad+bc=-1\cdot 1+1\cdot 2=-1+2=1\neq 3$, so that doesn't work. The other possibility for solutions of $a-a^2+2=0$ is $2-2^2+2=0$. So, assume $a=2$. Then, $c=-1$ and we would have $1-2\cdot 1+1=2-2=0$, but also $2\cdot 1-1\cdot 1=1\neq 3$, so that is impossible. Assume $b=-1$. Then, $1-a+a^2+1=0$, i.e. $a^2-a+2=0$. We see that the possible roots for a are $R=\{\pm 1,\pm 2\}$ and that $R^2-R+2=\{2,4,8\}$. So, as $0\notin R^2-R+2$, a^2-a+2 has no rational roots and the case for $b=-1$ is impossible. Thus, $p(x)$ cannot be shown as a product of two quadratics and it has no rational roots. In conclusion, x^4+x^3+3x+1 is irreducible over $\mathbb{Q}$.

Remark. For the following problems we will deal with $\mathbb{Z}/5\mathbb{Z}$ field, so we will write out the addition and multiplication table (the squares are bold):

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\mathbf{\overline{0}}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\mathbf{\overline{1}}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\mathbf{\overline{4}}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\mathbf{\overline{4}}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\mathbf{\overline{1}}$

Also, notice that, as $\overline{x}^2\in\{\overline{1},\overline{4}\}$, for all $\overline{x}\in\mathbb{Z}/5\mathbb{Z}-\{\overline{0}\}$, then $\overline{x}^4=\overline{1}$, for all $\overline{x}\in\mathbb{Z}/5\mathbb{Z}-\{0\}$. That is actually a consequence of Fermat's theorem. :-)

Problem. Prove that the following polynomials are irreducible in $\mathbb{Z}/5\mathbb{Z}[x]$: (a) $\overline{2}x^3+x^2+\overline{4}x+\overline{1}$; (b) $x^4+\overline{2}$; (c) $x^4+\overline{4}x^2+\overline{2}$; (d) $x^4+\overline{1}$.

Solution. (a) Let $p(x)=\overline{2}x^3+x^2+\overline{4}x+\overline{1}$. We only need to check values for $\overline{0},\overline{1},\ \overline{2},\ \overline{3}$ and $\overline{4}$. Thus, $p(\overline{0})=\overline{1}$, $p(\overline{1})=\overline{8}=\overline{3}$, $p(\overline{2})=\overline{2}\cdot\overline{8}+\overline{4}+\overline{9}=\overline{29}=\overline{4}$, $p(\overline{3})=\overline{2}\cdot\overline{2}+\overline{4}+\overline{3}=\overline{11}=\overline{1}$, $p(\overline{4})=\overline{8}+\overline{1}+\overline{2}=\overline{1}$. Therefore, $p(x)$ has no roots in $\mathbb{Z}/5\mathbb{Z}$, so by a previous proposition, it is irreducible in $\mathbb{Z}/5\mathbb{Z}[x]$.

(b) Let $p(x)=x^4+\overline{2}$. First we will check for the roots. We have $p(\overline{0})=\overline{2}$, $p(\overline{1})=p(\overline{2})=p(\overline{3})=p(\overline{4})=\overline{1}+\overline{2}=\overline{3}$, so there are no roots. The only possibility is that $p(x)$ is a product of two quadratics, that is, $x^4+\overline{2}=(x^2+\overline{a}x+\overline{b})(x^2+\overline{c}x+\overline{d})$. From that we have $\overline{a}+\overline{c}=\overline{0}$, $\overline{b}+\overline{ac}+\overline{d}=\overline{0}$, $\overline{ad}+\overline{bc}=\overline{0}$ and $\overline{bd}=\overline{2}$. We have $\overline{c}=-\overline{a}$, so $\overline{b}-\overline{a}^2+\overline{d}=\overline{0}$ and $\overline{a}(\overline{d}-\overline{b})=\overline{0}$. Assume $\overline{a}=\overline{0}$. That would imply $\overline{b}+\overline{d}=\overline{0}$. Multiplying that by $\overline{d}$ would give us $\overline{2}+\overline{d}^2=\overline{0}$, i.e. $\overline{d}^2=\overline{3}$. There does not exist such $\overline{d}\in\mathbb{Z}/5\mathbb{Z}$. Assume $\overline{a}\neq 0$. Then, from $\overline{a}(\overline{d}-\overline{b})=\overline{0}$ we have $\overline{d}=\overline{b}$. That gives

us $\overline{bd} = \overline{b}^2 = \overline{2}$. There does not exist such $\overline{b} \in \mathbb{Z}/5\mathbb{Z}$, so $p(x)$ must be irreducible in $\mathbb{Z}/5\mathbb{Z}[x]$.

(c) Take $p(x) = x^4 + \overline{4}x^2 + \overline{2}$. As $\overline{x}^4 = \overline{1}$, for all $\overline{x} \in \mathbb{Z}/5\mathbb{Z}$ it's easy to see that $p(\overline{1}) = p(\overline{4}) = \overline{1} + \overline{4} + \overline{2} = \overline{2}$ and $p(\overline{2}) = p(\overline{3}) = \overline{1} + \overline{1} + \overline{2} = \overline{4}$. Also, $p(\overline{0}) = \overline{2}$, so we will be observing $p(x)$ as a product of two quadratics, $x^2 + \overline{a}x + \overline{b}$ and $x^2 + \overline{c}x + \overline{d}$. Using the previous remark we can see that $\overline{a} + \overline{c} = \overline{0}$, i.e. $\overline{c} = -\overline{a}$. Then, using that fact, we have $\overline{b} - \overline{a}^2 + \overline{d} = \overline{4}$, $\overline{a}(\overline{d} - \overline{b}) = \overline{0}$ and $\overline{bd} = \overline{2}$. Assume that $\overline{a} = \overline{0}$. Then we have $\overline{c} = 0$ and $\overline{b} + \overline{d} = \overline{4}$. Multiplying that by $\overline{d}$ gives us $\overline{2} + \overline{d}^2 + \overline{d} = \overline{0}$, i.e. $\overline{d}^2 + \overline{d} + \overline{2} = \overline{0}$. Let $q(x) = x^2 + x + \overline{2}$. Then, $q(\overline{1}) = \overline{4}$, $q(\overline{2}) = \overline{3}$, $q(\overline{3}) = \overline{4}$ and $q(\overline{4}) = \overline{2}$. Therefore, there does not exist $\overline{d} \in \mathbb{Z}/5\mathbb{Z}$ such that $\overline{d}^2 + \overline{d} + \overline{2} = \overline{0}$ and $\overline{a} = \overline{0}$ is an impossibility. Thus, it must be that $\overline{a} \neq 0$. Then from $\overline{a}(\overline{d} - \overline{b}) = \overline{0}$ we get $\overline{b} = \overline{d}$ and then $\overline{b}^2 = \overline{2}$. It is easy to see from the multiplication table above that there does not exist such $\overline{b} \in \mathbb{Z}/5\mathbb{Z}$. That implies that $p(x)$ is irreducible over field $\mathbb{Z}/5\mathbb{Z}$.

(d) Let $p(x) = x^4 + \overline{1}$. It is easy to see that $p(\overline{0}) = \overline{1}$ and $p(\overline{1}) = p(\overline{2}) = p(\overline{3}) = p(\overline{4}) = \overline{1}$, due to Fermat's theorem. Therefore, as $p(x)$ has no roots in $\mathbb{Z}/5\mathbb{Z}$, and is of degree 4, it can only be that $p(x) = (x^2 + \overline{a}x + \overline{b})(x^2 + \overline{c}x + \overline{d})$, if it is reducible. That implies, by observing previous remark, $\overline{a} + \overline{c} = \overline{b} + \overline{ac} + \overline{d} = \overline{ad} + \overline{bc} = \overline{0}$ and $\overline{bd} = \overline{1}$. We have $\overline{a} = \overline{-c}$ and then $\overline{b} - \overline{a}^2 + \overline{d} = \overline{0}$ and $\overline{a}(\overline{d} - \overline{b}) = \overline{0}$. If $\overline{a} = \overline{0}$ we have $\overline{b} + \overline{d} = \overline{0}$, i.e. $\overline{d} = -\overline{b}$. Thus, $-\overline{b}^2 = \overline{1}$, i.e. $\overline{b}^2 = \overline{4}$. If $\overline{b} = \overline{2}$, then $\overline{d} = \overline{3}$. Also, remember that $\overline{a} = \overline{c} = \overline{0}$. Then, checking $p(x) = (x^2 + \overline{2})(x^2 + \overline{3}) = x^4 + \overline{2}x + \overline{3}x + \overline{6} = x^4 + \overline{5}x + \overline{1} = x^4 + \overline{1}$ and $p(x)$ is reducible over field $\mathbb{Z}/5\mathbb{Z}$.

Proposition. Let $m \in \mathbb{Z}^+$ and let $h : \mathbb{Z}[x] \to \mathbb{Z}/m\mathbb{Z}[x]$ be a mapping defined as:

$$h(a_m x^m + \cdots + a_1 x + a_0) = \overline{a_m} x^m + \cdots + \overline{a_1} x + \overline{a_0}.$$

Then, h is a homomorphism and if $h(a(x))$ is irreducible in $\mathbb{Z}/m\mathbb{Z}[x]$ and $a(x)$ is monic, then $a(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. We have already proved that h is a homomorphism in a previous proposition. Let $a(x) \in \mathbb{Z}[x]$ be a monic polynomial. Let $h(a(x))$ be irreducible in $\mathbb{Z}/m\mathbb{Z}[x]$ and assume $a(x)$ is reducible in $\mathbb{Z}[x]$. As $a(x)$ is reducible in $\mathbb{Z}[x]$, there exist $q(x), r(x) \in \mathbb{Z}[x]$ such that $a(x) = q(x)r(x)$ (and degrees of $q(x)$ and $r(x)$ are greater or equal to one). Then, $h(a(x)) = h(q(x)r(x))$, as h is a function. As h is also a homomorphism, we have $h(a(x)) = h(q(x))h(r(x))$. Now, as the leading coefficient of $a(x)$ is 1, then the leading coefficient of $h(a(x))$ is $\overline{1}$. Thus, the degree of $h(a(x))$ remains the same as the degree of $a(x)$. That also implies that degrees of $h(q(x))$ and $h(r(x))$ remain the same as $q(x)$ and $r(x)$. But, that would imply that $h(a(x))$ is reducible, which is a contradiction to assumption that $h(a(x))$ is irreducible.

□

Problem. Prove that $x^4 + 10x^3 + 7$ is irreducible in $\mathbb{Q}[x]$ by using the natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/5\mathbb{Z}$.

Solution. We have $h(x^4 + 10x^3 + 7) = x^4 + \overline{2}$ in $\mathbb{Z}/5\mathbb{Z}[x]$. We have proved in the previous problem that $x^4 + \overline{2}$ is irreducible, and so is $x^4 + 10x^3 + 7$ irreducible in $\mathbb{Z}[x]$. But then, due to Gauss' lemma (applicable as $x^4 + 10x^3 + 7 \in \mathbb{Z}[x]$, it is also irreducible in $\mathbb{Q}[x]$).

Problem. Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$: (a) $x^4 - 10x^2 + 1$; (b) $x^4 + 7x^3 + 14x^2 + 3$; (c) $x^5 + 1$.

Solution. (a) In $\mathbb{Z}/5\mathbb{Z}$, we have $x^4 + \overline{1}$, which is, again, irreducible as argued in the previous problem. Then, as $x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$, by Gauss' lemma, it is also irreducible in $\mathbb{Q}[x]$. (b) In $\mathbb{Z}/7\mathbb{Z}$ we have $x^4 + \overline{3}$. For $x = \overline{4}$, we have $\overline{16}^2 + \overline{3} = \overline{2}^2 + \overline{3} = \overline{4} + \overline{3} = \overline{7}$. So, we can't prove the irredicibility of $x^4 + 7x^3 + 14x^2 + 3$ by using a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/7\mathbb{Z}$. However, in $\mathbb{Z}/2\mathbb{Z}$, we have $x^4 + x^3 + \overline{1}$. It is obvious that $\overline{0}$ and $\overline{1}$ are not the roots of $x^4 + x^3 + \overline{1}$. So, assume that $x^4 + x^3 + \overline{1} = (x^2 + \overline{a}x + \overline{b})(x^2 + \overline{c}x + \overline{d})$. It is obvious that $\overline{b} = \overline{d} = \overline{1}$. But then $\overline{c + a} = \overline{1}$ (for x^3), $\overline{d + b + ac} = \overline{0}$, i.e. $\overline{ac} = \overline{0}$ (for x^2) and $\overline{ad + bc} = \overline{0}$. Assume $\overline{a} = \overline{1}$. If $\overline{c} = \overline{1}$, then $\overline{c + a} = \overline{0}$. If $\overline{c} = \overline{0}$, then $\overline{a + c} = \overline{0}$ and $\overline{ac} = \overline{0}$, which is in accordance with the formulae. But, also we need $\overline{cb} + \overline{ad} = \overline{0}$, i.e. $\overline{0} + \overline{1} = \overline{1}$, which is a contradiction. Therefore, $x^4 + 7x^3 + 14x^2 + 3$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$ and so it is in $\mathbb{Z}[x]$ and, by Gauss' lemma (as $x^4 + 7x^3 + 14x^2 + 3 \in \mathbb{Z}[x]$), in $\mathbb{Q}[x]$. (c) In $\mathbb{Z}/7\mathbb{Z}[x]$ we have already shown that $x^5 + \overline{1}$ is irreducible. So, $x^5 + 1$ is irreducible in $\mathbb{Z}[x]$ and, because $x^5 + 1 \in \mathbb{Z}[x]$, by Gauss' lemma, it is also irreducible in $\mathbb{Q}[x]$.

Theorem (Lagrange interpolation formula). Let F be a field and let $a_1, \ldots, a_m \in F$ and $b_1, \ldots, b_m \in F$, where $a_i \neq a_j$ (but some b_i might be equal), for all $i \neq j$, $i, j \in \{1, \ldots, m\}$. Then, there exists a unique polynomial $p(x) \in F[x]$ such that $\deg p(x) = m - 1$ and $p(a_i) = b_i$, for all $i \in \{1, \ldots, m\}$, given with formula:

$$p(x) = \sum_{i=1}^{m} b_i [q_i(a_i)]^{-1} q_i(x),$$

where

$$q_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{m} (x - a_j).$$

Proof. *Existence.* Existence is of course implied by formula, as we see that it confines to properties of the field F. All we need to do is check that $p(a_i) = b_i$, for all $i \in \{1, \ldots, m\}$. First, notice that $q_i(a_i) \neq 0$. For, if it were that $q_i(a_i) = 0$, then it would mean that $x - a_i | q_i(x)$, but that is impossible because by definition of $q_i(x)$, $x - a_i \nmid q_i(x)$. The only other possibility would be $x - a_i = x - a_j$, for some $j \in \{1, \ldots, m\}$ and $i \neq j$, but that would imply $a_i = a_j$ for some $i \neq j$, which is contrary to assumption that $a_1, \ldots, a_m$ are all distinct. Furthermore, we have:

$$p(a_j) = \sum_{i=1}^{m} b_i [q_i(a_i)]^{-1} q_i(a_j).$$

Then, we can view the sum as:

$$p(a_j) = \sum_{i=1}^{j-1} b_i [q_i(a_i)]^{-1} q_i(a_j) + b_j [q_j(a_j)]^{-1} q_j(a_j) + \sum_{i=j+1}^{m} b_i [q_i(a_i)]^{-1} q_i(a_j).$$

When, $i \neq j$, notice that $q_i(a_j) = 0$ as, by definition, $x - a_j | q_i(x)$, for all $j \in \{1, \ldots, m\} - \{i\}$. Then, all members of the sum vanish except for j-th member (the member in the "middle" of the equality above). Thus we have:

$$p(a_j) = \sum_{i=1}^{j-1} b_i [q_i(a_i)]^{-1} 0 + b_j [q_j(a_j)]^{-1} q_j(a_j) + \sum_{i=j+1}^{m} b_i [q_i(a_i)]^{-1} 0.$$

That is,

$$p(a_j) = b_j [q_j(a_j)]^{-1} q_j(a_j).$$

As $q_j(a_j) \neq 0$, then $[q_j(a_j)]^{-1} q_j(a_j) = 1$ and we have $p(a_j) = b_j$, for all $j \in \{1, \ldots, m\}$. Now, the degree of the polynomial is of course $m - 1$ as the degree of $q_i(x)$ is $m - 1$. The final polynomial $p(x)$ includes only the sums of $q_i(x)$ along with some zero degree coefficients.

Uniqueness. Assume that there exist two polynomials $p(x), q(x) \in F[x]$, such that $p(x) \neq q(x)$ and $p(a_i) = q(a_i) = b_i$, for all $i \in \{1, \ldots, m\}$ and that $\deg p(x) = \deg q(x) = m - 1$. Then, if $r(x) = p(x) - q(x)$ it must be $r(x) \neq 0$ and $r(x) \leq \max\{\deg p(x), \deg q(x)\} = m - 1$. Also, $r(a_i) = p(a_i) - q(a_i) = b_i - b_i = 0$, for all $i \in \{1, \ldots, m\}$, so a_i is the root of $r(x)$ in F and we have $x - a_i | r(x)$ for all $i \in \{1, \ldots, m\}$. But, that implies $r(x) = t(x)(x - a_1) \cdots (x - a_m)$ and we have $\deg r(x) = \deg t(x) + m$, i.e. $m - 1 \leq \deg r(x) > m - 1$. That would imply $m - 1 > m - 1$ which is impossible. So, it must be $p(x) = q(x)$, which is possible as then $r(x) = 0$ and $x - a_i | 0$, for all $i \in \{1, \ldots, m\}$.

□

Corollary. Let F be a finite field, $S, T \subseteq F$ non-empty sets and let $f : S \to T$ be a function. There exists a polynomial function $p : S \to T$ such that $p(x) = f(x)$, for all $x \in S$. Also, $\deg p(x) = |S| - 1$.

Proof. As F is finite, then S and T are finite. Assume $|S| = m$, i.e. $S = \{s_1, \ldots, s_m\}$ (of course $s_i \neq s_j$, for all $i \in \{1, \ldots, m\}$). Then, let $f(S) = \{f(s_1), \ldots, f(s_m)\}$ (some $f(s_i)$ might not be distinct, as f is not necessarily an injection). Thus, by Lagrange interpolation formula, there exists unique $p(x) \in F[x]$ such that $p(s_i) = f(s_i)$, for all $i \in \{1, \ldots, m\}$. It is easy to see now that $p(x) = f(x)$, for all $x \in S$. Also, from Lagrange interpolation formula, we have $\deg p(x) = |S| - 1$.

□

Definition. Let F be a field, $q(x) \in F[x]$ and $a_1, \ldots, a_m \in F$. The unique polynomial $p(x) \in F[x]$ such that $\deg p(x) < m$ and $p(a_1) = t(a_1), \ldots, p(a_m) = t(a_m)$ is called the **Lagrange interpolator** for $q(x)$ and $a_1, \ldots, a_m$.

Proposition. Let F be a field and $q(x) \in F[x]$. Let $p(x) \in F[x]$ be the Lagrange interpolator for $q(x)$ and $a_1, \ldots, a_m \in F$. Then, the remainder of $q(x)$ divided by $(x - a_1) \cdots (x - a_m)$ is $p(x)$.

Proof. Let $p(x)$ be the Lagrange interpolator for $q(x)$ and $a_1, \ldots, a_m \in F$. Then, $p(a_i) = q(a_i)$ for all $i \in \{1, \ldots, m\}$. By theorem of polynomial division we have $q(x) = (x - a_1) \cdots (x - a_m) + r(x)$, where $0 \leq \deg r(x) < m$. Then, $p(a_i) = q(a_i) = (a_i - a_1) \cdots (a_{i-1} - a_i)(a_i - a_i)(a_i - a_{i+1}) \cdots (a_i - a_m) + r(a_i) = 0 + r(a_i) = r(a_i)$, for all $i \in \{1, \ldots, m\}$. As $p(a_i) = q(a_i) = r(a_i)$ and as $\deg p(x), \deg r(x) < m$, by a previous proposition, $p(x) = r(x)$.

□

Problem. Find three polynomials in $\mathbb{Z}/5\mathbb{Z}[x]$ which determine the same function as $x^2 - x + \overline{1}$.

Solution. Let $f(x) = x^2 - x + \overline{1}$. Then, $f(\overline{0}) = f(\overline{1}) = \overline{1}$, $f(\overline{2}) = f(\overline{4}) = \overline{3}$, $f(\overline{3}) = \overline{2}$. By using the previous proposition, we can see that for $p_1(x) = x(x-\overline{1})(x-\overline{2})(x-\overline{3})(x-\overline{4}) + f(x)$ we have $p_1(x) = f(x)$, for all $x \in \mathbb{Z}/5\mathbb{Z}$. So, after some calculation $p_1(x) = x^5 + x^2 + \overline{3}x + \overline{1}$. Now, other polynomials can be obtained by changing powers of $(x - \overline{a})$, for some $\overline{a} \in \mathbb{Z}/5\mathbb{Z}$. Thus, $p_2(x) = x(x-\overline{1})(x-\overline{2})^2(x-\overline{3})(x-\overline{4}) + f(x) = x^6 + \overline{3}x^5 + x + \overline{1}$ and $p_2(x) = x(x - \overline{1})(x - \overline{2})^2(x - \overline{3})^2(x - \overline{4}) + f(x) = x^7 + x^5 + \overline{4}x^3 + x^2 + \overline{3}x + \overline{1}$.

Proposition. Let $p \in P$. Then, in $\mathbb{Z}/p\mathbb{Z}[x]$:

$$x^p - x = x(x - \overline{1})(x - \overline{2}) \cdots (x - (\overline{p-1})).$$

Proof. By Fermat's theorem $x^{p-1} = \overline{1}$ for all $x \in \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$. That is, $x^p = x$. From that we have $x^p - x = \overline{0}$, for all $x \in \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$. Also $\overline{0}^p - \overline{0} = \overline{0}$. Therefore, $x^p - x = \overline{0}$, for all $x \in \mathbb{Z}/p\mathbb{Z}$. If $q(x) = x^p - x$, then $q(\overline{a}) = \overline{0}$ for all $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$. Therefore, $x - \overline{a} | x^p - x$ for all $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$. As $\deg(x^p - x) = p$ and there are p roots, we have $x^p - x = x(x - \overline{1}) \cdots (x - (\overline{p-1}))$.

□

Proposition. Let $p \in P$ and $a(x), b(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ such that $a(x) = b(x)$ for all $x \in \mathbb{Z}/p\mathbb{Z}$. Then, $x^p - x | a(x) - b(x)$.

Proof. If $a(x) = b(x)$ for all $x \in \mathbb{Z}/p\mathbb{Z}$, then also $a(x) - b(x) = 0$ for all $x \in \mathbb{Z}/p\mathbb{Z}$. Therefore, $x - \overline{q} | a(x) - b(x)$ for all $\overline{q} \in F$. Thus, $x(x - \overline{1}) \cdots (x - (\overline{p-1})) | a(x) - b(x)$, i.e. $x^p - x | a(x) - b(x)$.

□

Proposition. Let F be a finite field and $a(x), b(x) \in F[x]$. If $a(x) = b(x)$, for all $x \in F$, and if $|F| > \deg a(x), \deg b(x)$, then[87] $a(x) = b(x)$.

Proof. As F is finite, then $F = \{c_1, \ldots, c_m\}$, for some $m \in \mathbb{Z}^+ - \{1\}$. Thus, by a previous proposition, as $a(c_i) = b(c_i)$, for all $i \in \{1, \ldots, m\}$, and as $\deg a(x), \deg b(x) < m$, then $a(x) = b(x)$.

□

Proposition. Let F be a finite field and $J = \{a(x) \in F[x] : (\forall x \in F)(a(x) = 0)\}$. Then, $J \trianglelefteq F[x]$.

Proof. First, by definition $J \subseteq F[x]$. Take $a(x), b(x) \in J$. Then, as $a(x) = 0$ and $b(x) = 0$ for all $x \in F$, then $a(x) - b(x) = 0 + 0 = 0$, for all $x \in F$. Also, $a(x)b(x) = 0 \cdot 0 = 0$, for all $x \in F$. That implies $a(x) - b(x), a(x)b(x) \in J$. If $c(x) \in F[x]$, then $a(x)c(x) = 0c(x) = 0$ and $c(x)a(x) = c(x)0 = 0$, for all $x \in F$, and that implies $a(x)c(x), c(x)a(x) \in J$. In other words, $J \trianglelefteq F[x]$.

[87] Notice that $a(x) = b(x)$ for all $x \in F$ is an equality for polynomial functions while $a(x) = b(x)$ means that the polynomial $a(x)$ is equal to the polynomial $b(x)$, i.e. they have the same degrees and coefficients.

□

Remark. Notice that, as $F[x]$ is a principal ideal domain, J is a principal ideal. So, if $J = \langle g(x) \rangle$ and $a(x) \in J$, then $g(x) = a(x) = 0$, for all $x \in F$. Generator is $g(x) = x^p - x$. If it were one of a lesser degree, it could only be 0. For a field with $a_1, \ldots, a_m$ as its elements, of course $J = \langle (x - a_1) \cdots (x - a_m) \rangle$.

Proposition. Let $F = \{a_1, \ldots, a_m\}$ be a finite field. Let $\mathcal{F}(F)$ be the ring of all functions from F to F, defined in the same way as $\mathcal{F}(\mathbb{R})$. Let $h : F[x] \to \mathcal{F}(F)$ send every polynomial $a(x)$ to the polynomial function which it determines. Then, h is a homomorphism from $F[x]$ onto[88] $\mathcal{F}(F)$ and $F[x]/\langle (x - a_1) \cdots (x - a_m) \rangle \cong \mathcal{F}(F)$.

Proof. It is obvious that h is a well-defined function. For every $p(x) \in F[x]$ there exists $p \in \mathcal{F}(F)$ such that $h(p(x)) = p$. Then, if $p(x) = q(x)$, i.e. $p(x)$ and $q(x)$ have the same coefficients (and same degrees) we also have $p(x) = q(x)$, for all $x \in F$, i.e. $p = q$. Take $p \in \mathcal{F}(F)$. Then, by a previous proposition, there exists $q(x) \in F[x]$ such that $q(x) = p(x)$, for all $x \in F$. Therefore, $h(q(x)) = p$ and h is surjective. Now we will show that h is a homomorphism. Let $h_1 = h(p(x) + q(x))$, $h_p = h(p(x))$ and $h_q = h(q(x))$. Then, $[h_p + h_q](x) = p(x) + q(x)$, for all $x \in F$. But, $h_1(x) = p(x) + q(x)$, for all $x \in F$, so $h_1(x) = [h_p + h_q](x)$, for all $x \in F$, i.e. $h_1 = h_p + h_q$. The same is proved for multiplication up to the change of symbol of operation. Thus, h is a surjective homomorphism. We have $\ker(h) = \{p(x) \in F[x] : \ h(p(x)) = 0\}$, i.e. $\ker(h) = \{p(x) \in F[x] : \ (\forall x \in F)(p(x) = 0)\}$, and from previous proposition and remark $\ker(h) = \langle (x - a_1) \cdots (x - a_m) \rangle$. By FHT that implies $\mathcal{F}(F)$ and $F[x]/\langle (x - a_1) \cdots (x - a_m) \rangle \cong \mathcal{F}(F)$.

□

[88] It is surjective.

Extensions of fields

Definition. Let F be a field and $K \leq F$. We say that K is a **subfield** of F and that F is an **extension field** of K.

Remark. Notice that from the beginning of the ring theory we have proved that $K \leq F$, when F is a field, implies that K is also a field.

Definition. Let E and F be fields such that $F \leq E$. Let $c \in E$ and $a(x) \in F[x]$. The mapping $\sigma_c : F[x] \to E$ defined with $\sigma_c(a(x)) = a(c)$ is called a **substitution function**.

Theorem. Let E be a field, $F \leq E$ and $c \in E$. Then, the substitution function σ_c is a homomorphism.

Proof. It is obvious that σ_c is well-defined. Also, if $a(x) = b(x)$, then $a(c) = b(c)$, i.e. $\sigma_c(a(x)) = \sigma_c(b(x))$. Then, $\sigma_c(a(x) + b(x)) = a(c) + b(c) = \sigma_c(a(x)) + \sigma_c(b(x))$. Also, $\sigma_c(a(x)b(x)) = a(c)b(c) = \sigma_c(a(x))\sigma_c(b(x))$. Thus, σ_c is a homomorphism.

□

Corollary. Let E be a field, $F \leq E$ and $c \in E$. Then, there exists $p(x) \in F[x]$ such that $\ker(\sigma_c) = \langle p(x) \rangle$.

Proof. We have $\ker(\sigma_c) = \{a(x) \in F[x] : \ \sigma_c(a(x)) = 0\} = \{a(x) \in F[x] : \ a(c) = 0\}$. Thus, $a(x) \in \ker(\sigma_c)$ if and only if $c \in E$ is a root of $a(x)$. Also, $\ker(\sigma_c) \trianglelefteq F[x]$, and as $F[x]$ is a principal ideal domain, $\ker(\sigma_c)$ is principal, i.e. $\ker(\sigma_c) = \langle p(x) \rangle$, for some $p(x) \in F[x]$.

□

Definition. Let E be a field, $F \leq E$ and $c \in E$. We say that a polynomial $a(x) \in F[x]$ such that $\deg a(x) > 0$, is a **minimal polynomial of** c **over** F if:

1. $a(x)$ is monic and $a(c) = 0$;
2. For all $b(x) \in F[x]$, if $b(c) = 0$ then $\deg a(x) \leq \deg b(x)$.

Theorem. Let E be a field, $F \leq E$ and $c \in E$. Then a minimal polynomial of c over F exists[89] and is unique.

[89] In fact, monic generator of $\ker(\sigma_c)$ is a minimal polynomial of c over F.

Proof. Let us observe the substitution function $\sigma_c : F[x] \to E$. We have already proved that it is a homomorphism and that:

$$\ker(\sigma_c) = \{a(x) \in F[x] : \ a(c) = 0\}.$$

Existence. We have already shown that, as $F[x]$ is a PID, then there exists $p(x) \in \ker(\sigma_c)$ such that $\ker(\sigma_c) = \langle p(x) \rangle$. If $p(x)$ is not monic then it is obvious that for some $p^{-1}_{\deg p(x)} \in F$ (the inverse of the leading coefficient of $p(x)$), $p^{-1}_{\deg p(x)} p(x)$ is monic and is in $\langle p(x) \rangle$. So, we can assume that $p(x)$ already is monic. Now we will show that $p(x)$ is a minimal polynomial of c over F. It is obvious, as $p(x) \in \ker(\sigma_c)$, that $p(c) = 0$. Now, assume that there exists $b(x) \in F[x]$ such that $b(c) = 0$. That implies that $b(x) \in \ker(\sigma_c) = \langle p(x) \rangle$, i.e. there exists $q(x) \in F[x]$ such that $b(x) = p(x)q(x)$. Then $\deg b(x) = \deg p(x) + \deg q(x)$, that is equivalent to $\deg p(x) = \deg b(x) - \deg q(x)$, which implies $\deg p(x) \leq \deg b(x)$. Thus $p(x)$ satisfies all conditions to be a minimal polynomial of c over F.

Uniqueness. Assume that $q(x) \in F[x]$ is also a minimal polynomial of c over F. Then, $q(c) = 0$, so $q(x) \in \langle p(x) \rangle$. Thus, there exists $r(x) \in F[x]$ such that $q(x) = p(x)r(x)$. But, as $q(x)$ is minimal, it must be $\deg q(x) \leq \deg p(x)$. But, also as $p(x)$ is minimal, $\deg p(x) \leq \deg q(x)$. That implies $\deg p(x) = \deg q(x)$. So from $q(x) = p(x)r(x)$ we have $\deg q(x) = \deg p(x) + \deg r(x)$, i.e. $\deg q(x) - \deg p(x) = \deg r(x)$. But, $\deg q(x) = \deg p(x)$ so $\deg r(x) = 0$, i.e. $r(x) = v$, for some $v \in F$. Thus, $q(x) = vp(x)$. But, as both $p(x)$ and $q(x)$ are monic, their leading coefficients are 1. That means that $1 = v \cdot 1$ and from that follows that $v = 1$. Thus we have $q(x) = p(x)$.

□

Theorem. Let E be a field, $F \leq E$, $c \in E$ and $p(x) \in F[x]$ such that $p(c) = 0$. Then, $p(x)$ is a minimal polynomial of c over F if and only if $p(x)$ is monic and irreducible.

Proof. *Necessity.* Let $p(x)$ be a minimal polynomial of c over F. If $p(x)$ was not monic, that would be an immediate contradiction to definition of a minimal polynomial. Therefore, assume that $p(x)$ is monic, but reducible. Then, there exist $q(x), r(x) \in F[x]$, with $\deg q(x), \deg r(x) > 0$, such that $p(x) = q(x)r(x)$. As $p(c) = 0$ we have $q(c)r(c) = 0$. As $F[x]$ is an integral domain, it must be that $q(c) = 0$ or $r(c) = 0$. Assume that $q(c) = 0$, without loss of generality. Then, as $\deg p(x) = \deg q(x) + \deg r(x)$, we have $\deg q(x) = \deg p(x) - \deg r(x)$ and from that $\deg q(x) < \deg p(x)$ (as surely $r(x) \neq 0$). But, that is in contradiction that $p(x)$ is minimal, i.e. that $\deg p(x) \leq \deg t(x)$, for all $t(x) \in F[x]$ such that $t(c) = 0$ (and that also includes $q(x)$). Thus, $p(x)$ cannot be reducible and must be irreducible (and also monic).

Sufficiency. Let $p(x) \in F[x]$ be monic and irreducible with $p(c) = 0$. Assume that some $q(x) \in F[x]$ is a minimal polynomial of c over F. Then, $\ker(\sigma_c) = \langle q(x) \rangle$ by a previous theorem. So, it also must be that $p(x) \in \langle q(x) \rangle$ and there must exist $r(x) \in F[x]$ such that $p(x) = q(x)r(x)$. But, as $p(x)$ is irreducible, it must be that $r(x) = u$, for some $u \in F$ (and obviously $\deg p(x) = \deg q(x)$). Therefore, $p(x) = uq(x)$. As $q(x)$ is monic, and so is $p(x)$, the coefficients give rise to equation $1 = u \cdot 1$, so it must be $u = 1$. That gives us $p(x) = q(x)$, i.e. $p(x)$ is a minimal polynomial of c over F.

□

Definition. Let E be a field, $F \leq E$ and $c \in E$. If there exists $a(x) \in F[x] - \{0\}$ such that $a(c) = 0$, then we say that $c \in E$ is **algebraic over** F. If there does not exist $a(x) \in F[x] - \{0\}$ such that $a(c) = 0$, then we say that $c \in E$ is **transcendental over** F**.**

Definition. Let E be a field, $F \leq E$ and let $c \in E$ be algebraic over F. We define the set $F(c) = \{a(c) : \ a(x) \in F[x]\}$ and say that $F(c)$ is a **field generated by** F **and** c.

Remark. Notice that the existence of the minimal polynomial c over F automatically implies that c is also algebraic over F (as it is the root of the polynomial with coefficients in F).

Theorem. Let E be a field, $F \leq E$, $c \in E$ and $p(x)$ a minimal polynomial of c over F. Then,

$$F(c) \cong F[x]/\langle p(x) \rangle .$$

Proof. Let $\sigma_c : F[x] \to F$ be a substitution function. We have already proved that σ_c is a homomorphism. We will prove that $\langle p(x) \rangle = \ker(\sigma_c)$, where $p(x)$ is a minimal polynomial. As $p(c) = 0$, that implies $p(x) \in \ker(\sigma_c)$. We know that $\ker(\sigma_c)$ is generated by some $q(x) \in F[x]$, i.e. $\ker(\sigma_c) = \langle q(x) \rangle$ so $p(x) \in \langle q(x) \rangle$ implies $p(x) = q(x)r(x)$, for some $r(x)$. But, by a previous theorem, as $p(x)$ is a minimal polynomial of c over F, it is irreducible and it must be that $r(x) = u$ for some $u \in F$. So, we have $p(x) = q(x)u$ (with $\deg p(x) = \deg q(x)$). Take $a(x) \in \langle p(x) \rangle$. Then, $a(x) = p(x)t(x)$, for some $t(x) \in F[x]$. We have $a(x) = q(x)(ut(x))$, and as $ut(x) \in F[x]$, it's $a(x) \in \langle q(x) \rangle$, i.e. $\langle p(x) \rangle \subseteq \langle q(x) \rangle$ (although this is understandable as $p(x) \in \langle q(x) \rangle$, so the principal ideal generated by $p(x)$ is obviously a subring of $\langle q(x) \rangle$). Now, take $a(x) \in \langle q(x) \rangle$. We have $a(x) = q(x)t(x)$, for some $t(x) \in F[x]$. From $p(x) = uq(x)$, as $u \in F$, we have $q(x) = u^{-1}p(x)$. Then, $a(x) = p(x)(u^{-1}t(x))$,

so $u^{-1}t(x) \in F[x]$ and $a(x) \in \langle p(x) \rangle$, meaning $\langle q(x) \rangle \subseteq \langle p(x) \rangle$. Finally, that means $\langle q(x) \rangle = \langle p(x) \rangle$ and $\ker(\sigma_c) = \langle p(x) \rangle$. Also, $\text{ran}(\sigma_c) = \{\sigma_c(a(x)) : \ a(x) \in F[x]\} = \{a(c) : \ a(x) \in F[x]\} = F(c)$. So, by FHT, $\text{ran}(\sigma_c) \cong F[x]/\ker(\sigma_c)$, i.e. $F(c) \cong F[x]/\langle p(x) \rangle$.

□

Proposition. Let E be a field, $F \leq E$ and $c \in E$. Then $J \subseteq F(c)$, where J is a field such that $c \in J$ and $F \subseteq J$, implies[90] $F(c) = J$.

Proof. Assume that there exists $a \in F(c) - J$. As $a \in F(c)$, then $a = p(c)$, for some $p(x) \in F[x]$. But, as the coefficients of $p(x)$ are in F, then clearly $p(c) \in F \subseteq J$, which is a contradiction. Thus, $F(c) = J$.

□

Theorem (Basic theorem of field extensions). Let F be a field and $a(x) \in F[x] - \{0\}$ such that $\deg a(x) > 0$ and $a(x) = a_m x^m + \cdots + a_1 x + a_0$. There exists (an extension) field E along with injective homomorphism $\phi : F \to E$ and $c \in E$ such that $\phi(F) \leq E$ and $\overline{a}(c) = 0$, where $\overline{a}(x) = \phi(a_m)x^m + \cdots + \phi(a_1)x + \phi(a_0)$.

Proof. First, consider the case when $a(x)$ is irreducible and monic (if it is not monic, we can just observe its monic associate). Let $J = \langle a(x) \rangle$. Then, $F[x]/J$ is a field and we can take $E = F[x]/J$. Every element in E' is of the form $J + p(x)$, for some $p(x) \in F[x]$. Now, we want to have F as a subfield of the field E or some field isomorphic to it. Thus, we can consider adjusting F with a map $\phi : F \to E$ defined by $\phi(t) = J + t$, for all $t \in F$. First, we will show that ϕ is function. Take $t \in F$. Then, also $t \in F[x]$ and there exists $J + t \in E$ such that $\phi(t) = J + t$. Assume that $t_1 = t_2$. Then, $J + t_1, J + t_2 \in E$. If we take $j + t_1 \in J + t_1$, then $j + t_1 = j + t_2 \in J + t_2$, so $J + t_1 \subseteq J + t_2$. Similarly, if $j + t_2 \in J + t_2$, then, $j + t_2 = j + t_1 \in J + t_1$, which means $J + t_2 \subseteq J + t_1$. So, $J + t_1 = J + t_2$, i.e. $\phi(t_1) = \phi(t_2)$ and ϕ is a function. Now, for all $t_1, t_2 \in F$, $\phi(t_1 + t_2) = J + (t_1 + t_2) = (J + t_1) + (J + t_2) = \phi(t_1) + \phi(t_2)$ and $\phi(t_1 t_2) = J + (t_1 t_2) = (J + t_1)(J + t_2) = \phi(t_1)\phi(t_2)$ implies that ϕ is a homomorphism. Also, note that $\text{ran}(\phi) = \{J + t : \ t \in F\}$.

We will now show that it is also an injection. If $J + t_1 = J + t_2$, for some $t_1, t_2 \in \text{ran}(\phi)$ (so it must be $t_1, t_2 \in F$), we need to show $t_1 = t_2$. Well, $J + t_1 = J + t_2$ implies $t_1 - t_2 \in J$. What is the kernel of ϕ? We have $\ker(\phi) = \{t \in F : \ J + t = J\} = \{t \in F : \ t \in J\}$. So, $t_1 - t_2 \in \ker(\phi)$. We know that $\ker(\phi) \trianglelefteq F$. As F is a field, it has only trivial ideals, i.e. either $\ker(\phi) = \{0\}$ or $\ker(\phi) = F$. What if $\ker(\phi) = F$? If we took $t \in F$, we would have $t \in \ker(\phi)$ and that would give us $t \in J$. That would

[90] In other words, $F(c)$ is the **smallest field** containing F and $c \in F$.

imply $F \subseteq J = \langle a(x) \rangle$. I.e. there would exist $t \in \langle a(x) \rangle$ such that $t = a(x)q(x)$, for some $q(x)$, meaning that both $a(x)$ and $q(x)$ are zero degree polynomials, against the assumption. So, we can only have $\ker(\phi) = \{0\}$, then $t_1 - t_2 = 0$, and $t_1 = t_2$, making ϕ injective.

Now, $\text{ran}(\phi) \leq E$. Assume $a(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$. As $a_i \in F$, then $J + a_i \in \text{ran}(\phi)$. So, we can define:

$$\overline{a}(x) := x^m + (J + a_{m-1})x^{m-1} + \cdots + (J + a_1)x + (J + a_0).$$

Because $x \in F[x]$, we can take $c = J + x \in E = F[x]/J$ and observe $\overline{a}(c) = \overline{a}(J + x)$ in the following manner:

$$\overline{a}(J + x) = (J + x)^m + (J + a_{m-1})(J + x)^{m-1} + \cdots + (J + a_1)(J + x) + (J + a_0).$$

After using the fact that $(J + x)^i = J + x^i$, for all $i \in \mathbb{Z}^+$, we get:

$$\overline{a}(J + x) = (J + x^m) + (J + a_{m-1})(J + x^{m-1}) + \cdots + (J + a_1)(J + x) + (J + a_0).$$

We use the fact that $(J + a_i)(J + x^i) = J + (a_ix^i)$ and we have:

$$\overline{a}(J + x) = (J + x^m) + (J + a_{m-1}x^{m-1}) + \cdots + (J + a_1x) + (J + a_0).$$

Now, after taking the sum of all members,

$$\overline{a}(J + x) = J + (x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0).$$

But, that implies that $\overline{a}(J + x) = J + a(x)$. As $J = \langle a(x) \rangle$, we will show that $\langle a(x) \rangle + a(x) = \langle a(x) \rangle$. Take $p(x) \in \langle a(x) \rangle + a(x)$. That means that there exists $q(x) \in F[x]$ such that $p(x) = a(x)q(x) + a(x) = a(x)(q(x) + 1) \in \langle a(x) \rangle$, so $\langle a(x) \rangle + a(x) \subseteq \langle a(x) \rangle$. If we take $p(x) \in \langle a(x) \rangle$, then there exists $q(x) \in F[x]$ such that $p(x) = q(x)a(x) = q(x)a(x) - a(x) + a(x) = a(x)(q(x) - 1) + a(x) \in \langle a(x) \rangle + a(x)$, so $\langle a(x) \rangle \subseteq \langle a(x) \rangle + a(x)$, which finally implies $\langle a(x) \rangle = \langle a(x) \rangle + a(x)$, i.e. $J + a(x) = J$. So, $\overline{a}(J + x) = J + a(x) = J$ and J is a zero in $E = F[x]/J$. The difference in polynomials $\overline{a}(x)$ and $a(x)$ is merely in notation by which we immersed $a(x)$ in E, as we could have easily defined $a_i := J + a_i$ and then calculate $a_i(J + x) = J + (a_ix)$, in the same fashion. Finally, if $a(x)$ was not irreducible, it could have been factor into irreducible factors, and we could, for one of them repeat the process and that

will also be the root of $a(x) = p(x)q(x)$, where we may assume $p(x)$ is irreducible, as $a(c) = p(c)q(c) = 0q(c) = 0$.

□

Corollary. Let F be a field and $a(x) \in F[x] - \{0\}$ such that $\deg a(x) = m$, where $m \in \mathbb{Z}^+$. There exists an extension field E of F which contains all m roots of $a(x)$.

Proof. This can be obtained by repeating previous theorem m times. First we obtain a root for $a(x)$, and then find an extension of the polynimial divided by $x - c$, where c is a root in that extension, and so on.

□

Remark. One of the most notable examples would be the field of complex numbers $\mathbb{C}$, obtained by observing solutions to the equation $x^2 + 1 = 0$ in $\mathbb{R}$. This polynomial is obviously irreducible in $\mathbb{R}$ as it is of degree 2 and can only be written as a product of two polynomials of degree 1. But then it would be reducible if and only if it had a root in $\mathbb{R}$. Yet, if there was a root I in $\mathbb{R}$, it would have to satisfy $I^2 = -1$, which is impossible. Therefore, we observe extension field $\mathbb{R}[x]/\langle x^2 + 1\rangle$, which we can, because $x^2 + 1$ is irreducible in $\mathbb{R}$. Obviously $(\langle x^2 + 1\rangle + x)^2 + (\langle x^2 + 1\rangle + 1) = \langle x^2 + 1\rangle + (x^2 + 1) = \langle x^2 + 1\rangle$, and as $\langle x^2 + 1\rangle$ is a zero in $\mathbb{R}[x]/\langle x^2 + 1\rangle$, it is a root of the polynomial x^2+1. We can take $I = \langle x^2 + 1\rangle + x$. Notice that then $I^2 + (\langle x^2 + 1\rangle + 1) = \langle x^2 + 1\rangle$, i.e. I is a root of $x^2 + 1 = 0$ (with coefficients from isomorphic copy of $\mathbb{R}$). Also, the elements of the isomorphic copy of $\mathbb{R}$ look like $\langle x^2 + 1\rangle + c$, where $c \in \mathbb{R}$, while all other elements look like $\langle x^2 + 1\rangle + (ax + b)$, where $a, b \in \mathbb{R}$. Actually, all elements in $\mathbb{R}[x]/\langle x^2 + 1\rangle$ can be written as $\langle x^2 + 1\rangle + (ax + b) = (\langle x^2 + 1\rangle + a)(\langle x^2 + 1\rangle + x) + (\langle x^2 + 1\rangle + b) = (\langle x^2 + 1\rangle + a)I + (\langle x^2 + 1\rangle + b)$. It is then clear that $\mathbb{C} = \mathbb{R}(I) \cong \mathbb{R}[x]/\langle x^2 + 1\rangle$.

Problem. Prove that each of the following numbers is algebraic over $\mathbb{Q}$: (a) $\sqrt{1+\sqrt{2}}$; (b) i; (c) $\sqrt{2}$; (d) $2 + 3i$; (e) $\sqrt{1+\sqrt[3]{2}}$; (f) $\sqrt{i-\sqrt{2}}$; (g) $\sqrt{2}+\sqrt{3}$; (h) $\sqrt[3]{2}+\sqrt[3]{4}$.

Solution. (a) Let $x = \sqrt{1+\sqrt{2}}$. Then, $x^2 = 1 + \sqrt{2}$ and $x^2 - 1 = \sqrt{2}$. From that we obtain $x^4 - 2x^2 + 1 = 2$, i.e. $x^4 - 2x^2 - 1 = 0$. So, $p(x) = x^4 - 2x^2 - 1$ is the polynomial with rational coefficients such that $p\left(\sqrt{1+\sqrt{2}}\right) = 0$ and from that $\sqrt{1+\sqrt{2}}$ is algebraic over $\mathbb{Q}$. (b) We already know that, if $p(x) = x^2 + 1$, where obviously $p(x) \in Q[x]$, then $p(i) = i^2 + 1 = -1 + 1 = 1$, so i is algebraic over $\mathbb{Q}$. (c) We have $p(x) = x^2 - 2 \in \mathbb{Q}[x]$, and $p\left(\sqrt{2}\right) = 2 - 2 = 0$, so $\sqrt{2}$ is algebraic over $\mathbb{Q}$. (d) We know that $z + \overline{z}, z \cdot \overline{z} \in \mathbb{R}$ so we can use that fact and form $p(x) = (x - (2 + 3i))(x - (2 - 3i)) = x^2 - 2x + 3ix - 2x - 3ix + (2 + 3i)(2 - 3i) = x^2 - 4x + 4 - 9i^2 = x^2 - 4x + 13 \in \mathbb{Q}[x]$. Obviously $p(2 + 3i) = 0$, so $2 + 3i$ is algebraic

over $\mathbb{Q}$. (e) Let $x=\sqrt{1+\sqrt[3]{2}}$. We have $x^2=1+\sqrt[3]{2}$ and from that $x^2-1=\sqrt[3]{2}$. Then, $x^6-3x^2+3x-1=2$ and $p(x)=x^6-3x^2+3x-3$ is the polynomial in $\mathbb{Q}[x]$ such that $p\left(\sqrt[3]{2}\right)=0$. (f) Let $x=\sqrt{i-\sqrt{2}}$. We have $x^2=i-\sqrt{2}$. Then, $x^4=-1-2i\sqrt{2}+2$. So, $x^4-1=-2i\sqrt{2}$ and $x^8-2x^4+1=-8$. From that we have $x^8-2x^4+9=0$. So, $p(x)=x^8-2x^4+9\in\mathbb{Q}[x]$ and $p\left(\sqrt{i-\sqrt{2}}\right)=0$ and $\sqrt{i-\sqrt{2}}$ is algebraic over $\mathbb{Q}$.

(g) Let $x=\sqrt{2}+\sqrt{3}$. Then, $x^2=2+2\sqrt{6}+3$, i.e. $x^2-5=2\sqrt{6}$. That gives us $x^4-10x^2+1=0$. Thus, $x^4-20x^2+19=p(x)\in\mathbb{Q}[x]$ and $p\left(\sqrt{2}+\sqrt{3}\right)=0$, so $\sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$. We know that $p(x)=x^2-2$ gives $p(\sqrt{2})=2-2=0$ and that $q(x)=x^2-3$ gives $q(\sqrt{3})=3-3=0$ and that $\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbb{Q}$. Now, there is another way of proving this. Let $p=\sqrt{2}$ and $q=\sqrt{3}$. Then, $p^2=2$, $p^3=2p$, $p^4=4$ and $q^2=3$, $q^3=3q$, $q^4=9$. We have $(p+q)^4=p^4+4p^3q+6p^2q^2+4pq^3+q^4=4+8pq+36+12pq+9=49+20pq$. Also $(p+q)^2=p^2+2pq+q^2=2+2pq+3=5+2pq$ and obviously $-10(p+q)^2=-50-20pq$. Therefore, $(p+q)^4-10(p+q)^2=49+20pq-50-20pq=-1$. Finally, $(p+q)^4-10(p+q)^2+1=-1+1=0$. Thus, again we have $x^4+10x^2+1=0$ and $p+q$ is algebraic over $\mathbb{Q}$.

(h) We have $x=\sqrt[3]{2}+\sqrt[3]{4}$. We can take $x=\sqrt[3]{2}\left(1+\sqrt[3]{2}\right)$. So, $x^3=2(1+\sqrt[3]{2})^3$, i.e. $x^3=4+6\sqrt[3]{4}+6\sqrt[3]{2}+2$. That is, $x^3-6=6\left(\sqrt[3]{4}+\sqrt[3]{2}\right)$. But, that is obviously $x^3-6=6x$, i.e. $x^3-6x-6=0$. Therefore, $p(x)=x^4-6x-6\in\mathbb{Q}[x]$ with $p\left(\sqrt[3]{2}+\sqrt[3]{4}\right)=0$ proves that $\sqrt[3]{2}+\sqrt[3]{4}$ is algebraic over $\mathbb{Q}$.

Problem. Prove that: (a) $\sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$; (b) $\sqrt{\pi}$ is algebraic over $\mathbb{Q}\left(\pi^2\right)$; (c) π^2-1 is algebraic over $\mathbb{Q}\left(\pi^3\right)$.

Solution. (a) Notice that

$$\mathbb{Q}(\pi)=\left\{a_m\pi^m+\cdots+a_1\pi+a_0:\ \left(\forall i\in\{1,\ldots,m\}\right)\left(a_i\in\mathbb{Q}\right)\right\}.$$

That also means that $\mathbb{Q}\subset\mathbb{Q}\left(\pi\right)$ (obviously a proper subset as $\pi\notin\mathbb{Q}$). Therefore, $\sqrt{\pi}=x$ gives us $x^2=\pi$. Taking $p(x)=x^2-\pi$ gives us $p\left(\sqrt{\pi}\right)=\pi-\pi=0$ and also $p(x)\in\mathbb{Q}(\pi)$. Therefore, $\sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$. (b) Notice that $\pi\notin\mathbb{Q}\left(\pi^2\right)$. So, from $\sqrt{\pi}=x$ and $\pi=x^2$, we must continue to $\pi^2=x^4$. Therefore $p\left(\sqrt{\pi}\right)=0$ with $p(x)=x^4-\pi^2\in\mathbb{Q}\left(\pi^2\right)[x]$ and $\sqrt{\pi}$ is algebraic over $\mathbb{Q}\left(\pi^2\right)$. (c) Take $x=\pi^2-1$. Then, $x+1=\pi^2$ and taking $x^3+3x^2+3x+1=\pi^6$. That is equivalent to $x^3+3x^2+3x+1-\pi^6=0$. As $\pi^3\in\mathbb{Q}\left(\pi^3\right)$, then also $\pi^6=1\cdot\left(\pi^3\right)^2+0\cdot\pi^3+0\in\mathbb{Q}\left(\pi^3\right)$. So, $p\left(\pi^2-1\right)=0$, where $p(x)=x^3+3x^2+3x-1-\pi^6\in\mathbb{Q}\left(\pi^3\right)[x]$ and π^2-1 is algebraic over $\mathbb{Q}\left(\pi^3\right)$.

Problem. Find the minimum polynomial of each of the following numbers over $\mathbb{Q}$: (a) $1+2i$; (b) $1+\sqrt{2}$; (c) $1+\sqrt{2i}$; (d) $\sqrt{2+\sqrt[3]{3}}$; (e) $\sqrt{3}+\sqrt{5}$; (f) $\sqrt{1+\sqrt{2}}$.

Solution. (a) Let $p(x)=(x-1-2i)(x-1+2i)=x^2-x+2xi-x-2xi+5=x^2-2x+5$.

It is obvious that $p(1+2i)=0$, from the very way we defined $p(x)$. To show that $p(x)$ is irreducible over $\mathbb{Q}$ we will check for rational roots by observing divisors of 5. As 5 is prime, then we only need to check for $x \in \{\pm 1, \pm 5\}$. We have $p(1) = 1-2+5 = 4$, $p(-1) = 1+2+5 = 8$, $p(5) = 25-10+5 = 15+5 = 20$ and $p(-5) = 25+10+5 = 40$. Thus, $p(x)$ has no rational roots, and as it is of degree 2, it is irreducible over $\mathbb{Q}$. That also implies that $p(x) = x^2 - 2x + 5$ is a minimal polynomial of $1+2i$ over $\mathbb{Q}$.

(b) Let $x = 1+\sqrt{2}$. Then, $x-1 = \sqrt{2}$. From that we have $x^2 - 2x + 1 = 2$, i.e. $x^2 - 2x - 1 = 0$. That means that we can take $p(x) = x^2 - 2x - 1$ and $p\left(1+\sqrt{2}\right) = 0$. To show that $p(x)$ is irreducible over $\mathbb{Q}$ we observe possible roots $x \in \{\pm 1\}$. Then, $p(1) = 1-2-1 = -2$ and $p(-1) = 1+2-1 = 2$. Thus $p(x)$ is a minimal polynomial if $1+\sqrt{2}$ over $\mathbb{Q}$.

(c) Let $x = 1+\sqrt{2i}$. Then, $x-1 = \sqrt{2i}$ and $(x-1)^2 = 2i$. From that we have $(x-1)^4 = 2$, i.e. $p(x) = (x-1)^4 - 2 = 0$. Take $x \to x+1$. Then, $t(x) = p(x+1) = x^4 - 2$. Remember that, if $p(x+1)$ is irreducible, then so is $p(x)$. For, if it were that $p(x+1)$ was irreducible and $p(x)$ reducible, we could write $p(x) = q(x)r(x)$, but also $p(x+1) = q(x+1)r(x+1)$ (the detailed discussion is in a proposition above, the only thing left to argue is that linear transformation preservs degree of a polynomial) which would be a contradiction. So, let's observe $t(x) = x^4 - 2$. We have $2|-2$, $2^2 = 4 \nmid -2$, $2|0$ (coefficients for x, x^2 and x^3) and $2 \nmid 1$ (leading coefficient of $t(x)$), so by Eisenstein's criterion, polynomial $t(x)$ is irreducible over $\mathbb{Q}$, but then so is $p(x+1)$ and $p(x)$. Thus, the minimal polynomial for $1+\sqrt{2i}$ over $\mathbb{Q}$ is $(x-1)^4 - 2$.

(d) Let $x = \sqrt{2+\sqrt[3]{3}}$. Then, $x^2 = 2+\sqrt[3]{3}$ and $\left(x^2-2\right)^3 = 3$. So, let $p(x) = (x^2-2)^3 - 3 = x^6 - 6x^4 + 12x^2 - 11$. In $\mathbb{Z}/3\mathbb{Z}[x]$ we have $\overline{p}(x) = x^6 - \overline{11} = x^6 + \overline{1}$. For now, we will not prove irreducibility of this polynomial - although it is irreducible: by Fermat's little theorem, it has no roots, because for all $\overline{a} \in \{\overline{1}, \overline{2}\}$, we have $\overline{a}^2 = \overline{1}$; so, $\overline{p}(\overline{a}) = \left(\overline{a}^2\right)^3 + \overline{1} = \overline{1}^2 + \overline{1} = \overline{2}$, for all $\overline{a} \in \mathbb{Z}/3\mathbb{Z} - \{\overline{0}\}$, and it is obvious that $\overline{p}(\overline{0}) = \overline{1}$). So, I will, for now exclude the check for reduction of $\overline{p}(x)$ as a product of two polynomials, either when they're of degree 2 and 3, or when they're both of degree 3.

(e) Let $x = \sqrt{3}+\sqrt{5}$. We have $x^2 = 3+2\sqrt{15}+5$ and $x^2 - 8 = 2\sqrt{15}$. From this we have $x^4 - 16x^2 + 64 = 60$, i.e. $p(x) = x^4 - 16x^2 + 4$. The possible roots are ± 1, ± 2 and ± 4. We can see that $p(\pm 1) = 1 - 16 + 4 = -11 \neq 0$, $p(\pm 2) = 16 - 16 \cdot 4 + 4 = 20 - 64 = -44 \neq 0$ and $p(\pm 4) = 4^4 - 16 \cdot 16 + 4 = 4^2 \cdot 4^2 - 4^2 \cdot 4^2 + 4 = 4 \neq 0$. Therefore, we must only check if $x^4 - 16x^2 + 4 = (x^2 + ax + b)(x^2 + cx + d)$. From this we have $bd = 4$, $ad + bc = 0$, $ac + b + d = -16$ and $a + c = 0$. Thus, $c = -a$ and we have $ad - ab = 0$, i.e. $a(d-b) = 0$. Thus, either $a = 0$, or $b = d$. If $a = 0$, we have $b + d = -16$ and $bd = 4$. This gives us, after multiplying with d, $bd + d^2 = -16d$, i.e. $d^2 + 16d + 4 = 0$. We can take $q(x) = x^2 + 16x + 4$. Then, all we need to do is check for roots in $\{\pm 1, \pm 2, \pm 4\}$. We see that $q(1) = 5 + 16 = 21$, $q(-1) = 5 - 16 = -11$, $q(2) = 8+32 = 40$, $q(-2) = 8-32 = -24$, $q(4) = 20+64 = 84$, $q(-4) = 20-64 = -44$.

Thus, $d^2+16d+4=0$ has no rational solutions, and there does not exist $d\in\mathbb{Q}$ that would satisfy $bd=4$ and $b+d=-16$. So, we may assume $d-b=0$, i.e. $b=d$. But, then $bd=4$ implies $b^2=4$ and $2b=-16$. We would have $b=d=\pm 2$, but then $-a^2+2\cdot(\pm 2)=-16$, i.e. $a^2=16+\pm 4$. First case would yield $a^2=12$ and second $a^2=20$. Such rational numbers do not exist. Thus, $p(x)$ is irreducible.

(f) Let $x=\sqrt{1+\sqrt{2}}$. Then, $x^2-1=\sqrt{2}$ and $x^4-2x^2+1=2$. From that we have $p(x)=x^4-2x^2-1$. The possibilities for roots lie in ± 1. It is obvious that $p(\pm 1)=1-2-1=-2$. Thus, we are left with $x^4-2x^2-1=(x^2+ax+b)(x^2+cx+d)$. So, $bd=-1$, $ad+bc=0$, $ac+b+d=-2$ and $a+c=0$. We have $c=-a$ and that implies $ad-ab=0$, i.e. $a(d-b)=0$. If $a=0$, we have $b+d=-2$ and $bd=-1$. After multiplying former equality by d we have $d^2+2d-1=0$. Let $q(x)=x^2+2x-1$. Then, solutions lie in ± 1. We have $q(1)=1+2-1=2$ and $q(-1)=1-2-1=-2$. Thus, there does not exist such $d\in\mathbb{Q}$ and it must be that $b-d=0$, i.e. $b=d$. From that we have, as $bd=-1$, that $d^2=-1$, which is again impossible. Thus, $p(x)$ is irreducible.

Problem. Show that the minimal polynomial of $\sqrt{2}+i$ is: (a) $x^2-2x\sqrt{2}+3$ over $\mathbb{R}$; (b) x^4-2x^2+9 over $\mathbb{Q}$; (c) $x^2-2ix-3$ over $\mathbb{Q}(i)$.

Solution. (a) If $p(x)=x^2-2x\sqrt{2}+3$ were reducible over $\mathbb{R}$, we would have $a^2-2a\sqrt{2}+3=0$, for some $a\in\mathbb{R}$ and we would have $p(x)=(x-a)q(x)$, for some $q(x)\in\mathbb{R}[x]$, $\deg q(x)=1$. But, as $p\left(\sqrt{2}+i\right)=2+2i\sqrt{2}-1-4-2i\sqrt{2}+3=0$ and $p\left(\sqrt{2}-i\right)=2-2i\sqrt{2}-1-4+2i\sqrt{2}+3=0$, so either $x-(\sqrt{2}+i)|x-a$ or $x-(\sqrt{2}+i)|q(x)$. As $x-(\sqrt{2}+i)|x-a$ would imply $a=\sqrt{2}+i\notin\mathbb{R}$, it must be that $q(x)=x-(\sqrt{2}+i)$ (due to $\deg q(x)=1$). Then, we have $p(x)=(x-a)(x-(\sqrt{2}+i))$. But, as $x-(\sqrt{2}-i)$ is also a root, and $x-(\sqrt{2}-i)\nmid x-(\sqrt{2}+i)$ (due to obvious reasons), it must be that $x-(\sqrt{2}-i)|x-a$ which would impliy $a=\sqrt{2}-i\notin\mathbb{R}$. Thus, $p(x)$ is irreducible over $\mathbb{R}$ and $p(\sqrt{2}+i)=0$, so $p(x)$ is the minimal polynomial of $\sqrt{2}+i$ over $\mathbb{R}$.

(b) Let $p(x)=x^4-2x^2+9$. Then, $p\left(\sqrt{2}+i\right)=4+8i\sqrt{2}-12-4i\sqrt{2}+1-4-4i\sqrt{2}+2+9=16+8i\sqrt{2}-16-8i\sqrt{2}=0$. Now, the only possible roots are ± 1, ± 3 and ± 9. We have $p(\pm 1)=1-2+9=8$, $p(\pm 3)=81-18+9=54$, $p(\pm 9)=6561-162+9=6408$. Thus, the only possibility is that $x^4-2x+9=(x^2+ax+b)(x^2+cx+d)$. From that we have $bd=9$, $ad+bc=0$, $ac+b+d=-2$ and $a+c=0$. From the latter expression we get $c=-a$, so from $ad+bc=0$ we have $ad-ab=0$, i.e. $a(d-b)=0$. Thus, as $\mathbb{Q}$ is an integral domain, we have $a=0$ or $d=b$. If $a=0$, then $b+d=-2$ and $bd=9$. Multiplying former equality by d we have $d^2+2d+9=0$. Let $q(x)=x^2+2x+9$. The possible roots are ± 1, ± 3, ± 9. We have $q(1)=1+9+2=12$, $q(-1)=1+9-2=8$, $q(3)=9+9+6=24$, $q(-3)=9+9-6=12$, $q(9)=81+9+18=108$ and $q(-9)=81+9-18=72$. As $q(x)$ has no roots in $\mathbb{Q}$, then $d^2+2d+9=0$ has

no rational solutions and this case is impossible. Now, if $b = d$, we have $d^2 = 9$, i.e. $b = d = \pm 3$. Also, $-a^2 + 2 \cdot (\pm 3) = -2$, that is, $a^2 = 2 + \pm 6$. In the first case we have $a^2 = 8$ and in the second case $a^2 = -4$. Both cases are impossible (in $\mathbb{Q}$ of course), so $p(x)$ is irreducible and is a minimal polynomial of $\sqrt{2} + i$ over $\mathbb{Q}$.

(c) Let $p(x) = x^2 - 2ix - 3$. Then, $p(\sqrt{2}+i) = 2 + 2i\sqrt{2} - 1 - 2i\sqrt{2} + 2 - 3 = 0$. To show that $p(x)$ is irreducible over $\mathbb{Q}(i)$, we will assume that $x^2 - 2ix - 3 = (x + a + bi)(x + c + di)$, where $a, b, c, d \in \mathbb{Q}$. Then, $(a + c) + i(b + d) = -2i$ and $ac - bd + i(ad + bc) = -3$ So, $a + c = 0$, $b + d = -2$, $ac - bd = -3$ and $ad + bc = 0$. First equality gives us $c = -a$, so we have $ad - ab = 0$, i.e. $a(d - b) = 0$. As $\mathbb{Q}$ is an integral domain, $a = 0$ or $b = d$. If $a = 0$, then $bd = -3$ and $d + b = -2$. If we multiply latter equality by d, we get $d^2 + 2d - 3 = 0$. We can see that $d \in \{1, -3\}$. If $d = 1$, then $b = -3$. But, then $ac - bd = -3$ would imply $0 - (-3) \cdot 1 = 3 \neq -3$, so this case is impossible. If $d = -3$, then $b = 1$, and again we would have $0 - 1 \cdot (-3) = 3 \neq -3$. Assume $b = d$. Then, $d^2 = -3$, which is impossible. Thus, $p(x)$ is irreducible over $\mathbb{Q}(i)$, which implies $p(x)$ is the minimal polynomial of $\sqrt{2} + i$ over $\mathbb{Q}(i)$.

Problem. Find the minimum polynomial of the following numbers over the indicated fields:

(a) $\sqrt{3} + i$ over $\mathbb{R}$; over $\mathbb{Q}$; over $\mathbb{Q}(i)$; over $\mathbb{Q}\left(\sqrt{3}\right)$;

(b) $\sqrt{i + \sqrt{2}}$ over $\mathbb{R}$; over $\mathbb{Q}$; over $\mathbb{Q}(i)$; over $\mathbb{Q}\left(\sqrt{2}\right)$.

Solution. (a) Let $x = \sqrt{3} + i$. Then, $x - \sqrt{3} = i$ and $x^2 - 2x\sqrt{3} + 3 = -1$. Thus, we can take $p_1(x) = x^2 - 2x\sqrt{3} + 4$. To show that it is irreducible over $\mathbb{R}$, we will note that the root of $p_1(x)$ is also $\sqrt{3} - i$, and that the factorization is then $p_i(x) = (x - \sqrt{3} - i)(x - \sqrt{3} + i)$. So, if there was a real root c of $p_1(x)$, we would have $x - c | x - \sqrt{3} - i$ or $x - c | x - \sqrt{3} + i$, which would be a contradiction in each case (as c would be complex).

Now, over $\mathbb{Q}$, we need to get rid of both $\sqrt{3}$ and i. First we have $x - \sqrt{3} = i$. Then, $x^2 - 2x\sqrt{3} + 3 = -1$ and $2x\sqrt{3} = 4 + x^2$, which gives us $12x^2 = 16 + 8x^2 + x^4$, and we can take $x^4 - 4x^2 + 16 = 0$. Let $p_2(x) = x^4 - 4x^2 + 16$. Then, the roots are in $\{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$. We have $p_2(\pm 1) = 1 - 4 + 16 = 13$, $p_2(\pm 2) = 16$, $p_2(\pm 4) = 208$, $p_2(\pm 8) = 3856$ and $p_2(\pm 16) = 64528$ so $p_2(x)$ has no roots in $\mathbb{Q}$. But, maybe it can be reduced as $x^4 - 4x^2 + 16 = (x^2 + ax + b)(x^2 + cx + d)$. Then we have $a + c = 0$, $ac + b + d = -4$, $ad + bc = 0$ and $bd = 16$. We have $c = -a$ and then $ad - ab = 0$, i.e. $a(d - b) = 0$. As $\mathbb{Q}$ is an integral domain, either $a = 0$ or $d = b$. Assume $a = 0$. Then, $b + d = -4$ and $bd = 16$. We multiply former equality by d and get $d^2 + 4d + 16 = 0$. This polynomial is irreducible over $\mathbb{Q}$ as its discriminant is $D = 16 - 64 < 0$. Thus, this is an impossible case, as there does not exist such d. Assume $b = d$. Then we have $b + b = -4$, i.e. $2b = -4$, which gives us $b = -2$. But, from $bd = 16$, we have $b^2 = 4 \neq 16$, which is again impossible.

In this case, we don't have to worry about i. Let $x = \sqrt{3} + i$. Then, $x - i = \sqrt{3}$ and we have $x^2 - 2ix - 1 = 3$, i.e. $p_3(x) = x^2 - 2ix - 4$. Assume that $x^2 - 2ix - 4 = (x+(a+bi))(x+(c+di))$. Then, $a+c+i(b+d) = -2i$ and $ac-bd+i(bc+ad) = -4$. From the former equality we have $b + d = -2$, $a + c = 0$ and from the latter $bc + ad = 0$ and $ac - bd = -4$. Therefore, because $c = -a$, we have $-a^2 - bd = -4$ and $-ab + ad = 0$, i.e. $a(d - b) = 0$. As $\mathbb{Q}$ is an integral domain, either $a = 0$ or $d = b$. If $a = 0$, we have $-bd = -4$, i.e. $bd = 4$. Also we have $b + d = -2$, so multiplying that by d gives us $d^2 + 2d + 4 = 0$. The discriminant of this equation is $D = 4 - 16 < 0$, so there are no real, and consequently, no rational solutions. Thus, it must be $b = d$. But then $b^2 = 4$, i.e. $b = \pm 2$, but $b + b = -2$ gives us $2b = -2$, i.e. $b = -1 \neq \pm 2$, which is again impossible.

Finally, in $\mathbb{Q}(\sqrt{3})$, we disregard $\sqrt{3}$. Let $x = \sqrt{3} + i$. Then, $x - \sqrt{3} = i$ and $x^2 - 2x\sqrt{3} + 3 = -1$, i.e. $p_4(x) = x^2 - 2x\sqrt{3} + 4$. All $\sqrt{3}^m$ yield either a rational number or, if $m = 2k + 1$, $\sqrt{3^{2k} \cdot 3} = 3^k\sqrt{3}$, so in $\mathbb{Q}(\sqrt{3})$, every number is of the form $a + b\sqrt{3}$, where $a, b \in \mathbb{Q}$. Assume $x^2 - 2x\sqrt{3} + 4 = (x + (a + b\sqrt{3}))(x + (c + d\sqrt{3}))$. We have $a + c + (b + d)\sqrt{3} = -2\sqrt{3}$ and $ac + 3bd + (ad + bc)\sqrt{3} = 4$. So, $a + c = 0$, $b + d = -2$, $ac + 3bd = 4$ and $ad + bc = 0$. From $c = -a$ we have $ad - ab = 0$, i.e. $a(d - b) = 0$. As $\mathbb{Q}$ is an integral domain, $a = 0$ or $b = d$. Assume $a = 0$. Then, $3bd = 4$, i.e. $bd = \frac{4}{3}$. Also, as $b+d = -2$, multiplying that by d gives us $d^2+2d+\frac{4}{3} = 0$. The discriminant is $4-\frac{16}{3} = 4-5\frac{1}{3} < 0$, and there are no real, and by that no rational, solutions. Therefore, it must be $d = b$. But then $b^2 = \frac{4}{3}$ and $2b = -2$, i.e. $b = -1$. It is obvious that this is a contradiction because $1 \neq \frac{4}{3}$.

(b) Let $x = \sqrt{i + \sqrt{2}}$. We need to get rid of i only. Thus, $x^2 = i + \sqrt{2}$ and we have $x^2 - \sqrt{2} = i$. After squaring that we get $x^4 - 2x^2\sqrt{2} + 2 = -1$ and we can take $p_1(x) = x^4 - 2x^2\sqrt{2} + 3$. It is obvious that $\pm\sqrt{i + \sqrt{2}}$ will be roots of $p_1(x)$. But, due to squaring in $x^2 - \sqrt{2} = i$, we will also have the roots $\pm\sqrt{-i + \sqrt{2}}$. As all roots are complex, the existence of a real root would imply that a real number equals a complex number, which would be a contradiction. The only other possibility is that $p_1(x)$ can be written as a product of two degree 2 irreducible polynomials. But, that would imply that these irreducible polynomials over $\mathbb{R}$ would have to divide some product of two $x - c$, where c is a root. But, these products will always contain i, as multiplication will only remove the square root over i, but not i. Let $x = \sqrt{i + \sqrt{2}}$. We need to get rid of $\sqrt{2}$ and i to be able to find a minimal polynomial over $\mathbb{Q}$. We have $x^2 = i + \sqrt{2}$ and $x^2 - \sqrt{2} = i$. Then, $x^4 - 2x^2\sqrt{2} + 2 = -1$. Then, $x^4 + 3 = 2x^2\sqrt{2}$. Squaring that gives us $x^8 + 6x^4 + 9 = 8x^4$, i.e. $x^8 - 2x^4 + 9 = 0$. Thus, $p_2(x) = x^8 - 2x^4 + 9$. For now we will not check irreducibility. Let $x = \sqrt{i + \sqrt{2}}$. We need to get rid of $\sqrt{2}$ only to find a minimal polynomial over $\mathbb{Q}(i)$. Then, $x^2 = i + \sqrt{2}$ and $x^2 - i = \sqrt{2}$. Thus, $x^4 - 2ix^2 - 1 = 2$ and we can take $p_3(x) = x^4 - 2ix^2 - 3$. Let $x = \sqrt{i + \sqrt{2}}$. Over $\mathbb{Q}\left(\sqrt{2}\right)$ we need only remove i. So, we have $x^2 = i + \sqrt{2}$ and $x^2 - \sqrt{2} = i$. Finally, $x^4 - 2x^2\sqrt{2} + 2 = -1$ and we can take $p_4(x) = x^4 - 2x^2\sqrt{2} + 3$. We will not check

irreducibility for $p_2(x)$, $p_3(x)$ and $p_4(x)$. It is too cumbersome for me now.

Problem. For each of the following polynomials $p(x)$, find a number a such that $p(x)$ is the minimum polynomial of a over $\mathbb{Q}$: (a) x^2+2x-7; (b) x^4+2x^2-1; (c) x^4-10x^2+1.

Solution. (a) We can use the formula for the quadratic equation and get $x_{1,2}=\frac{-2\pm\sqrt{28}}{2}$. Thus, we can take $a=\sqrt{7}-1$. Then $a^2+2a-7=0$ and x^2+2x-7 is irreducible over $\mathbb{Q}$ (the divisors ±1 and ±7 are obviously not roots). (b) Let $t=x^2$. Then we have $x^4+2x^2-1=t^2+2t-1=0$ and $t_{1,2}=\frac{-2\pm\sqrt{8}}{2}$. We can take $t=\sqrt{2}-1$ and then $a=\sqrt{\sqrt{2}-1}$. (c) Let $t=x^2$. Then, $t^2-10t+1=0$ and $t_{1,2}=\frac{10\pm\sqrt{96}}{2}$ and we can take $t=5+2\sqrt{6}$ and $a=\sqrt{5+2\sqrt{6}}$.

Problem. Find a monic irreducible polynomial $p(x)$ such that $\mathbb{Q}[x]/\langle p(x)\rangle$ is isomorphic to: (a) $\mathbb{Q}\left(\sqrt{2}\right)$; (b) $\mathbb{Q}\left(1+\sqrt{2}\right)$; (c) $\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$.

Solution. (a) Let $p(x)=x^2-2$. Then, $\sqrt{2}^2-2=2-2=0$ and $p(x)$ is irreducible over $\mathbb{Q}$ (for ±1 we have $p(\pm1)=1-2=-1$ and $p(\pm2)=4-2=2$, so there are no roots over $\mathbb{Q}$). Thus, by the previous theorem, $\mathbb{Q}[x]/\langle x^2-2\rangle\cong\mathbb{Q}[x]\left(\sqrt{2}\right)$. (b) Let $x=1+\sqrt{2}$. Then, $x-1=\sqrt{2}$ and we have $x^2-2x+1=2$ and we can take $p(x)=x^2-2x-1$. Polynomial $p(x)$ is obviously irreducible as $p(1)=1-2-1=-2$ and $p(-1)=1+2-1=2$. By the previous theorem, $\mathbb{Q}/\langle x^2-2x-1\rangle\cong\mathbb{Q}[x]\left(1+\sqrt{2}\right)$. (c) Let $x=\sqrt{1+\sqrt{2}}$. Then, $x^2=1+\sqrt{2}$. We have $x^2-1=\sqrt{2}$ which gives us $x^4-2x^2+1=2$ and we can take $p(x)=x^4-2x^2-1$. We will not check irreducibility of this polynomial for now, as extensive work of testing irreducibility has already been done in previous chapter. By previous theorem we have $\mathbb{Q}[x]/\langle x^4-2x^2-1\rangle\cong\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$.

Proposition. Let F be a field, $p(x)\in F[x]$ irreducible polynomial with $\deg p(x)=m$, $m\in\mathbb{Z}^+-\{1\}$ and let $c\in E$, where E is an extension field of F, such that $p(c)=0$. Let $a\in F(c)$. Then, there exists a unique $r(x)\in F[x]$ with $\deg r(x)<m$, such that a can be written as $r(c)$.

Proof. As c is a root of irreducible polynomial $p(x)$, by previous theorem we have $F(c)\cong F[x]/\langle p(x)\rangle$. Then, there exists an isomorphism $\phi:F(c)\to F[x]/\langle p(x)\rangle$ and, as $a\in F(c)$, we have $\phi(a)=\langle p(x)\rangle+t(x)$, for some $t(x)\in F[x]$. Thus, $\phi(a)=\langle p(x)\rangle+t(x)$.

Recall that this result is obtained by a surjective homomorphism, or the substitution function, $\sigma_c:F[x]\to F(c)$ whose kernel is $p(x)$. The function is defined with $\sigma_c(q(x))=q(c)$, for all $q(x)\in F[x]$. As $a\in F(c)$, and σ_c is surjective, there exists $t(x)\in F[x]$ such that $\sigma_c(t(x))=a$, i.e. $t(c)=a$. Now, if the degree of $t(x)$ is less then m, we simply take

$r(x) = t(x)$. If it is not, by division algorithm, there exist $q(x), r(x) \in F[x]$ such that $t(x) = q(x)p(x) + r(x)$, with $0 \leq \deg r(x) < \deg p(x) = m$. As $t(x) \in F[x]$, there exists $\langle p(x)\rangle + t(x) \in F[x]/\langle p(x)\rangle$. But, then $\langle p(x)\rangle + t(x) = \langle p(x)\rangle + [q(x)p(x) + r(x)] = \langle p(x)\rangle + r(x)$, implying $t(x) - r(x) \in \langle p(x)\rangle$. As $\langle p(x)\rangle$ is the kernel of σ_c, that means that $\sigma_c(t(x) - r(x)) = 0$, i.e. $t(c) - r(c) = 0$. That finally implies $t(c) = r(c)$, that is $a = r(c)$.

□

Problem. Explain why there are exactly four elements in $\mathbb{Z}/2\mathbb{Z}[x]/\left\langle x^2 + x + \overline{1}\right\rangle$. List these four elements, and give their addition and multiplication tables.

Solution. Let $p(x) = x^2 + x + \overline{1}$. If $a \in \mathbb{Z}/2\mathbb{Z}[x]/\langle p(x)\rangle$, then there exists $t(x) \in \mathbb{Z}/2\mathbb{Z}[x]$ such that $a = \langle p(x)\rangle + t(x)$. By division algorithm there exist $q(x), r(x)$ such that $t(x) = q(x)p(x) + r(x)$, where $0 \leq \deg r(x) < 2$. Thus, $r(x) = Ax + B$, for some $A, B \in \mathbb{Z}/2\mathbb{Z}$, and $t(x) = q(x)p(x) + (Ax + B)$. That implies $a = \langle p(x)\rangle + t(x) = \langle p(x)\rangle + [q(x)p(x) + (Ax + B)] = \langle p(x)\rangle + [Ax + B]$. As $A, B \in \mathbb{Z}/2\mathbb{Z}$, there are only four options: $\langle p(x)\rangle$, $\langle p(x)\rangle + \overline{1}$, $\langle p(x)\rangle + x$ and $\langle p(x)\rangle + [x + \overline{1}]$. Let us use the following notation: $Ax + B := \langle p(x)\rangle + [Ax + B]$. Also, note that $x^2 = (x^2 + x + \overline{1}) - (x + \overline{1}) = (x^2 + x + \overline{1}) + (x + \overline{1})$. Thus, $x^2 + x = (x^2 + x + \overline{1}) + (\overline{1})$, $(x + \overline{1})^2 = x^2 + \overline{1} = (x^2 + x + \overline{1}) + (x)$. The addition and multiplication tables are:

$+$	$\overline{0}$	$\overline{1}$	x	$x+\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	x	$x+\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$x+\overline{1}$	x
x	x	$x+\overline{1}$	$\overline{0}$	$\overline{1}$
$x+\overline{1}$	$x+\overline{1}$	x	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	x	$x+\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	x	$x+\overline{1}$
x	$\overline{0}$	x	$x+\overline{1}$	$\overline{1}$
$x+\overline{1}$	$\overline{0}$	$x+\overline{1}$	$\overline{1}$	x

Problem. Describe $\mathbb{Z}/2\mathbb{Z}[x]/\langle x^3 + x + 1\rangle$.

Solution. Let $F = \mathbb{Z}/2\mathbb{Z}[x]/\left\langle x^3 + x + \overline{1}\right\rangle$ are of the form $\langle p(x)\rangle + [Ax^2 + Bx + C]$, so there are eight possible configurations of coefficients. Due to shortness of space, we can denote $\overline{ABC} := \langle p(x)\rangle + [Ax^2 + Bx + C]$. The addition is then the same as in binary arithmetic, but the digits do not carry. The table for addition is:

$+$	$\overline{0}$	$\overline{1}$	$\overline{10}$	$\overline{11}$	$\overline{100}$	$\overline{101}$	$\overline{110}$	$\overline{111}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{10}$	$\overline{11}$	$\overline{100}$	$\overline{101}$	$\overline{110}$	$\overline{111}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{11}$	$\overline{10}$	$\overline{101}$	$\overline{100}$	$\overline{111}$	$\overline{110}$
$\overline{10}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{110}$	$\overline{111}$	$\overline{100}$	$\overline{101}$
$\overline{11}$	$\overline{11}$	$\overline{10}$	$\overline{1}$	$\overline{0}$	$\overline{111}$	$\overline{110}$	$\overline{101}$	$\overline{100}$
$\overline{100}$	$\overline{100}$	$\overline{101}$	$\overline{110}$	$\overline{111}$	$\overline{0}$	$\overline{1}$	$\overline{10}$	$\overline{11}$
$\overline{101}$	$\overline{101}$	$\overline{100}$	$\overline{111}$	$\overline{110}$	$\overline{1}$	$\overline{0}$	$\overline{11}$	$\overline{10}$
$\overline{110}$	$\overline{110}$	$\overline{111}$	$\overline{100}$	$\overline{101}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$
$\overline{111}$	$\overline{111}$	$\overline{110}$	$\overline{101}$	$\overline{100}$	$\overline{11}$	$\overline{10}$	$\overline{1}$	$\overline{0}$

The multiplication is somewhat cumbersome, although we essentialy multiply the elements and divide them with $x^3 + x + \overline{1}$ and get the remainder. Thus we get (I did it with some help from the computer):

$+$	$\overline{0}$	$\overline{1}$	$\overline{10}$	$\overline{11}$	$\overline{100}$	$\overline{101}$	$\overline{110}$	$\overline{111}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{10}$	$\overline{11}$	$\overline{100}$	$\overline{101}$	$\overline{110}$	$\overline{111}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{10}$	$\overline{11}$	$\overline{100}$	$\overline{101}$	$\overline{110}$	$\overline{111}$
$\overline{10}$	$\overline{0}$	$\overline{10}$	$\overline{100}$	$\overline{110}$	$\overline{11}$	$\overline{1}$	$\overline{111}$	$\overline{101}$
$\overline{11}$	$\overline{0}$	$\overline{11}$	$\overline{110}$	$\overline{101}$	$\overline{111}$	$\overline{100}$	$\overline{1}$	$\overline{10}$
$\overline{100}$	$\overline{0}$	$\overline{100}$	$\overline{11}$	$\overline{111}$	$\overline{110}$	$\overline{10}$	$\overline{101}$	$\overline{1}$
$\overline{101}$	$\overline{0}$	$\overline{101}$	$\overline{1}$	$\overline{100}$	$\overline{10}$	$\overline{111}$	$\overline{11}$	$\overline{110}$
$\overline{110}$	$\overline{0}$	$\overline{110}$	$\overline{111}$	$\overline{1}$	$\overline{101}$	$\overline{11}$	$\overline{10}$	$\overline{100}$
$\overline{111}$	$\overline{0}$	$\overline{111}$	$\overline{101}$	$\overline{10}$	$\overline{1}$	$\overline{110}$	$\overline{100}$	$\overline{11}$

Problem. Describe $\mathbb{Z}/3\mathbb{Z}[x]/\left\langle x^3 + x^2 + \overline{2}\right\rangle$.

Solution. In this exercise we have a field with 3^3, i.e. twenty seven, elements. I will not draw out the addition and multiplication table.

Proposition. Let F be any field and $c, d \in E - \{0\}$, where E is an extension field of F. Then:

1. If c is algebraic over F, so are $c + k$ and kc, for all $k \in F$;
2. If c is algebraic over F, so is c^{-1};
3. If cd is algebraic over F, then c is algebraic over $F(d)$;
4. If $c + d$ is algebraic over F, then c is algebraic over $F(d)$;

Proof. *Ad* 1. Assume that c is algebraic over F. Then there exists $p(x) \in F[x]$ such that $p(c) = 0$. As $k \in F$, then $p(x - k) \in F[x]$. Also, $p(c + k - k) = p(c) = 0$, thus $c + k$ is algebraic over F, as it is the root of the polynomial $p(x - k)$. Also, as $k \in F$, then $k^{-1} \in F$ and we have $p(k^{-1}x) \in F[x]$. Also, $p(k^{-1}ck) = p(k^{-1}kc) = p(1c) = p(c) = 0$, so kc is algebraic over F. *Ad* 2. As c is algebraic over F, then there exists $p(x) \in F[x]$ such that $p(c) = 0$. Assume that $p(x) = p_m x^m + \cdots + p_1 x + p_0$. Then, $p_m c^m + \cdots + p_1 c + p_0 = 0$. Multiplying that by c^{-m} gives us $p_m + \cdots + p_1 c^{1-m} + p_0 c^{-m} = 0$, and terms are of the form $p_i c^{i-m} = p_i \left(c^{-1}\right)^{m-i}$, for all $i \in \{1, \ldots, m\}$. Thus, we get that $p_m + p_{m-1}c^{-1} + \cdots + p_2 \left(c^{-1}\right)^{m-2} + p_1 \left(c^{-1}\right)^{m-1} + p_0 \left(c^{-1}\right)^m = 0$. Taking $\overline{p}(x) = p_0 x^m + \cdots + p_{m-1}x + p_m$ it is easy to see that $\overline{p}(c^{-1}) = 0$, and, as $\overline{p}(x) \in F[x]$, c^{-1} is algebraic over F. *Ad* 3. Assume that cd is algebraic over F. Then there exists $p(x) \in F[x]$ such that $p(cd) = 0$. Assume that $p(x) = p_m x^m + \cdots + p_1 x + p_0$. Then, $p(cd) = p_m (cd)^m + \cdots + p_1 (cd) + p_0 = (p_m d^m) c^m + \cdots + (p_1 d) c + p_0 = 0$. As $p_i d^i \in F(d)$,

then $p(xd) \in F(d)[x]$ and $p(cd) = 0$, which implies c is algebraic over $F(d)$. *Ad* 4. Assume that $c + d$ is algebraic over F. Then, there exists $p(x) \in F[x]$ such that $p(c + d) = 0$. It is easy to see that $p(x + d) \in F(d)$ and that, because $p(c + d) = 0$, we have that c is algebraic over $F(d)$.

□

Proposition. Let F be a field and K an extension of F. Let $a \in K$. Then, the minimal polynomial of a over F is of degree 1 if and only if $a \in F$.

Proof. *Necessity.* Assume that the minimal polynomial of a over F is of degree 1. Let that polynomial be $p(x) = x + p_0$ (it has to be monic). Then, $p(a) = 0$, i.e. $a + p_0 = 0$. Then, $a = -p_0$. As $p_0 \in F$, by definition, then also $a = -p_0 \in F$. *Sufficiency.* Let $a \in F$. Then, we will show that $p(x) = x - a$ is a minimal polynomial of a over F. We have $p(a) = a - a = 0$, and $p(x) \in F$ because $a \in F$. Also, $p(x)$ is monic. As $\deg p(x) = 1$, there can be no polynomial of a lesser degree whose root is a. Therefore $x - a \in F[x]$ is the minimal polynomial of a over F.

□

Problem. Name a field (not $\mathbb{R}$ or $\mathbb{C}$) which contains a root of $x^5 + 2x^3 + 4x^2 + 6$.

Solution. Let $p(x) = x^5 + 2x^3 + 4x^2 + 6$. We have $2 \nmid 1$, $2|0$, $2|4$, $2|6$ and $2^2 = 4 \nmid 6$, so by Eisenstein's criterion $p(x)$ is irreducible over $\mathbb{Q}$. Thus, $\mathbb{Q}/\langle x^5 + 2x^3 + 4x^2 + 6\rangle$ is a field and $\langle p(x)\rangle + x \in F[x]$ is the root of $\overline{p}(x)$. We have $p(\langle p\rangle + x) = \langle p(x)\rangle$ as in the basic theorem for field extensions.

Problem. Prove that $\mathbb{Q}(1 + i) \cong \mathbb{Q}(1 - i)$ and $\mathbb{Q}\left(\sqrt{2}\right) \ncong \mathbb{Q}\left(\sqrt{3}\right)$.

Solution. The minimal polynomial of $1 + i$ over $\mathbb{Q}$ is obtained by setting $x = 1 + i$. Then, $x - 1 = i$ and $x^2 - 2x + 1 = -1$, which gives us $p(x) = x^2 - 2x + 2$. Similarly, $x = 1 - i$ gives us $x - 1 = -i$ and $x^2 - 2x + 1 = -1$. That means that $q(x) = x^2 - 2x + 2$ is the minimal polynomial of $1 - i$ over $\mathbb{Q}$. Thus, $\mathbb{Q}(1 + i) \cong \mathbb{Q}/\langle x^2 - 2x + 2\rangle \cong \mathbb{Q}(1 - i)$, which gives us $\mathbb{Q}(1 + i) = \mathbb{Q}(1 - i)$.

Assume that there exists an isomorphism $\phi : \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{Q}\left(\sqrt{3}\right)$. For all $x \in \operatorname{dom}(\phi)$, we have $\phi(x^2) = \phi(xx) = \phi(x)\phi(x) = (\phi(x))^2$. Thus, if some $x \in \operatorname{dom}(\phi)$ is a square then it must be also that $\phi(x)$ is a square in $\operatorname{cod}(\phi)$. Take $x = \sqrt{2}$. We have that $x^2 = 2$ in $\mathbb{Q}\left(\sqrt{2}\right)$. So, it also must be that $\phi(x^2) = \phi(2)$, i.e. $\phi(x)^2 = \phi(2)$. Note that $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1)$, and as 1 is a unit, then it must be $\phi(1) = 1$, and so $\phi(2) = 1 + 1 = 2$. Therefore there must exist some $y \in \mathbb{Q}\left(\sqrt{3}\right)$ such that $y^2 = 2$. But, as $y \in \mathbb{Q}\left(\sqrt{3}\right)$, it is of the form $y = a + b\sqrt{3}$ and we have $y^2 = a^2 + 2ab\sqrt{3} + 3b^2$.

So, as $y^2 = 2$, we have $a^2 + 2ab\sqrt{3} + 3b^2 = 2$, i.e. $(a^2 + 3b^2 - 2) + (2ab)\sqrt{3} = 0$. That is equivalent to $(2ab)\sqrt{3} = 2 - a^2 - 3b^2$. Assume $a = 0$. Then, $0 = 2 - 3b^2$, i.e. $\frac{2}{3} = b^2$. This is impossible because there does not exist such rational b (we can check through the divisors of the free term for rational solutions; we will find none). Assume $b = 0$. Then, $0 = 2 - a^2$, i.e. $2 = a^2$. This is again impossible as there does not exist a rational number which, squared, yields 2 (elementary proof). Assume $a \neq 0$ and $b \neq 0$. Then we can divide $(2ab)\sqrt{3} = 2 - a^2 - 3b^2$ with $2ab$ and get $\sqrt{3} = \frac{2-a^2-3b^2}{2ab}$, which would imply, as the expression on the right-hand side is rational, that $\sqrt{3} \in \mathbb{Q}$, which is a contradiction. Therefore, our assumption that there exists an isomorphism ϕ from $\mathbb{Q}\left(\sqrt{2}\right)$ to $\mathbb{Q}\left(\sqrt{3}\right)$ has brought about a contradiction and it must be that $\mathbb{Q}\left(\sqrt{2}\right) \ncong \mathbb{Q}\left(\sqrt{3}\right)$.

Proposition. Let F be a field. If $p(x) \in F[x]$ is irreducible and $\deg p(x) = 2$, then $F[x]/\langle p(x)\rangle$ contains both roots of $p(x)$.

Proof. Assume that F is a field and that $p(x) = x^2 + ax + b \in F[x]$ is irreducible. Then, $F[x]/\langle p(x)\rangle \cong F(c)$, where $c^2 + ac + b = 0$. Multiplying that equality with c^{-2} (which exists in $F(c)$ as $F(c)$ is a field) gives us $1 + ac^{-1} + bc^{-2} = 0$. Multiplying with b gives us $b + a(bc^{-1}) + \left(b^2\left(c^{-1}\right)^2\right) = 0$, i.e. $b + a(bc^{-1}) + \left(bc^{-1}\right)^2 = 0$. It is obvious that bc^{-1} is another root of $p(x)$. Another way of proving that is taking $p(-a - c) = (a^2 + 2ac + c^2) + (-a^2 - ac) + b = c^2 + ac + b = 0$.

□

Remark. Let F and E be fields. Recall the definition of $F(a)$. It is a field such that $F \subseteq F(a)$, $a \in F(a)$ and, $F \subseteq E$ and $a \in E$ implies $F(a) \subseteq E$. Similarly, $F(a, b)$ is a field such that $F \subseteq F(a, b)$, $a, b \in F$ and, $F \subseteq E$ and $a, b \in E$ implies $F(a, b) \subseteq E$.

Proposition. Let F be a field, $k \in F - \{0\}$ and $c, d \in E - \{0\}$, where E is some extension field of F. Then:

1. $F(c) = F(c + k)$;
2. $F(c) = F(kc)$;
3. $F(c^2) \subseteq F(c)$ and the converse is not necessarily true;
4. $F(c + d) \subseteq F(c, d)$ and the converse is not necessarily true.

Proof. *Ad* 1. As $k \in F$, then $c + k \in F(c)$. So, we have $c + k \in F(c)$ and $F \subseteq F(c)$, which implies $F(c + k) \subseteq F(c)$. Similarly, $c \in F(c + k)$ (we can take $c = (c + k) - k$, due to $k \in F$) and $F \subseteq F(c + k)$, which implies $F(c + k) \subseteq F(c)$. From that follows $F(c) = F(c + k)$. *Ad* 2. Again, as $k \in F$, we have $kc \in F(c)$. Also, $F \subseteq F(c)$ by

definition of $F(c)$, but that implies that $F(kc) \subseteq F(c)$. Also, $c \in F(kc)$ (because $c = k^{-1}(kc)$; this works because $k \in F$) and $F \subseteq F(kc)$, so $F(c) \subseteq F(kc)$ and $F(c) = F(kc)$. *Ad* 3. We have $c^2 \in F(c)$ (because obviously $c^2 = c^2 + 0c + 0$) and $F \subseteq F(c)$, finally implies $F(c^2) \subseteq F(c)$. The converse is not necessarily true, a counterexample would be $\mathbb{Q} = \mathbb{Q}(2) \subseteq \mathbb{Q}(\sqrt{2})$, but $\sqrt{2} \notin \mathbb{Q}$. *Ad* 4. Notice that $F(c, d)$ is a field containing c and d so it also must contain their sum, i.e. $c+d \in F(c, d)$. Also, $F \subseteq F(c, d)$, by definition, which with former expression gives us $F(c + d) \subseteq F(c, d)$. The converse is not necessarily true because it is not necessary that $c, d \in F(c + d)$; a good counterexample is $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, but obviously $\sqrt{2} \notin \mathbb{Q}(\sqrt{2} + \sqrt{3})$. We would have $a_1(\sqrt{2} + \sqrt{3}) + a_0 = \sqrt{2}$, and from that $\sqrt{2}(a_1 - 1) + a_1\sqrt{3} = -a_0$, but $-a_0 \in \mathbb{Q}$.

□

Proposition. Let F be a field, $k \in F$, $c \in E$, where E is some extension of F, let $p(x) \in F[x]$. Then,

1. $c + k$ is a root of $p(x)$ if and only if c is a root of $p(x + k)$;
2. kc is a root of $p(x)$ if and only if c is a root of $p(kx)$.

Proof. *Ad* 1. *Necessity.* Assume $c+k$ is a root of $p(x)$. Then, $p(c+k) = 0$. From this it is evident that c is a root of $p(x + k)$, because $p(c + k) = 0$. *Sufficiency.* Assume c is a root of $p(x + k)$. Then, $p(c + k) = 0$, which is the same as saying $c + k$ is a root of $p(x)$. *Ad* 2. *Necessity.* Assume kc is a root of $p(x)$. Then, $p(kc) = 0$, which means that c is a root of $p(kx)$. *Sufficiency.* Let c be a root of $p(kx)$. Then, $p(kc) = 0$, meaning that kc is a root of $p(x)$.

□

Proposition. Let F be a field, $k \in F$ and let $p(x) \in F[x]$ be an irreducible polynomial. Then:

1. $F[x]/\langle p(x + k)\rangle \cong F[x]/\langle p(x)\rangle$;
2. $F[x]/\langle p(kx)\rangle \cong F[x]/\langle p(x)\rangle$.

Proof. *Ad* 1. Let $c \in E$ be a root of $p(x+k)$, where E is an extension of F. Then, $c+k$ is a root of $p(x)$. From the previuos proposition we have that $F[x]/\langle p(x + k)\rangle \cong F(c)$ and $F[x]/\langle p(x)\rangle \cong F(c + k)$. From the previous proposition, as $k \in F$, we have $F(c+k) = F(c)$, so $F[x]/\langle p(x + k)\rangle \cong F(c) = F(c+k) \cong F[x]/\langle p(x)\rangle$. *Ad* 2. Let E be an extension of F and $c \in E$ a root of $p(kx)$. Then, by previous proposition, kc is a root of $p(x)$. Thus, by previous proposition, $F[x]/\langle p(kx)\rangle \cong F(c)$ and $F[x]/\langle p(x)\rangle \cong F(kc)$. By previous proposition, $F(c) = F(kc)$, so $F[x]/\langle p(x)\rangle \cong F(kc) = F(c) \cong F[x]/\langle p(kx)\rangle$.

□

Problem. Prove that $\mathbb{Z}/11\mathbb{Z}[x]/\left\langle x^2+\overline{1}\right\rangle \cong \mathbb{Z}/11\mathbb{Z}[x]\left\langle x^2+x+\overline{4}\right\rangle$.

Solution. Let us observe $p(x+\overline{k}) = (x+\overline{k})^2+\overline{1}$. From that we have $p(x+\overline{k}) = x^2+\overline{2k}x+\overline{k^2+1}$. If we compare that with $x^2+x+\overline{4}$, we get $\overline{2k}=\overline{1}$ and $\overline{k^2+1}=\overline{4}$. From former equality we get, as $\overline{2}\cdot\overline{6}=\overline{12}=\overline{1}$, that $\overline{k}=\overline{6}$; substituting that in latter equality we have $\overline{36+1}=\overline{4}$, i.e. $\overline{37}=\overline{4}$, which is correct, due to the fact that $37\equiv 4 \pmod 1$1. So, if $p(x)=x^2+\overline{1}$, then $p(x+\overline{6})=x^2+x+\overline{4}$, and we have $\mathbb{Z}/11\mathbb{Z}[x]/\langle p(x)\rangle \cong \mathbb{Z}/11\mathbb{Z}[x]/\left\langle p(x+\overline{6})\right\rangle$, from the previous proposition.

Problem. If a is a root of x^2-2 and b is a root of x^2-4x+2, then $\mathbb{Q}(a)\cong\mathbb{Q}(b)$.

Solution. Let us take $(x+k)^2-2 = x^2+(2k)x+(k^2-2)$. Then, $2k=-4$ gives us $k=-2$. Substituting that into k^2-2 gives us $4-2=2$. So, $(x-2)^2-2=x^2-4x+2$. From the previous proposition, as $-2\in\mathbb{Q}$ and as a is a root of x^2-2, we have $\mathbb{Q}/\langle x^2-2\rangle\cong\mathbb{Q}(a)$. Also, as b is a root of $(x-2)^2-2$, we have $\mathbb{Q}/\langle x^2-4x+2\rangle\cong\mathbb{Q}(b)$. Then, by the previous proposition, $\mathbb{Q}(a)=\mathbb{Q}/\langle x^2-2\rangle\cong\mathbb{Q}/\langle x^2-4x+2\rangle=\mathbb{Q}(b)$.

Problem. If a is a root of x^2-2 and b is a root of $x^2-\frac{1}{2}$, then $\mathbb{Q}(a)\cong\mathbb{Q}(b)$.

Solution. Let a be a root of $p(x)=x^2-2$. Then, as $p(2x)=4x^2-2=4\left(x^2-\frac{1}{2}\right)$, b is a root of $p(2x)$. By previous proposition, as $2\in\mathbb{Q}$, we have $\mathbb{Q}(a)=\mathbb{Q}/\langle p(x)\rangle\cong\mathbb{Q}/\langle p(2x)\rangle=\mathbb{Q}(b)$.

Definition. If the minimal polynomial of c over F has degree 2, we say that $F(c)$ is a **quadratic extension** of F. Also, if $b^2=a$ for some $a,b\in F$, we say that b is the square root of a and write $b=\sqrt{a}$. If, for some $a\in F$, there does not exist $b\in F$ such that $b^2=a$, then we say that a is a non-square in F.

Proposition. If F is a field with $\operatorname{char}(F)\neq 2$, any quadratic extension of F is of the form $F(\sqrt{a})$, for some $a\in F$.

Proof. Let $q(x)$ be the minimal polynomial of c over F. Then, $F(c)\cong F[x]/\langle q(x)\rangle$ and we have $q(c)=0$. But, we have that $\deg q(x)=2$, so $q(x)=x^2+a_1x+a_0$, where $a_1,a_0\in F$. Then, $0=q(c)=c^2+a_1c+a_0$. Let $\operatorname{char}(F)=p$, $p\neq 2$. From that we have $q(x+k)=(x+k)^2+a_1(x+k)+a_0$ and $q(x+k)=x^2+2kx+k^2+a_1x+a_1k+a_0=x^2+x(2k+a_1)+(k^2+a_1k+a_0)$. Let $k=\left(\frac{p-1}{2}\right)\cdot(-a_1)$. That will work because $p\neq 2$, so $\frac{p-1}{2}\in\mathbb{Z}$. Then, $q\left(x+\left(\frac{p-1}{2}\right)a_1\right)=x^2+x(2(\frac{p-1}{2})a_1+a_1)+\left(\left(\frac{p-1}{2}\right)a_1\right)^2+a_1\left(\left(\frac{p-1}{2}\right)a_1\right)+a_0$. Let $-a=\left(\left(\frac{p-1}{2}\right)a_1\right)^2+a_1\left(\left(\frac{p-1}{2}\right)a_1\right)+a_0$. Then, $q\left(x+\left(\frac{p-1}{2}\right)a_1\right)=x^2+x((p-1)a_1+a_1)-a$. Notice that $(p-1)a_1+a_1=pa_1=0$, because $\operatorname{char}(F)=p$. Then, $q\left(x+\left(\frac{p-1}{2}\right)a_1\right)=$

$x^2 - a$. Let $r(x) = x^2 - a$. As $\left(\frac{p-1}{2}\right) \in F$, then, by a previous proposition, $F[x]/\langle r(x)\rangle \cong F[x]/\langle q(x)\rangle$ and we have, because $\sqrt{a}^2 - a = a - a = 0$, we have $F[x]/\langle x^2 + a\rangle \cong F(\sqrt{a})$.

□

Proposition. Let F be a finite field with $\mathrm{char}(F) \neq 2$ and let F^* be a multiplicative group of F. Let $a, b \in F$. If a and b are non-squares in F, then ab^{-1} is a square in F.

Proof. Let $S = \{x^2 : x \in F^*\}$. It is obvious that $S \subseteq F^*$, as F^* is a group and therefore closed with respect to multiplication (and also squaring). Then, if $x^2, y^2 \in S$, we have, $x^2y^2 = (xy)^2$. That is true because F is a field, which implies that F^* is Abelian. Thus, $S \leq F^*$. As F is a field, if $x \in F$, then $-x \in F$. That is also true for F^* (which actually contains all elements of F, but without zero, as F is a field). Then, either $x \neq -x$ or $x = -x$. Can it be the latter case? Assume $x = -x$, i.e. $x + x = 0$. That would imply $2x = 0$, that is, $\mathrm{char}(F) = 2$, which is a contradiction. So we construct $S(x_i)$ inductively. Take $x_1 \in F^*$. Then, $S(x_1) = \{x_1, -x_1\}$ (from that, as $x_1 \neq -x_1$, $|S(x_1)| = 2$). Then, we construct $S(x_2)$ by taking $x_2 \in F^* - S(x_1)$ and letting $S(x_2) = \{x_2, -x_2\}$. Thus we continue by taking $x_{i+1} \in F^* - (S(x_1) \cup \cdots \cup S(x_i))$ with $S(x_{i+1}) = \{x_{i+1}, -x_{i+1}\}$. As F^* is finite, the construction ends with partition $S(x_i) \cap S(x_j) = \emptyset$, if $i \neq j$ and $F^* = S(x_1) \cup \cdots \cup S(x_m)$ for some $m \in \mathbb{Z}^+$. That implies $F^* = 2 \cdots m$. Now, observe that $(S(x_i))^2 \subseteq S$ and we have $S(x_i) = \{x_i^2\}$, as $x_i^2 = (-x_i)^2$. Can it be that $(S(x_i))^2 = (S(x_j))^2$ for some $(S(x_i)) \neq (S(x_j))$? That would imply $x_i^2 = x_j^2$, i.e. $x_i^2 - x_j^2 = 0$. Then, $(x_i - x_j)(x_i + x_j) = 0$. As F^* is also an integral domain, either $x_i - x_j = 0$ or $x_i + x_j = 0$. From the former condition we get $x_i = x_j$, and from the latter $x_i = -x_j$, both a contradiction to $(S(x_i)) \neq (S(x_j))$. Thus, $|S| = (S(x_1))^2 + \cdots + (S(x_m))^2 = m$. Therefore, $[F^* : S] = \frac{|F^*|}{|S|} = \frac{2m}{m} = 2$. Take $a, b \in F^*$ that are not squares, i.e. $a, b \in F^* - S$. Then assume $Sa = S$. That would imply $a \in S$, a contradiction. Same goes for b. Thus, we have $Sa \neq S$ and $Sb \neq S$. As the index of S in F^* is 2, $Sa \neq Sb$ would imply that it is at least 3. So, it must be $Sa = Sb$, and from that we have $ab^{-1} \in S$. In other words, ab^{-1} is a square.

□

Theorem. Any two quadratic extensions of a finite field are isomorphic.

Proof. Let $F(\sqrt{a})$ and $F\left(\sqrt{b}\right)$ be quadratic extensions of field F. Then, $F(\sqrt{a}) \cong F/\langle x^2 - a\rangle$ and $F\left(\sqrt{b}\right) \cong F/\langle x^2 - b\rangle$. Let $p(x) = x^2 - a$ and $q(x) = x^2 - b$. We want $p(k\sqrt{b}) = 0$. Thus, $p(k\sqrt{b}) = (k\sqrt{b})^2 - a = k^2b - a$. Then, $k^2b - a = 0$ implies $k^2b = a$, i.e. $k^2 = ab^{-1}$. Then, as ab^{-1} is a square (followed by a, b non-squares), we can denote $k = \sqrt{ab^{-1}}$. Therefore, $\sqrt{ab^{-1}} \in F^*$ and $p(\sqrt{ab^{-1}}x)$ is defined so that

$p(\sqrt{ab^{-1}}\sqrt{b}) = 0$. Also, by a previous proposition, we have $F(\sqrt{a}) \cong F/\langle p(x)\rangle \cong F/\left\langle p(\sqrt{ab^{-1}}x)\right\rangle \cong F\left(\sqrt{b}\right)$. Therefore, $F(\sqrt{a}) \cong F\left(\sqrt{b}\right)$.

□

Remark. Notice that the only non-squares in $\mathbb{R}$ are in $\mathbb{R}^- = \{-x \in \mathbb{R} : \ x > 0\}$. Thus, if $x, y \in \mathbb{R}^-$, then $\frac{x}{y} > 0$ and it is a square. Thus, any two simple extensions of $\mathbb{R}$ are isomorphic (and isomorphic to $\mathbb{C}$). That can be seen from the fact that the proof from above, although for finite fields, actually depends on the fact that ab^{-1} is a square if a and b are non squares. The different notation here is that ab^{-1} is $\frac{a}{b}$.

Proposition. Let $F \trianglelefteq E$, $\operatorname{char}(F) \neq 2$, and let $a, b \in E$. Let $p(x)$ be minimal polynomial of a, and of b, over F such that $\deg p(x) = 2$. Then, $F(a) = F(b)$.

Proof. If $a = b$, we are done. Assume $a \neq b$ and $p(x) = x^2 + kx + l$ for some $k, l \in F$. Then, $p(a) = 0 = p(b)$, i.e. $a^2+ka+l = b^2+kb+l$. From this we get $a^2-b^2+ka-kb = 0$. This is equivalent to $(a-b)(a+b)+k(a-b) = 0$, or $(a-b)(a+b+k) = 0$. As $a \neq b$, then $a - b \neq 0$, so it must be $a + b + k = 0$, i.e. $a = -(b + k)$. Let us examine $F(b)$. As $k \in F \subseteq F(b)$, then $a = -(b + k) \in F(b)$. As $F(b)$ contains a and F, and as $F(a)$ is the smallest field containing a and F, it has to be $F(a) \subseteq F(b)$. In the same way, from $a = -(b + k)$ we can get $-(a + k) = b$, we get $b \in F(a)$, meaning $F(b) \subseteq F(a)$. That gives us $F(a) = F(b)$.

□

Proposition. Let F be a field, and let c be transcendental over F. Then:

1. $\{a(c) : \ a(x) \in F[x]\}$ is an integral domain isomorphic to $F[x]$;
2. $F(c)$ is the field of quotients[91] of $\{a(c) : \ a(x) \in F[x]\}$, and is isomorphic to $F(x)$, the field of quotients of $F[x]$;
3. $c + k$, c^m and kc, where $k \in F$, $m \in \mathbb{Z}^+$, are transcendental over F;
4. Every element in $F(c) - F$ is transcendental over F.

Proof. Let $A = \{a(c) : \ a(x) \in F[x]\}$. *Ad* 1. Let $f : A \to F[x]$ be a mapping defined with $f(a^m c^m + \cdots + a_1 c + a_0) = a^m x^m + \cdots + a_1 x + a_0$. First, we will show that f is a well-defined function. It is obvious that for any $a(c) \in A$ there exists $a(x) \in F[x]$. Now,

[91] Not quotient field! Field of quotients Q for this problem would look like:

$$Q = \left\{ \frac{a(c)}{b(c)} : \ (a(x) \in F[x]) \wedge (b(x) \neq 0) \right\}.$$

assume that $a^m c^m + \cdots + a_1 c + a_0 = b^n c^n + \cdots + b_1 c + b_0$. Assume that $m = n$, allowing some coefficients to be equal to zero. Then, $c^m(a_m - b_m) + \cdots + c(a_1 - b_1) + (a_0 - b_0) = 0$. If it were that all a_i and b_i are not equal, c would be root of the polynomial $x^m(a_m - b_m) + \cdots + x(a_1 - b_1) + (a_0 - b_0)$, which would contradict the fact that c is transcendental over F. Thus, it must be that $a_i = b_i$ and $m = n$ (so this would be a zero polynomial, excluded from definition of what it means for an element to be algebraic). Now, the surjectivity and injectivity are rather straightforward. Same thing for $f(a(c)b(c)) = a(x)b(x)$ and $f(a(c) + b(c)) = a(x) + b(x)$. *Ad* 2. Let Q be the field of quotients. Then it is obvious that $c \in Q$ and $F \subseteq Q$. But, $F(c)$ is the smallest field containing F and c, so it must be $F(c) \subseteq Q$. As every element in Q is of the form $\frac{a(c)}{b(c)}$. But, as F and c are in $F(c)$, then $a(c)$ and $b(c)$ are in $F(c)$. Also[92], $[b(c)]^{-1}$ is in $F(c)$ and we have $a(c)[b(c)]^{-1} \in F(c)$, implying $Q \subseteq F(c)$. Therefore, we have $F(c) = Q$. From the previous problem we have that $A = \{a(c) : \ a(x) \in F[x]\}$ is isomorphic to $F[x]$, i.e. $A \cong F[x]$. As these integral domains are isomorphic, then so are their fields of quotients. *Ad* 3. Let c be transcendental over F and let $k \in F$. Assume that $c + k$ is algebraic over F. Then there exists $p(x) \in F[x]$ such that $p(c+k) = 0$. By a previos proposition, $c+k$ is root of $p(x)$ if and only if c is root of $p(x+k)$. As $p(x+k) \in F[x]$, due to $k \in F$, this is a contradiction to the assumption that c is transcendental over F. Similarly, if $p(kc) = 0$, then c is root of $p(kx) \in F[x]$, and that cannot be as c is transcendental over F. Finally, assume c^m is algebraic over F. Then, for some $p(x) \in F[x]$, we have $p(c^m) = 0$, i.e. $p_n\,(c^m)^n + \cdots + p_1 c^m + p_0 = 0$. But, that is equivalent to $p_n c^{mn} + \cdots + p_1 c^m + p_0 = 0$, which implies that c is root of $p(x^m) \in F[x]$, again a contradiction to assumption that c is transcendental over F. *Ad* 4. Assume that $t \in F(c) - F$ is algebraic over F. Then, there exists $p(x) \in F[x]$ such that $p(t) = 0$. As $t = \frac{a(c)}{b(c)}$, then $p(t)$ is of the form $p(t) = p_m t^m + \cdots + p_1 t + p_0 = 0$. Multiplying everything by $b(c)^m$ gives us $0 = p_m[a(c)]^m + p_{m-1}[a(c)]^{m-1}b(c) + \cdots + p_1 a(c)[b(c)]^{m-1} + p_0[b(c)]^m$. That would imply that all $[a(c)]^k[b(c)]^{m-k} \in F$. But that would mean that $a(c)$ and $b(c)$ cannot contain c (due to previous proposition), and that they have to be in F. Then also $t \in F$, which is contrary to our assumption.

□

Proposition. Let F be a field and $a(x), b(x) \in F[x]$. Then, if $a(x)$ and $b(x)$ have a common root c in some extension of F, they have a common factor of positive degree in $F[x]$.

Proof. Let E be an extension of F where $c \in E$. Then, we observe $\sigma_c : F[x] \to E$. As $a(c) = b(c) = 0$, then $a(x), b(x) \in \ker(\sigma_c) = \langle p(x) \rangle$, for some $p(x) \in F[x]$. Thus, $a(x) = p(x)r(x)$ and $b(x) = p(x)s(x)$. Their common factor is $p(x)$, which is obviously of positive degree. Assume that $\deg p(x) = 0$. Then, $p(x) = a$, for some $a \in F$.

[92] I will elaborate on this more in the future; for now I consider it to be rather intuitive.

Therefore, $\langle a \rangle = \{aq(x) : \ q(x) \in F[x]\}$ and we have $\langle a \rangle = F[x]$. Thus, $\sigma_c(a(x)) = 0$, for all $a(x)$. So, also $\sigma_c(x) = 0$, i.e. $c = 0$, which is impossible as that would mean $c \in F$, not in an extension of F. Therefore, $\deg p(x) > 0$.

□

Proposition. Let F be a field and $a(x), b(x) \in F[x]$. Let K be any extension of F. Then, $\gcd(a(x), b(x)) = 1$ in $F[x]$ if and only if $\gcd(a(x), b(x)) = 1$ in $K[x]$.

Proof. *Necessity.* Assume $\gcd(a(x), b(x)) = 1$ in $F[x]$. Then by Bezout's lemma, $a(x)p(x)+b(x)q(x) = 1$, for some $p(x), q(x) \in F[x]$. But, as $p(x), q(x) \in F[x]$, i.e. their coefficients are in $F \leq K$, then they are also in K, so $p(x), q(x) \in K[x]$. Thus we have $\gcd(a(x), b(x)) = 1$, by Bezout's lemma. *Sufficiency.* Assume that $\gcd(a(x), b(x)) = 1$ in $K[x]$. Then there exist $p(x), q(x) \in K[x]$ such that $a(x)p(x)+b(x)q(x) = 1$. Assume that $\gcd(a(x), b(x)) = g(x)$ in $F[x]$. Then, there exist $r(x), s(x) \in F[x]$ such that $a(x) = g(x)r(x)$ and $b(x) = g(x)s(x)$. But, then also $g(x), r(x), s(x) \in K[x]$, as $F[x] \subseteq K[x]$. So, from Bezout's equality we get $g(x)r(x)p(x)+g(x)s(x)q(x) = 1$. That is equivalent to $g(x)[r(x)p(x) + s(x)q(x)] = 1$ and we have $g(x)|1$. Thus, $a(x)$ and $b(x)$ are also relatively prime in $F[x]$.

□

Definition. Let $a(x) = a_m x^m + \cdots + a_1 x + a_0 \in F[x]$, where F is a field. The **derivative** of $a(x)$ is defined as $a'(x) = ma_m x^{m-1} + \cdots + 2a_2 x + a_1$.

Proposition. Let F be a field, $\lambda, \mu \in F$ and $a(x), b(x) \in F[x]$. Then:

1. $[\lambda a(x) + \mu b(x)]' = \lambda a'(x) + \mu b'(x)$;
2. $[a(x)b(x)]' = a'(x)b(x) + a(x)b'(x)$.

Proof. Let $a(x) = a_m x^m + \cdots + a_1 x + a_0$ and $b(x) = b_m x^m + \cdots + b_1 x + b_0$ (allowing some b_i to equal zero so to not force degree equality). *Ad* 1. Then, $[a(x) + b(x)]' = [(a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)]' = m(a_m + b_m)x^{m-1} + \cdots + (a_1 + b_1) = (ma_m x^{m-1} + \cdots + a_1) + (mb_m x^{m-1} + \cdots + b_1) = a'(x) + b'(x)$. Also, $[\lambda a(x)]' = [\lambda a_m x^m + \cdots + \lambda a_1 x + \lambda a_0]' = \lambda m a_m x^{m-1} + \cdots + \lambda a_1 = \lambda(ma_m x^{m-1} + \cdots + a_1) = \lambda a'(x)$. Therefore, $[\lambda a(x)+\mu b(x)]' = [\lambda a(x)]' + [\mu b(x)]' = \lambda a'(x) + \mu b'(x)$. *Ad* 2. Assume $a(x) = a_{m+1}x^{m+1} + A(x)$, when necessary. First, we will prove $[\lambda x^k a(x)]' = k\lambda x^{k-1}a(x) + \lambda x^k a'(x)$. Assume the statement is true for $\deg a(x) = 0$. Then, $a(x) = a_0$ and the result directly follows from previos problem. Then, assume the statement is true when $\deg a(x) = m$. Then, $[\lambda x^k a_{m+1}x^{m+1} + \lambda x^k A(x)]' = [(\lambda a_{m+1})x^{k+m+1}]' + [\lambda x^k A(x)]' = (k+m+1)(\lambda a_{m+1})x^{k+m} + k\lambda x^k A'(x) + k\lambda x^{k-1}A(x) = k(\lambda a_{m+1})x^{k+m} + (m+1)(\lambda a_{m+1})x^{k+m} +$

$\lambda x^k A'(x) + k\lambda x^{k-1} A(x) = \lambda k x^{k-1}[a_{m+1}x^{m+1} + A(x)] + x^k \lambda[(m+1)a_{m+1}x^m + A'(x)] = \lambda k x^{k-1} a(x) + x^k \lambda a'(x)$. This proves the first part needed. Then, note that $[a_0 b_0]' = 0 = 0 + 0 = a_0 0 + b_0 0 = a_0[b_0]' + [a_0]' b_0$. Assume $\deg a(x) \geq \deg b(x)$ and assume the statement is true for all polynomials with degree less than or equal to m. Then, $[a_{m+1}x^{m+1}b(x) + A(x)b(x)]' = [a_{m+1}x^{m+1}b(x)] + [A(x)b(x)]' = (m+1)a_{m+1}x^m b(x) + a_{m+1}x^{m+1}b'(x) + A(x)b'(x) + A'(x)b(x) = b(x)[(m+1)a_{m+1}x^m + A'(x)] + b'(x)[a_{m+1}x^{m+1} + A(x)] = b(x)a'(x) + b'(x)a(x)$.

□

Proposition. Let F be a field such that $\operatorname{char}(F) = 0$. Let $a(x) \in F[x]$ such that $a'(x) = 0$. Then, $a(x)$ is a constant polynomial. If $\operatorname{char}(F) \neq 0$, then this is not necessarily true.

Proof. Let $a(x) \in F[x]$ and $a'(x) = 0$. Assume that $a(x)$ is a non constant polynomial, i.e. $a(x) = a_m x^m + \cdots a_1 x + a_0$. Then, $a'(x) = m a_m x^{m-1} + \cdots + a_1 = 0$. That would imply that $i a_i = 0$, for all $i \in \{1, \ldots, m\}$. But, that is impossible because $\operatorname{char}(F) = 0$ and $a(x)$ must be a constant polynomial. If $\operatorname{char}(F) \neq 0$, for example in $\mathbb{Z}/5\mathbb{Z}$, we have $[x^5 + \overline{1}]' = (5 \cdot \overline{1})x^4 = \overline{5}x^4 = \overline{0}x^4 = \overline{0}$.

□

Problem. Find the derivatives of the following polynomials in $\mathbb{Z}/5\mathbb{Z}[x]$: (a) $x^6 + \overline{2}x^3 + x + \overline{1}$; (b) $x^5 + \overline{3}x^2 + \overline{1}$; (c) $x^{15} + \overline{3}x^{10} + \overline{4}x^5 + \overline{1}$.

Solution. (a) We have $[x^6 + \overline{2}x^3 + x + \overline{1}]' = (6 \cdot \overline{1})x^5 + (3 \cdot \overline{2})x^2 + (1 \cdot \overline{1}) = \overline{6}x^5 + \overline{6}x^2 + \overline{1} = x^5 + x^2 + \overline{1}$. (b) Following in the similar fashion, we may conclude that $[x^5 + \overline{3}x^2 + \overline{1}]' = \overline{5}x^5 + \overline{6}x = \overline{0} + x = x$. (c) Same as before, $[x^{15} + \overline{3}x^{10} + \overline{4}x^5 + \overline{1}]' = \overline{15}x^{14} + \overline{30}x^9 + \overline{20}x^4 = \overline{0} + \overline{0} + \overline{0} = \overline{0}$.

Proposition. If F is a field with $\operatorname{char}(F) = p$, for some $p \in P$ and if $a(x) \in F[x]$ with $a'(x) = 0$, then the only nonzero terms of $a(x)$ are of the form $a_{kp}x^{kp}$, for some $k \in \mathbb{Z}^+$.

Proof. Assume that some $a_i x^i \neq 0$ (meaning $a_i \neq 0$). Then, the derivative of that term is $(i \cdot a_i)x^{i-1}$. As $a'(x) = 0$, then $i \cdot a_i = 0$. As $a_i \neq 0$, then $\operatorname{char}(F) \,|i$, so it must be $i = \operatorname{char}(F)\, k$, for some $k \in \mathbb{Z}^+$. That implies $i = pk$, and $a_i x^i = a_{pk} x^{pk}$.

□

Definition. Let $a(x) \in F[x]$ and let K be an extension of field F. An element $c \in K$ is called a **multiple root** of $a(x)$ if $(x - c)^m | a(x)$, for some $m \in \mathbb{Z}^+ - \{1\}$.

Theorem. A polynomial $a(x) \in F[x]$ has a multiple root in some extension of F if and only if there exists $b(x) \in F[x]$, $\deg b(x) > 0$, such that $b(x)|a(x)$ and $b(x)|a'(x)$.

Proof. *Necessity.* Assume that a polynomial $a(x) \in F[x]$ has a multiple root $c \in K$. Then, $(x-c)^m|a(x)$, for some $m \in \mathbb{Z}^+ - \{1\}$. That implies that $a(x) = (x-c)^m q(x)$, for some $q(x) \in K[x]$. Then, $a'(x) = [(x-c)^m q(x)]' = m(x-c)^{m-1}q(x) + (x-c)^m q'(x)$. As $m > 1$, then $m - 2 \geq 0$ and we can extract $(x-c)$ from $a'(x)$. We have $a'(x) = (x-c)[m(x-c)^{m-2} + (x-c)^{m-1}q'(x)]$ and that implies $(x-c)|a'(x)$, i.e. c is a root of $a'(x)$. Then, by a previous proposition, there exists $b(x) \in F[x]$, $\deg b(x) > 0$ such that $b(x)|a(x)$ and $b(x)|a'(x)$. *Sufficiency.* Assume $b(x)|a(x)$ and $b(x)|a'(x)$ and that $a(x)$ does not have a multiple root. As $b(x) \in F[x]$, and $\deg b(x) > 0$, it has a root c in some extension K of F. Then, $b(x) = (x-c)p(x)$. So, $a(x) = b(x)q(x)$ and $a'(x) = b'(x)q(x) + b(x)q'(x)$. We have $b'(x) = p(x) + (x-c)p'(x)$ and $a'(x) = p(x)q(x) + (x-c)p'(x)q(x) + (x-c)p'(x)q'(x)$. Also, $a'(x) = (x-c)p(x)r(x)$ and we have $(x-c)p(x)r(x) = p(x)q(x) + (x-c)p'(x)q(x) + (x-c)p'(x)q'(x)$. This is equivalent to $p(x)q(x) = (x-c)[p(x)r(x) - p'(x)q(x) - p'(x)q'(x)]$. That implies that $x-c|p(x)$ or $x-c|q(x)$, by Euclid's lemma. If $x-c|p(x)$ then $b(x) = (x-c)(x-c)s(x)$ and $a(x) = (x-c)^2 s(x)q(x)$, i.e. it has a multiple root in K. If $x-c|q(x)$, then $a(x) = (x-c)p(x)q(x) = (x-c)p(x)(x-c)t(x) = (x-c)^2 p(x)t(x)$, which means $a(x)$ has a multiple root c in K.

□

Problem. Show that each of the following polynomials has no multiple roots in any extension of its field of coefficients: (a) $x^3 - 7x^2 + 8 \in \mathbb{Q}[x]$; (b) $x^2 + x + \overline{1} \in \mathbb{Z}/5\mathbb{Z}[x]$; (c) $x^{100} - \overline{1} \in \mathbb{Z}/7\mathbb{Z}[x]$.

Solution. (a) If $a(x) = x^3 - 7x^2 + 8$, then $a'(x) = 3x^2 - 14x$. We will divide these two polynomials and find the greatest common divisor. We have:

$$\begin{aligned}
&(x^3 - 7x^2 + 8) : (3x^2 - 14x) = \frac{1}{3}x - \frac{7}{9} \\
- \;& \underline{\left(x^3 - \frac{14}{3}x^2\right)} \\
& -\frac{7}{3}x^2 + 8 \\
- \;& \underline{\left(-\frac{7}{3}x^2 + \frac{98}{9}x\right)} \\
& -\frac{98}{9}x + 8.
\end{aligned}$$

So, we have $x^3 - 7x^2 + 8 = (3x^2 - 14x)\left(\frac{1}{3}x - \frac{7}{9}\right) + \left(-\frac{98}{9}x + 8\right)$. Then we divide $(3x^2 - 14x)$ by $\left(-\frac{98}{9}x + 8\right)$ and get:

$$\begin{array}{rl} & (3x^2 - 14x) : \left(-\frac{98}{9}x + 8\right) = -\frac{27}{98}x + \frac{2601}{2401} \\ - & \underline{\left(3x^2 - \frac{108}{49}x\right)} \\ & -\frac{578}{49}x \\ - & \underline{\left(-\frac{578}{49}x + \frac{20808}{2401}\right)} \\ & -\frac{20808}{2401}. \end{array}$$

Therefore, $3x^2 - 14x = \left(-\frac{27}{98}x + \frac{2601}{2401}\right)\left(-\frac{98}{9}x + 8\right) - \frac{20808}{2401}$ and, if we divide $-\frac{98}{9}x + 8$ with $-\frac{20808}{2401}$ we get $-\frac{98}{9}x + 8 = -\frac{-20808}{2401}\left(-\frac{117649}{93636}x - \frac{2401}{2601}\right) + 0$. The greatest common divisor is the monic polynomial in the equivalence class of associates of $-\frac{20808}{2401}$ and that is 1. Therefore, polynomial $x^3 - 7x^2 + 8$ and its derivative $3x^2 - 14x$ have no common factors in $\mathbb{Q}[x]$ and, in conclusion, $x^3 - 7x^2 + 8$ has no multiple roots.

(b) We observe $q(x) = x^2 + x + \overline{1}$ over the field $\mathbb{Z}/5\mathbb{Z}$. Then, $q'(x) = \overline{2}x + \overline{1}$. We will find their greatest common divisor. We have:

$$\begin{array}{rl} & \left(x^2 + x + \overline{1}\right) : \left(\overline{2}x + \overline{1}\right) = \overline{3}x + \overline{4} \\ - & \underline{\left(x^2 + \overline{3}x\right)} \\ & \overline{3}x + \overline{1} \\ - & \underline{\left(\overline{3}x + \overline{4}\right)} \\ & \overline{2}. \end{array}$$

From that we have $x^2 + x + \overline{1} = \left(\overline{3}x + \overline{4}\right)\left(\overline{2}x + \overline{1}\right) + \overline{2}$, and finally $\overline{2}x + \overline{1} = \overline{2}\left(x + \overline{3}\right) + \overline{0}$. Therefore, the greatest common divisor is the monic associate of $\overline{2}$ and that is $\overline{1}$. That implies that $q(x)$ and $q'(x)$ have no common divisors and that implies that $q(x)$ has no multiple roots.

(c) Let $r(x) = x^{100} - \overline{1}$ in $\mathbb{Z}/7\mathbb{Z}[x]$. Then, $r'(x) = (100 \cdot \overline{1})x^{99} = \overline{100}x^{99} = \overline{2}x^{99}$. We divide $r(x)$ with $r'(x)$. Thus we get:

$$\begin{array}{rl} & \left(x^{100} - \overline{1}\right) : \left(\overline{2}x^{99}\right) = \overline{4}x \\ - & \underline{\left(x^{100}\right)} \\ & \overline{6}. \end{array}$$

Therefore, we have $x^{100}-\overline{1} = \overline{4}x\cdot\overline{2}x^{99}+\overline{6}$. Finally, $\overline{2}x^{99} = \overline{6}\cdot\overline{5}x^{99}+\overline{9}$, so $\gcd r(x), r'(x) = \overline{1}$ and $r(x)$ has no multiple roots (the reasoning is the same as above).

Vector spaces

Definition. A **vector space** over a field F is an ordered triple $(V, \oplus, \odot)$, where $\oplus$ denotes **vector addition**[93] and $\odot$ **scalar multiplication**[94], and V is a set such that:

- $(V, \oplus)$ is an Abelian group;
- For any $k, l \in F$ and $\mathbf{a}, \mathbf{b} \in V$:
  1. $k \odot \mathbf{a} \in V$;
  2. $k \odot (\mathbf{a} \oplus \mathbf{b}) = (k \odot \mathbf{a}) \oplus (k \odot \mathbf{b})$;
  3. $(k + l) \odot \mathbf{a} = (k \odot \mathbf{a}) \oplus (l \odot \mathbf{a})$ (the $+$ sign denotes addition in F);
  4. $k \odot (l \odot \mathbf{a}) = (k \cdot l) \odot \mathbf{a}$ (the $\cdot$ sign denotes multiplication in F);
  5. $1 \odot \mathbf{a} = \mathbf{a}$ (the 1 denotes unity in F).

The elements of V are called **vectors** and the elements of F are called **scalars**.

Remark. From now on, due to previous definition, we will make no difference between $\oplus$ and $+$, and between $\odot$ and $\cdot$ (unless stated otherwise).

Theorem. Let V be a vector space over F. Then, for every $\mathbf{a} \in V$ and $k \in F$:

1. $0\mathbf{a} = \mathbf{0}$ (where $\mathbf{0}$ is the neutral element in V);
2. $k\mathbf{0} = \mathbf{0}$;
3. If $k\mathbf{a} = \mathbf{0}$ then $k = 0$ or $\mathbf{a} = \mathbf{0}$;
4. $(-1)\mathbf{a} = -\mathbf{a}$.

Proof. *Ad* 1. We have $0\mathbf{a} = (0+0)\mathbf{a}$. By distributivity, $(0+0)\mathbf{a} = 0\mathbf{a}+0\mathbf{a}$. From these two equalities we have $0\mathbf{a} = 0\mathbf{a}+0\mathbf{a}$ and, as V with vector addition (and $0\mathbf{a} \in V$) is an Abelian group, we can add $-0\mathbf{a}$ on both sides of equality and get $0\mathbf{a}-0\mathbf{a} = 0\mathbf{a}+0\mathbf{a}-0\mathbf{a}$. As $-0\mathbf{a}$ is inverse of $0\mathbf{a}$, and neutral element is $\mathbf{0}$, we have $\mathbf{0} = 0\mathbf{a}$. *Ad* 2. We have $k\mathbf{0} = k(\mathbf{0}+\mathbf{0})$, as $\mathbf{0}$ is the neutral element. By distributivity, $k(\mathbf{0}+\mathbf{0}) = k\mathbf{0}+k\mathbf{0}$. Again, $k\mathbf{0} \in V$ and its inverse is $-k\mathbf{0}$, which with $k\mathbf{0}$ simply yields $\mathbf{0}$, the neutral element in V. So, $k\mathbf{0} = k\mathbf{0} + k\mathbf{0}$ is equivalent to $k\mathbf{0} - k\mathbf{0} = k\mathbf{0} + k\mathbf{0} - k\mathbf{0}$, i.e. $\mathbf{0} = k\mathbf{0}$. *Ad* 3. Assume that $k\mathbf{a} = \mathbf{0}$ and that $k \neq 0$ and $\mathbf{a} \neq \mathbf{0}$. That implies that k has an inverse in F and that $k^{-1}(k\mathbf{a}) = k^{-1}\mathbf{0}$. From that we have $(k^{-1}k)\mathbf{a} = \mathbf{0}$, which is equivalent to $\mathbf{a} = \mathbf{0}$, a contradiction to our assumption that $\mathbf{a} \neq \mathbf{0}$. Therefore, $\mathbf{a} = 0$ or $k = 0$. *Ad*

[93] $\oplus : V \times V \to V$
[94] $\odot : F \times V \to V$

4. We have $(-1)\mathbf{a} + 1\mathbf{a} = (-1+1)\mathbf{a} = \mathbf{0}$. So, $(-1)\mathbf{a} + \mathbf{a} = \mathbf{0}$. The inverse of $\mathbf{a}$ is $-\mathbf{a}$, so if we add that to the equality, we get $(-1)\mathbf{a} + \mathbf{a} - \mathbf{a} = \mathbf{0} - \mathbf{a}$, which is equivalent to $(-1)\mathbf{a} + \mathbf{0} = -\mathbf{a}$. That implies, as $\mathbf{0}$ is the neutral element in V, that $(-1)\mathbf{a} = -\mathbf{a}$.

□

Definition. Let V be a vector space over field F and let $U \subseteq V$. We say that U is **closed with respect to scalar multiplication** if $k\mathbf{a} \in U$, $\forall k \in F$ and $\mathbf{a} \in U$. We say that U is a **subspace** of V if U is closed with respect to (vector) addition and scalar multiplication.

Remark. Proof that a subspace U of V is a vector space, is straightforward. All the operations are preserved by definition, so any property of vector space, in its definition, holds. For example, take $(k+l)\mathbf{a}$. As $k + l \in F$, which is same for U and V, and closed with respect to scalar multiplication, then $(k+l)\mathbf{a} \in U \subseteq V$; in V, it holds that $(k+l)\mathbf{a} = k\mathbf{a} + l\mathbf{a}$. The rest can be proved in the exact same fashion.

Definition. Let U be a subspace of V consisting of all the linear combinations of $\mathbf{a_1}, \ldots, \mathbf{a_m}$ (i.e. each element of U can be shown as a linear combination of these vectors). We call U the subspace of V **spanned by** $\mathbf{a_1}, \ldots, \mathbf{a_m}$.

Definition. Let V be a vector space over field F and let $\mathbf{a_1}, \ldots, \mathbf{a_m} \in V$ and $k_1, \ldots, k_m \in F$. Then, the vector $k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m}$ is called a **linear combination** of $\mathbf{a_1}, \ldots, \mathbf{a_m}$.

Definition. Let V be a vector space over F. $S = \{\mathbf{a_1}, \ldots, \mathbf{a_m}\}$ be a set of distinct vectors $\mathbf{a_1}, \ldots, \mathbf{a_m} \in V$. If there exist $k_1, \ldots, k_m \in F$ such that $|\{k \in F : \ k \neq 0\}| > 0$ and $k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$, then we say that S is **linearly dependent**. If S is not linearly dependent, we say that it is **linearly independent.**

Remark. The previous definition actually states that S is linearly dependent if at least one of the vectors in S is a linear combination of the other vectors in S. Also, S is linearly independent if $k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$ implies $k_1 = \cdots = k_m = 0$ (no vector in S is equal to a linear combination of other vectors in S).

Proposition. Let V be a vector space over a field F and $S \subseteq V$. Then,

1. If $\mathbf{0} \in S$, S is linearly dependent;
2. If $S = \{\mathbf{a}\}$, for some $\mathbf{a} \in V - \{\mathbf{0}\}$, then S is linearly independent.

Proof. *Ad* 1. Assume that $\mathbf{0} \in S$. Then, $S = \{\mathbf{0}, \mathbf{a_1}, \ldots, \mathbf{a_m}\}$. Assume that S is linearly independent, i.e. $k_0\mathbf{0} + k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$ implies $k_0 = k_1 = \cdots = k_m = 0$. But, as $k_0\mathbf{0} = \mathbf{0}$, we have that $k_1\mathbf{a_1} + k_2\mathbf{a_2} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$. Let $k \in F - \{0\}$. Then, $k\mathbf{0} = \mathbf{0}$, so we have $k\mathbf{0} + k_1\mathbf{a_1} + k_2\mathbf{a_2} + \cdots + k_m\mathbf{a_m} = k\mathbf{0} + \mathbf{0}$, i.e. $k\mathbf{0} + k_1\mathbf{a_1} + k_2\mathbf{a_2} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$. Now, as S is linearly independent by assumption, it must be that $k = k_1 = \cdots = k_m = 0$, but we assumed that $k \neq 0$, which is a contradiction and S must be linearly dependent. *Ad* 2. Let $S = \{\mathbf{a}\} \neq \{\mathbf{0}\}$ and assume that S is linearly dependent. Then there exists $k \in F - \{0\}$ such that $k\mathbf{a} = \mathbf{0}$. But, that implies that $k = 0$ or $\mathbf{a} = \mathbf{0}$. As the latter possibility cannot be, due to assumption that $\mathbf{a} \neq \mathbf{0}$, it must be $k = 0$, which is a contradiction to assumption that $k \neq 0$. Thus, S must be linearly independent.

□

Lemma. Let V be a vector space over F. If $S = \{\mathbf{a_1}, \ldots, \mathbf{a_m}\} \subseteq V$ is linearly dependent, then there exists $\mathbf{a_i} \in S$, $i \in \{2, \ldots, m\}$, such that $\mathbf{a_i}$ is a linear combination of $\mathbf{a_1}, \ldots, \mathbf{a_{i-1}}$.

Proof. As S is linearly dependent, there exist $k_1, \ldots, k_m \in F$ such that $k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$ (where some k_i are not zero). Let $j = \max\{i \in \{1, \ldots, m\} : k_i \neq 0\}$. Such j exists as there is at least one element that is not zero, due to S being linearly dependent. Then, $k_{j+1}\mathbf{a_{j+1}} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$. Assume that $k_1\mathbf{a_1} + \cdots + k_j\mathbf{a_j} = \mathbf{a}$. Then we would have $\mathbf{a} + k_{j+1}\mathbf{a_{j+1}} + \cdots + k_m\mathbf{a_m} = \mathbf{a}$, i.e. $k_1\mathbf{a_1} + \cdots + k_j\mathbf{a_j} + k_{j+1}\mathbf{a_{j+1}} + \cdots + k_m\mathbf{a_m} = \mathbf{a}$, which implies that $\mathbf{a} = 0$. Thus, $k_1\mathbf{a_1} + \cdots + k_j\mathbf{a_j} = \mathbf{0}$ and we can take $k_j\mathbf{a_j} = (-k_1)\mathbf{a_1} + \cdots + (-k_{j-1})\mathbf{a_{j-1}}$, i.e. $\mathbf{a_j} = (-k_1k_j^{-1})\mathbf{a_1} + \cdots + (-k_{j-1}k_j)\mathbf{a_{j-1}}$, which means that $\mathbf{a_j}$ is a linear combination of $\mathbf{a_1}, \ldots, \mathbf{a_{j-1}}$.

□

Definition. Let V be a vector space over F and U a subspace of V. If there exist $\mathbf{a_1}, \ldots, \mathbf{a_m} \in U$ such that for any $\mathbf{a} \in U$ there exist $k_1, \ldots, k_m \in F$ such that $\mathbf{a} = k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m}$, then we say that U is a **subspace spanned by** $\mathbf{a_1}, \ldots, \mathbf{a_m}$.

Definition. Let V be a vector space over F. A set of vectors $\{\mathbf{a_1}, \ldots, \mathbf{a_m}\} \subseteq V$ is called a **basis** of V if it is linearly independent and spans V.

Theorem. Let V be a vector space over F. If $S, T \subseteq V$ are bases of V, then $|S| = |T|$.

Poof. Assume that S and T are bases of V and that $S = \{\mathbf{s_1}, \ldots, \mathbf{s_m}\}$ and $T = \{\mathbf{t_1}, \ldots, \mathbf{t_n}\}$, where $m, n \in \mathbb{Z}^+$. As $\mathbf{t_i} \in V$, and S spans V, there exist $k_1^{(i)}, \ldots, k_m^{(i)} \in F$ such that $\mathbf{t_i} = k_1^{(i)}\mathbf{s_1} + \cdots + k_i^{(i)}\mathbf{s_i} + \cdots + k_m^{(i)}\mathbf{s_m}$. Notice that not all $k_j^{(i)}$ are zero as

that would imply $\mathbf{t_i} = \mathbf{0}$, which would in turn imply, by previous proposition, that T is not linearly independent. That expression can be rewritten as $(-1)\mathbf{t_i} + k_1^{(i)}\mathbf{s_1} + \cdots + k_i^{(i)}\mathbf{s_i} + \cdots + k_m^{(i)}\mathbf{s_m} = \mathbf{0}$. Let $\mathbf{s_j}$ be the last vector whose coefficient is not zero. If that was $\mathbf{t_i}$, that would again imply that all $k_1^{(i)}, \ldots, k_m^{(i)}$ are zero and that $\mathbf{t_i} = \mathbf{0}$. So, such $\mathbf{s_j}$ must exist and as in the proof of the previous lemma, we can write $\mathbf{s_j}$ as a linear combination of $\mathbf{t_i}, \mathbf{s_1}, \ldots, \mathbf{s_{j-1}}$. In other words, $\mathbf{s_j} = p_0\mathbf{t_i} + p_1\mathbf{s_1} + \cdots + p_{j-1}\mathbf{s_{j-1}}$. But, that also means that $\mathbf{t_i} = (-p_1p_0^{-1})\mathbf{s_1} + \cdots + (-p_1p_0^{-1})\mathbf{s_{j-1}} + \mathbf{s_j}$.

We can write $B = \{\mathbf{t_i}, \mathbf{s_1}, \ldots, \mathbf{s_{j-1}}, \mathbf{s_{j+1}}, \ldots, \mathbf{s_m}\}$. Assume that B is linearly dependent. Then, $\mathbf{0} = q_1\mathbf{t_i} + q_2\mathbf{s_1} + \cdots + q_j\mathbf{s_{j-1}} + q_{j+1}\mathbf{s_{j+1}} + \cdots + q_m\mathbf{s_m}$, where $q_1, \ldots, q_m \in F$ are not all zero. But, as $\mathbf{t_i}$ is the linear combination of $\mathbf{s_1}, \cdots, \mathbf{s_j}$, we can write $\mathbf{0} = (q_2 - q_1p_1p_0^{-1})\mathbf{s_1} + \cdots + (q_j - q_1p_1p_0^{-1})\mathbf{s_{j-1}} + q_1\mathbf{s_j} + q_{j+1}\mathbf{s_{j+1}} + \cdots + q_m\mathbf{s_m}$. But, as $\mathbf{s_1}, \ldots, \mathbf{s_m}$ is linearly independent, $q_1 = q_{j+1} = \cdots = q_m = 0$. Therefore, $\mathbf{0} = q_2\mathbf{s_1} + \cdots + q_{j-1}\mathbf{sj} - \mathbf{1}$, where $q_2, \ldots, q_{j-1}$ are not all zero. But, that would mean that $\mathbf{s_1}, \ldots, \mathbf{s_{j-1}}$ is linearly dependent, which is a contradiction to the fact that S is linearly independent. Also B spans V as, if $\mathbf{s} \in V$, we can write $\mathbf{a}$ as a linear combination of all $\mathbf{s_1}, \ldots, \mathbf{s_j}, \ldots, \mathbf{s_m}$. But, as $\mathbf{s_j}$ is the linear combination of $\mathbf{s_1}, \ldots, \mathbf{s_{j-1}}, \mathbf{t_i}$, then so is $\mathbf{a}$. Therefore, B is the basis of V and $|B| = |S|$. This process can be repeated for all $\mathbf{t_i} \in T$, leaving us to $B = T$ and $|B| = |S|$, i.e. $|S| = |T|$.

□

Definition. Let V be a vector space over F. If there exists $m \in \mathbb{Z}^+$ such that $|\mathcal{B}(F)| = m$, we say that V is **finite-dimensional** vector space and that V is of **dimension** m. We symbolize that by writing $\dim(V) = m$. If $V = \{\mathbf{0}\}$, we say $\dim(V) = 0$.

Lemma. Let V be a vector space over F. If the set $S = \{\mathbf{a_1}, \ldots, \mathbf{a_m}\} \subseteq V$ spans V, then $B \subseteq S$, where B is some basis of V.

Proof. Let V be a vector space over F and let $S = \{\mathbf{a_1}, \ldots, \mathbf{a_m}\}$ be a set that spans V. That implies that every $\mathbf{a}$ can be written as a linear combination of elements of S. If the set S is linearly independent, then by definition S is a basis of V and $S \subseteq S$. If S is not linearly independent, then there exists some $\mathbf{a_i}$ that can be written as a linear combination of all other vectors. Let that vector be $\mathbf{a_1}$, for the sake of simplicity. Then, $\mathbf{a_1} = k_2\mathbf{a_2} + \cdots + k_m\mathbf{a_m}$, for some $k_2, \ldots, k_m \in F$ and not all $\mathbf{a_2}, \ldots, \mathbf{a_m}$ are null-vectors. If $\mathbf{a} \in V$, then as S spans V, we have $\mathbf{a} = l_1\mathbf{a_1} + \cdots + l_m\mathbf{a_m}$, for some $l_1, \ldots, l_m \in F$. Then, we can substitute $\mathbf{a_1}$ into:

$$\begin{aligned} \mathbf{a} &= (l_1k_2\mathbf{a_2} + \cdots + l_1k_m\mathbf{a_m}) + l_2\mathbf{a_2} + \cdots + l_m\mathbf{a_m} \\ &= (l_1k_2 + l_2)\mathbf{a_2} + \cdots + (l_1k_m + l_m)\mathbf{a_m}. \end{aligned}$$

So, as $\mathbf{a}$ can be written as a linear combination of $a_2, \ldots, a_m$, then the set $S - \{\mathbf{a_1}\}$ still spans V. If the set $S - \{\mathbf{a_1}\}$ is linearly indenpendent, it is the basis of V and $S - \{\mathbf{a_1}\} \subset S$. If it is not, we repeat the process as long as we do not obtain a linearly independent set of vectors. It can be done as S is finite. The process terminates if we are left with only one vector, i.e. $\mathbf{a_m}$; by previous proposition, if $S = \{\mathbf{a_m}\}$, then S is linearly independent and a basis of V, along with $\{\mathbf{a_m}\} \subseteq S$.

□

Lemma. Let V be a finite vector space of F. If the set $S = \{\mathbf{a_1}, \ldots, \mathbf{a_m}\} \subseteq V$ is linearly independent, then there exist $\mathbf{a_{m+1}}, \ldots, \mathbf{a_n} \in V$ such that $S \cup \{\mathbf{a_{m+1}}, \ldots, \mathbf{a_n}\}$ is a basis of V (where $m, n \in \mathbb{Z}^+$ and $m \leq n$).

Proof. If S spans V, we are done. Assume that S doesn't span V and $B = \{\mathbf{b_1}, \ldots, \mathbf{b_r}\}$ is a basis of V. Then, as B spans V, also $B \cup S$ spans V. Note that the set $B \cup S$ is not linearly independent, as it would mean $B \cup S$ is a basis and $|B \cup S| = |B|$, which cannot be, as $S \neq \emptyset$ by assumption. Therefore, $B \cup S$ is linearly dependent and spans V. As it is linearly dependent, then $k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m} + k_{m+1}\mathbf{b_1} + \cdots + k_{m+r}\mathbf{b_r} = \mathbf{0}$ and not all $k_1, \ldots, k_{r+m}$ are equal to zero. Assume that all $k_{m+1}, \ldots, k_{m+r}$ are equal to zero. That would mean that $k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$, where some $k_1, \ldots, k_m$ are equal to zero, i.e. that S is linearly dependent, which is contradiction to assumption that it is linearly independent. Therefore, there must exist some $k_{m+1}, \ldots, k_{m+r}$ that are non-zero. Assume it is k_{m+r}. Let us put $\mathbf{b_r}$ in set T. As $B \cup S$ spans V, then any vector $\mathbf{v}$ in V can be shown as a linear combination of vectors in $S \cup B$. So, as $\mathbf{b_r}$ can be shown as a linear combination of other vectors in $B \cup S$, the expression can be substituted by $\mathbf{b_r}$ in $\mathbf{v}$; so $(B \cup S) - \{\mathbf{b_r}\}$ still spans V. If it is linearly independent, we are done. If it is not, we repeat the process. Assume we exhaust all $\mathbf{b_1}, \ldots, \mathbf{b_r}$. That cannot be, as it would mean, again, that $\mathbf{a_1}, \ldots, \mathbf{a_m}$ are linearly dependent. Therefore, some $\mathbf{b_i}$ will remain, and it will be that $B - T \neq \emptyset$. So, we can make S basis of V by adding vectors in $B - T$.

□

Theorem. Let V be a vector space over F and $m \in \mathbb{Z}^+$ such that $\dim(V) = m$. Also, let $S = \{\mathbf{a_1}, \ldots, \mathbf{a_m}\} \subseteq V$. Then:

1. If S is linearly independent, then S is a basis of V;
2. If S spans V, then S is a basis of V.

Proof. *Ad* 1. Assume S is linearly independent and that it does not span V. Then, by previous lemma there exist some vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$, for some $n \in \mathbb{Z}^+$, such that

$S \cup \{\mathbf{b_1}, \ldots, \mathbf{b_n}\}$ is a basis of V (not that set has $m+n$ elements). But then $\dim(V) = m+n > m$, which is a contradiction. Therefore S spans V and it is therefore the basis of V. *Ad* 2. Assume S spans V but it is not basis of V (i.e. not linearly independent). Then, by previous lemma we can remove some $\mathbf{a_i} \in S$ to make S linearly independent and a basis of V. But then $|S| = \dim(V) < m$ which is a contradiction. Therefore, S must be linearly independent and a basis of V.

□

Definition. If U and V are vector spaces over a field F, a function $h : U \to V$ is called a homomorphism or a **linear transformation** if it satisfies the following two conditions:

$$\begin{aligned} h(\mathbf{a}+\mathbf{b}) &= h(\mathbf{a}) + h(\mathbf{b}), \\ h(k\mathbf{a}) &= kh(\mathbf{a}). \end{aligned}$$

The kernel of h is the set $\ker(h) = \{\mathbf{a} \in U : \ h(\mathbf{a}) = \mathbf{0}\}$, called the **null space** of h. The range of h is the set $\mathrm{ran}(h) = \{\mathbf{b} \in V : \ (\exists \mathbf{a} \in U)(h(\mathbf{a}) = \mathbf{b})\}$, called the **range space** of h.

Problem. Prove that $\mathbb{R}^n$ along with operations:

$$\begin{aligned} (a_1, \ldots, a_m) + (b_1, \ldots, b_m) &= (a_1 + b_1, \ldots, a_m + b_m), \\ k(a_1, \ldots, a_m) &= (ka_1, \ldots, ka_m), \end{aligned}$$

for all $(a_1, \ldots, a_m), (b_1, \ldots, b_m) \in \mathbb{R}^n$ and $k \in \mathbb{R}$ is a vector space over the field $\mathbb{R}$.

Solution. Set is obviously non-empty. We know that $\mathbb{R}^n$ defined with such addition is Abelian group from direct product of groups (the very definition of addition in this problem). Let $\mathbf{a} = (a_1, \ldots, a_m)$ and $\mathbf{b} = (b_1, \ldots, b_m)$. It is obvious that $k\mathbf{a} \in \mathbb{R}$, as the very definition of scalar multiplication, along with $ka_i \in \mathbb{R}$, gives us $k\mathbf{a} = (ka_1, \ldots, ka_m) \in \mathbb{R}^n$. Next, we need to prove that $k(\mathbf{a}+\mathbf{b}) = k\mathbf{a}+k\mathbf{b}$. It is obvious that $\mathbf{a}+\mathbf{b} = (a_1+b_1, \ldots, a_m+b_m)$ from definition, so multiplying with k (and using definition of scalar multiplication in this problem) gives us $k(\mathbf{a}+\mathbf{b}) = (ka_1+kb_1, \ldots, ka_m+kb_m)$, that can be broken to $k(\mathbf{a}+\mathbf{b}) = (ka_1, \ldots, ka_m) + (kb_1, \ldots, kb_m)$, and again using definition of scalar multiplication, we have $k(\mathbf{a}+\mathbf{b}) = k(a_1, \ldots, a_m) + k(b_1, \ldots, b_m)$, i.e. $k(\mathbf{a}+\mathbf{b}) = k\mathbf{a} + k\mathbf{b}$. Then, we need to prove that $(k+l)\mathbf{a} = k\mathbf{a} + l\mathbf{a}$, for $k, l \in \mathbb{R}$. From definition of scalar multiplication in this problem we have $(k+$

$l)\mathbf{a} = ((k+l)a_1, \ldots, (k+l)a_m)$, which is, due to distributivity over $\mathbb{R}$, equal to $(ka_1+la_1, \ldots, ka_m+la_m)$, and in the same fashion as in previous condition, we get that it equals $k\mathbf{a} + l\mathbf{a}$. Then, by using definition of scalar multiplication in this problem, we have $k(l\mathbf{a}) = k(la_1, \ldots, la_m) = (k(la_1), \ldots, k(la_m))$. This gives us, due to $\mathbb{R}$ being associative, $k(l\mathbf{a}) = ((kl)a_1, \ldots, (kl)a_m)$. Using the definition of scalar multiplication from here again, we have $(kl)\mathbf{a}$. Finally $1\mathbf{a} = (1a_1, \ldots, 1a_m)$ and as 1 is neutral in $\mathbb{R}$, with respect to multiplication, we have $1\mathbf{a} = (a_1, \ldots, a_m) = \mathbf{a}$. That means that $\mathbb{R}^n$ with such defined operations, over the field $\mathbb{R}$ is a vector space.

Problem. Let $\mathcal{F}(\mathbb{R})$ be a set of all functions from $\mathbb{R}$ to $\mathbb{R}$. Prove that $\mathcal{F}(\mathbb{R})$, along with operations:

$$\begin{aligned} [f+g](x) &= f(x)+g(x), \\ [kf](x) &= kf(x), \end{aligned}$$

for all $f, g \in \mathcal{F}(\mathbb{R})$ and $k \in \mathbb{R}$ is a vector space over the field $\mathbb{R}$.

Solution. Set is obviously non-empty. We know from before that $\mathcal{F}(\mathbb{R})$ with respect to addition is abelian. Also, if we take $f \in \mathcal{F}$ and $k \in \mathbb{R}$, by very definition in this problem, it is again $kf \in \mathcal{F}$. Next, using similar reasoning as in previous problem, $kf(x) + kg(x) = k(f(x) + g(x))$, as $k, f(x), g(x) \in \mathbb{R}$, which is distributive. That equals $k[f+g](x) = [k(f+g)](x)$. This means that $kf + kg = k(f+g)$. Next we have $[(k+l)f](x) = (k+l)f(x) = kf(x) + lf(x) = [kf](x) + [lf](x)$, i.e. $(k+l)f = kf + lf$. Then, $[(kl)f](x) = (kl)f(x) = k(lf(x)) = k[lf](x) = [k(lf)](x)$. Finally, $[1f](x) = 1f(x) = f(x)$. This means that $\mathcal{F}(\mathbb{R})$ is a vector space over $\mathbb{R}$. Note: it is more understandable if we use different signs for vector addition and scalar multiplication.

Problem. Let $\mathcal{P}(\mathbb{R})$ be a set of all polynomials with coefficients in $\mathbb{R}$, along with polynomial addition and scalar multiplication defined with:

$$k \cdot p(x) = k \cdot (a_m x^m + \cdots + a_1 x + a_0) = (ka_m)x^m + \cdots + (ka_1)x + (ka_0) = kp(x),$$

for all $k \in \mathbb{R}$. Prove $\mathcal{P}(\mathbb{R})$ is a vector space over field $\mathbb{R}$. Note: here we denote scalar multipliction with $\cdot$ and multiplication in $\mathbb{R}$ without any operation sign.

Solution. It is trivial to show that set is non-empty. First, we know that $\mathcal{P}(\mathbb{R})$ is abelian and $k \cdot p(x) \in \mathcal{P}(\mathbb{R})$, by very definition. Then, $k \cdot p(x) + k \cdot q(x) = kp(x) + kq(x) = k(p(x) + q(x))$. Further we have $(k+l) \cdot p(x) = (k+l)p(x) = kp(x) + lp(x) =$

$k \cdot p(x) + l \cdot p(x)$. Also, $k \cdot (l \cdot p(x)) = k \cdot (lp(x)) = k(lp(x)) = (kl)p(x) = (kl) \cdot p(x)$. Finally, $1 \cdot p(x) = 1p(x) = p(x)$, which proves $\mathcal{P}(\mathbb{R})$ defined as in this problem is a vector space over $\mathbb{R}$.

Problem. Let $\mathcal{M}(\mathbb{R})$ be the set of all 2×2 matrices of real numbers, with matrix addition and scalar multiplication defined with:

$$k \cdot A = k \begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} = \begin{bmatrix} \text{k a} & \text{k b} \\ \text{k c} & \text{k d} \end{bmatrix} = kA$$

for all $k \in \mathbb{R}$ is a vector space over $\mathbb{R}$.

Solution. The set is obviously non-empty. As we can view matrix A, structurally, as a polynomial, in the manner $p(x) = ax^3 + bx^2 + cx + d$, all reasoning is same as in previous problem.

Problem. Prove that $U = \{(a, b, c) \in \mathbb{R}^3 : \ 2a - 3b + c = 0\}$ is a subspace of $\mathbb{R}^3$.

Solution. Set is obviously non-empty, as $(0, 0, 0) \in U$. We can see that $U \subseteq \mathbb{R}^3$ from definition. Let us prove U is closed with respect to vector addition and scalar multiplication. Let $u_1 = (a_1, b_1, c_1)$ and $u_2 = (a_2, b_2, c_2)$ such that $2a_i - 3b_i + c_i = 0$, for $i \in \{1, 2\}$. Thus, $u_1, u_2 \in U$. We have $u_1 + u_2 = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$. So, $2(a_1 + a_2) - 3(b_1 + b_2) + (c_1 + c_2) = 2a_1 + 2a_2 - 3b_1 - 3b_2 + c_1 + c_2 = (2a_1 - 3b_1 + c_1) + (2a_2 - 3b_2 + c_2) = 0 + 0 = 0$, so $u_1 + u_2 \in U$. Let $k \in F$. We have $2(ka_1) - 3(kb_1) + (kc_1) = k(2a_1 - 3b_1 + c_1) = k0 = 0$, so $ku_1 = (ka_1, kb_1, kc_1) \in U$. Therefore, U is a subspace of $\mathbb{R}^3$.

Problem. Prove that the set of all $(x, y, z) \in \mathbb{R}^3$ which satisfy the pair of equations $ax + by + cz = 0$ and $dx + ey + fz = 0$ is a subspace of $\mathbb{R}^3$.

Solution. Set is obviously non-empty as $(0, 0, 0)$ satisfies these equations. Let $S \subseteq \mathbb{R}^3$ be a set containing (x, y, z) which satisfy $ax + by + cz = 0$ and $dx + ey + fz = 0$. By definition we have that S is a subset of $\mathbb{R}^3$. Let us take $(x_1, y_1, z_1), (x_2, y_2, z_2) \in S$. Then, $ax_1 + by_1 + cz_1 = 0$ and $ax_2 + by_2 + cz_2 = 0$. Adding these two equations gives us $a(x_1 + x_2) + b(y_1 + y_2) + c(z_1 + z_2) = 0$. We do this in the same manner for condition that $dx + ey + fz = 0$, and arrive to the same conclusion; namely, that equation holds for $(x_1 + x_2, y_1 + y_2, z_1 + z_2) = (x_1, y_1, z_1) + (x_2, y_2, z_2)$. Finally, if $k \in \mathbb{R}$ then multiplying $ax_1 + by_1 + cz_1 = 0$ with k gives us $a(kx_1) + b(ky_1) + c(kz_1) = 0$ (same can be shown for second equation), meaning $(kx_1, ky_1, kz_1) \in S$.

Problem. Prove that $S = \{f \in \mathcal{F}(\mathbb{R}) : \ f(1) = 0\}$ is a subspace of $\mathcal{F}(\mathbb{R})$.

Solution. Set is obviously non-empty, as $f(1) = 0$, for $f(x) = x - 1$. By definition, $S \subseteq \mathcal{F}(\mathbb{R})$. Take $f, g \in S$. Then, $f(1) = g(1) = 0$. We have $[f + g](x) = f(x) + g(x)$, so $[f + g](1) = f(1) + g(1) = 0 + 0 = 0$. Therefore, $f + g \in S$. Let $k \in \mathbb{R}$. Then, $[kf](x) = kf(x)$, so $[kf](1) = kf(1) = k0 = 0$. This means $kf \in S$. We have shown that S is a subspace of $\mathcal{F}(\mathbb{R})$.

Problem. Prove that $S = \{f \in \mathcal{F}(\mathbb{R}) : \ (\exists c \in \mathbb{R})(\forall x \in [0, 1])(f(x) = c)\}$ is a subspace of $\mathcal{F}(\mathbb{R})$.

Solution. Set is non-empty, which is trivial to show, i.e. $f \in S$, where $f(x) = 5$ (on whole $\mathbb{R}$, so also on $[0, 1]$). It is obvious that $S \subseteq \mathcal{F}(\mathbb{R})$, by definition of S. Let $f, g \in S$. Then, $f(x) = g(x) = c$, for all $x \in [0, 1]$. Then we have $[f + g](x) = f(x) + g(x)$, and restricting to $x \in [0, 1]$ gives us $[f + g](x) = f(x) + g(x) = c + c = 2c$, thus $f + g$ is again a constant function on $[0, 1]$, meaning $f + g \in S$. Let $k \in \mathbb{R}$. Then, for $x \in [0, 1]$, we have $[kf](x) = kf(x) = kc$. But, $kc \in \mathbb{R}$, so kf is again a constant function, and $f \in S$.

Problem. Prove that $S = \{f \in \mathcal{F}(\mathbb{R}) : \ (\forall x \in \mathbb{R})(f(-x) = f(x))\}$ is a subspace of $\mathcal{F}(\mathbb{R})$. Is the same true for odd functions?

Solution. Set is obviously non-empty, as $\cos(x) \in S$. By definition, $S \subseteq \mathcal{F}(\mathbb{R})$. Let $f, g \in S$. Then, f and g are even functions and $[f + g](-x) = f(-x) + g(-x) = f(x) + g(x) = [f + g](x)$. Also $[kf](-x) = kf(-x) = kf(x) = [kf](x)$, for any $k \in \mathbb{R}$. Therefore, $f + g$ and kf are even, meaning S is a subspace of $\mathcal{F}(\mathbb{R})$. Same holds for odd functions.

Problem. Prove that $S = \{p(x) \in \mathcal{P}(\mathbb{R}) : \ \deg p(x) \leq m\}$, for some $m \in \mathbb{Z}^+$, is a subspace of $\mathcal{P}(\mathbb{R})$.

Solution. Set is obviously non-empty, as we can define a polynomial with real coefficients for each $m \in \mathbb{Z}^+$. It is also obvious that $S \subseteq \mathcal{P}(\mathbb{R})$. Take $p(x), q(x) \in S$. Then, their sum, $p(x) + q(x)$ is also of the same degree, and must be in S. Same thing for $kp(x)$, where $k \in \mathbb{R}$; multiplying with a real number won't change its degree (unless multiplied by zero, but then the (zero) degree is surely less then any positive m). Therefore, S is a subspace of $\mathcal{P}(\mathbb{R})$.

Problem. Prove that $B = \{(0, 0, 0, 1), (0, 0, 1, 1), (0, 1, 1, 1), (1, 1, 1, 1)\}$ is a basis of $\mathbb{R}^4$.

Solution. Obviously $B \subseteq \mathbb{R}^4$. First we will test linear independence of vectors in B. Let $a(0,0,0,1) + b(0,0,1,1) + c(0,1,1,1) + d(1,1,1,1) = (0,0,0,0)$. (From now on we will denote $(0,0,\ldots,0) = \mathbf{0}$.) Then we have $(0,0,0,a) + (0,0,b,b) + (0,c,c,c) + (d,d,d,d) = \mathbf{0}$, which gives us set of linear equations:

$$\begin{aligned} d &= 0, \\ c+d &= 0, \\ b+c+d &= 0, \\ a+b+c+d &= 0. \end{aligned}$$

We can see that, as $d = 0$, then $c + 0 = 0$ gives $c = 0$. Then, $b + 0 + 0 = 0$ gives $b = 0$, and in the same way we get $a = 0$. Therefore, set B is linearly dependent. Does B span $\mathbb{R}^4$? Let $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$. We can see that $(x_1, x_2, x_3, x_4) = (x_4 - x_3 - x_2 - x_1)(0,0,0,1) + (x_3 - x_2 - x_1)(0,0,1,1) + (x_2 - x_1)(0,1,1,1) + x_1(1,1,1,1)$. Therefore, being linearly independent and spanning $\mathbb{R}^4$, B is basis of $\mathbb{R}^4$.

Problem. If $\mathbf{a} = (1,2,3,4)$ and $\mathbf{b} = (4,3,2,1)$, explain why $\{\mathbf{a}, \mathbf{b}\}$ may be extended to a basis of $\mathbb{R}^4$. Find a basis which includes $\mathbf{a}$ and $\mathbf{b}$.

Solution. Let us first prove that $\mathbf{a}$ and $\mathbf{b}$ are linearly independent over $\mathbb{R}$. Let $k_1, k_2 \in \mathbb{R}$. Then, let $k_1\mathbf{a} + k_2\mathbf{b} = \mathbf{0}$, i.e. $k_1(1,2,3,4) + k_2(4,3,2,1) = \mathbf{0}$ From that we get:

$$\begin{aligned} k_1 + 4k_2 &= 0, \\ 2k_1 + 3k_2 &= 0, \\ 3k_1 + 2k_2 &= 0, \\ 4k_1 + k_2 &= 0. \end{aligned}$$

From the first line we get $k_1 = -4k_2$, and putting that in the last line gives us $4 \cdot (-4k_2) + k_2 = 0$, i.e. $-15k_2 = 0$. That implies $k_2 = 0$, and, as $k_1 = -4k_2$, also that $k_1 = 0$, meaning $\mathbf{a}$ and $\mathbf{b}$ are linearly independent over $\mathbb{R}$. Let $\mathbf{c} = (0,1,0,0)$ and $\mathbf{d} = (0,0,1,0)$. Testing for linear independence through $k_1\mathbf{a} + k_2\mathbf{c} + k_3\mathbf{d} + k_4\mathbf{b} = \mathbf{0}$, we get:

$$\begin{aligned} k_1 + 4k_4 &= 0, \\ 2k_1 + k_2 + 3k_4 &= 0, \\ 3k_1 + k_3 + 2k_4 &= 0, \\ 4k_1 + k_4 &= 0. \end{aligned}$$

In the same fashion as before, we get $k_1 = k_4 = 0$. Putting that into the rest equations, obviously leads to $k_2 = k_3 = 0$, thus the set of vectors $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{d}$ is linearly independent. Let us show that any $\mathbf{x} = (x_1, x_2, x_3, x_4)$ can be represented as a linear combination of $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{d}$. Let $(x_1, x_2, x_3, x_4) = k_1(1, 2, 3, 4) + k_2(0, 1, 0, 0) + k_3(0, 0, 1, 0) + k_4(4, 3, 2, 1)$. We have a set of equations:

$$\begin{aligned} x_1 &= k_1 + 4k_4, \\ x_2 &= 2k_1 + k_2 + 3k_4, \\ x_3 &= 3k_1 + k_3 + 2k_4, \\ x_4 &= 4k_1 + k_4. \end{aligned}$$

From the first equation we have $k_1 = x_1 - 4k_4$, and from the last one $k_4 = x_4 - 4k_1$. Putting that into first equation gives us $k_1 = x_1 - 4x_4 + 16k_1$, and finally, also putting k_1 into expression for k_4:

$$\begin{aligned} k_1 &= -\frac{1}{15}x_1 + \frac{4}{15}x_4, \\ k_4 &= \frac{4}{15}x_1 - \frac{1}{15}x_4. \end{aligned}$$

From second equation we have $k_2 = x_2 - 2k_1 - 3k_4$. Then, putting k_1 and k_4 into the former equation, we have:

$$k_2 = x_2 + \frac{2}{15}x_1 - \frac{8}{15}x_4 - \frac{12}{15}x_1 + \frac{3}{15}x_4 = -\frac{2}{3}x_1 + x_2 - \frac{1}{3}x_4.$$

From the equation for x_3, we have $k_3 = x_3 - 3k_1 - 2k_4$. Putting expressions for k_1 and k_4 gives us:

$$k_3 = x_3 + \frac{3}{15}x_1 - \frac{12}{15}x_4 - \frac{8}{15}x_1 + \frac{2}{15}x_4 = -\frac{1}{3}x_1 + x3 - \frac{2}{3}x_4.$$

Thus, for any (x_1, x_2, x_3, x_4) we have shown a way to represent it through coefficients k_1, k_2, k_3 and k_4 as a linear combination of **a**, **b**, **c** and **d**.

Problem. Let A be the set of eight vectors (x, y, z) where $x, y, z \in \{1, 2\}$. Prove that A spans $\mathbb{R}^3$, and find a subset of A which is a basis of $\mathbb{R}^3$.

Solution. Let $\mathbf{a} = (2, 1, 1)$, $\mathbf{b} = (1, 2, 1)$ and $\mathbf{c} = (1, 1, 2)$. We will immediately show their linear independence and we will prove that they span $\mathbb{R}^3$ as a subset of A. Let $k_1, k_2, k_3 \in \mathbb{R}$ and $\mathbf{0} = k_1(2, 1, 1) + k_2(1, 2, 1) + k_3(1, 1, 2)$. Then we get a set of equations:

$$\begin{aligned} 2k_1 + k_2 + k_3 &= 0, \\ k_1 + 2k_2 + k_3 &= 0, \\ k_1 + k_2 + 2k_3 &= 0. \end{aligned}$$

From first equation we have $k_2 = -2k_1 - k_3$ and from third $k_1 = -k_2 - 2k_3$. Putting that into first equation we get $k_2 = 2k_2 + 4k_3 - k_3$, i.e. $k_2 = -3k_3$. Then, from second equation $k_1 - 6k_3 + k_3 = 0$, which gives us $k_1 = 5k_3$. We put that, along with $k_2 = -3k_3$ in the first equation and get $10k_3 - 3k_3 + k_3 = 0$. It is obvious that $k_3 = 0$ which implies that also $k_1 = k_2 = 0$. Thus, **a**, **b** and **c** are linearly independent over $\mathbb{R}$. Now, let us take $(x, y, z) \in \mathbb{R}^3$ and $(x, y, z) = k_1(2, 1, 1) + k_2(1, 2, 1) + k_3(1, 1, 2)$. This gives rise to following equations:

$$\begin{aligned} x &= 2k_1 + k_2 + k_3, \\ y &= k_1 + 2k_2 + k_3, \\ z &= k_1 + k_2 + 2k_3. \end{aligned}$$

Second equation gives us $k_3 = y - k_1 - 2k_2$ and third $k_2 = z - k_1 - 2k_3$. Putting second into third gives $k_2 = z - k_1 - 2y + 2k_1 + 4k_2$. That means $k_1 = -3k_2 - z + 2y$. Putting that into expression for k_3 gives us $k_3 = y + 3k_2 + z - 2y - 2k_2$, i.e. $k_3 = k_2 - y + z$. Putting that into first equation yields $x = -6k_2 - 2z + 4y + k_2 + k_2 - y + z = -4k_2 + 3y - z$, i.e.:

$$k_2 = -\frac{1}{4}x + \frac{3}{4}y - \frac{1}{4}z.$$

Now, if we put that into expression for k_3, we have:

$$k_3 = -\frac{1}{4}x - \frac{1}{4}y + \frac{3}{4}z.$$

Finally, if we put the same expression, for k_2, in equality for k_1 we have:

$$k_1 = \frac{3}{4}x - \frac{1}{4}y - \frac{1}{4}z.$$

Therefore, we have shown that the set of vectors **a**, **b** and **c** is a basis for $\mathbb{R}^3$ (i.e. is linearly independent and spans $\mathbb{R}^3$).

Problem. Let $\mathcal{P}_m(\mathbb{R}) = \{p(x) \in \mathcal{P}(\mathbb{R}) : \deg p(x) \leq m\}$, for some $m \in \mathbb{Z}^+$. Prove that $S = \{1, x, x^2, \ldots, x^m\}$ is a basis of $\mathcal{P}_m(\mathbb{R})$. Then find another basis of $\mathcal{P}_m(\mathbb{R})$.

Solution. It is obvious that $S \subseteq \mathcal{P}_m(\mathbb{R})$, as $\deg x^i \leq m$, for all $i \in \{1, \ldots, m\}$, by definition. To show that the vectors are independent, let $k_1, k_2, \ldots, k_{m+1} \in \mathbb{R}$ and $k_1 + k_2 x + \cdots + k_{m+1}x^m = 0$. Here we implicitly state that 0 on the right-hand side is actually a zero polynomial, not specifically a real number. The polynomial on the left-hand side will be a zero polynomial, by definition, if all of its coefficients are equal to zero, i.e. if $k_1 = k_2 = \ldots = k_{m+1} = 0$. Therefore S is linearly independent. Choose any $p(x) \in \mathcal{P}_m(\mathbb{R})$. Let its degree be $n \leq m$ and $p(x) = k_1 + k_2 x + \cdots + k_{n+1}x^n$. It is obvious that $p(x)$ can be, and already is, represented by vectors in S. Thus, S spans $\mathcal{P}_m(\mathbb{R})$. Another example of a base would be:

$$T = \{1, 1 + x, 1 + x + x^2, \ldots, 1 + x + x^2 + \cdots + x^m\}.$$

Let $k_1, k_2, \ldots, k_{m+1} \in \mathbb{R}$ and

$$k_1 + k_2(1 + x) + k_3(1 + x + x^2) + \cdots + k_{m+1}(1 + x + x^2 + \cdots + x^m) = 0.$$

From that we have:

$$(k_1 + k_2 + \ldots + k_{m+1}) + (k_2 + \ldots + k_{m+1})x + \ldots + (k_m + k_{m+1})x^{m-1} + k_{m+1}x^m = 0.$$

As 0 on the right-hand side is zero polynomial, then all the coefficients on the left-hand side must also equal zero, which bring us to following system of equations:

$$\begin{aligned} k_1 + k_2 + \cdots + k_{m+1} &= 0, \\ k_2 + k_3 + \cdots + k_{m+1} &= 0, \\ &\vdots \\ k_m + k_{m+1} &= 0, \\ k_{m+1} &= 0. \end{aligned}$$

Due to the last equality, namely, $k_{m+1} = 0$, we see that we produce a sort of domino effect. The equation before the last thus gives us $k_m + 0 = 0$, i.e. $k_m = 0$. Therefore, we get $k_1 = k_2 = ldots = k_{m+1} = 0$. Now, let $p(x) = l_1 + l_2x + \cdots + l_{n+1}x^n$, with $l_1, l_2, \ldots, l_{n+1} \in \mathbb{R}$ and $n \leq m$. We want to show that $p(x)$ can be shown as a linear combination of vectors in T, i.e. we must find coefficients $k_1, \ldots, k_{m+1}$ such that:

$$k_1 + k_2(1+x) + k_3(1+x+x^2) + \cdots + k_{m+1}(1+x+\ldots+x^m) = l_1 + l_2x + \cdots + l_{n+1}x^n.$$

Similarly to the procedure above, we get the following system of equations (note that for $n > m$ coefficients in $p(x)$ are equal to zero):

$$\begin{aligned} l_1 &= k_1 + \cdots + k_{m+1}, \\ l_2 &= k_2 + \cdots + k_{m+1}, \\ &\vdots \\ l_{n+1} &= k_{n+1} + \cdots + k_{m+1}, \\ 0 &= k_{n+2} + \cdots + k_{m+1}, \\ &\vdots \\ 0 &= k_m + k_{m+1}, \\ 0 &= k_{m+1}. \end{aligned}$$

Notice that again we have $k_{m+1} = 0$, and so we get up to l_n, having $k_{n+1} = \ldots = k_{m+1}$. Thus, from $l_{n+1} = k_{n+1} + k_{n+2} + \cdots + k_{m+1}$, we have $k_{n+1} = l_{n+1}$. For $l_n = k_n + k_{n+1} + \ldots + k_{m+1}$, we have $l_n = k_n + l_{n+1}$, i.e. $l_n = l_n - l_{n+1}$. Similarly, for $l_{n-1} = k_{n-1} + l_n - l_{n+1} + l_{n+1}$ we get $k_{n-1} = l_{n-1} - l_n$. By this logic we arrive at the following system of coefficients:

$$\begin{aligned} k_1 &= l_1 - l_2, \\ k_2 &= l_2 - l_3, \\ &\vdots \\ k_n &= l_n - l_{n+1}, \\ k_{n+1} &= l_{n+1}. \end{aligned}$$

Therefore, T spans $\mathcal{P}_m(\mathbb{R})$ and is its base.

Problem. Find a basis for each of the following subspaces of $\mathbb{R}^3$: (a) $S_1 = \{(x, y, z) : 3x - 2y + z = 0\}$, (b) $S_2 = \{(x, y, z) : \ (x + y - z = 0) \wedge (2x - y + z = 0)\}$.

Solution. (a) Let us first observe which vectors would span S_1. Assume $(a_i, b_i, c_i) \in B_1$, where B_1 is basis of S_1, and $i \in \{1, 2, 3\}$. But, as also $B_1 \subseteq S_1$, we have:

$$\begin{aligned} 3a_1 - 2b_1 + c_1 &= 0, \\ 3a_2 - 2b_2 + c_2 &= 0, \\ 3a_3 - 2b_3 + c_3 &= 0. \end{aligned}$$

If we let $a_1 = b_2 = c_3 = 0$, we have $c_1 = 2b_1$, $c_2 = -3a_2$ and $3a_3 = 2b_3$. Therefore, we can choose vectors $(0, 1, 2)$, $(1, 0, -3)$ and $(2, 3, 0)$ for basis B_1. We will show that they're linearly independent and span S_1. First, let $k_1, k_2, k_3 \in \mathbb{R}$ and $k_1(0, 1, 2) + k_2(1, 0, -3) + k_3(2, 3, 0) = \mathbf{0}$. From that we have:

$$\begin{aligned} k_2 + 2k_3 &= 0, \\ k_1 + 3k_3 &= 0, \\ 2k_3 - 3k_2 &= 0. \end{aligned}$$

From the first equality we have $k_2 = -2k_3$. Putting that into third equation gives us $2k_3 + 6k_3 = 0$, i.e. $k_3 = 0$. This gives us $k_1 = 0$ from second equation and $k_2 = 0$ from first, therefore vectors in B_1 are linearly independent. Let $(x, y, z) \in S_1$. We will show it can be represented as a linear combination of vectors in B_1. We have $(x, y, z) = k_1(0, 1, 2) + k_2(1, 0, -3) + k_3(2, 3, 0)$, and from that:

$$\begin{aligned} x &= k_2 + 2k_3, \\ y &= k_1 + 3k_3, \\ z &= 2k_3 - 3k_2. \end{aligned}$$

From first equation we have $k_2 = x - 2k_3$, and putting that in third gives us $z = 2k_3 - 3x + 6k_3$, that is:

$$k_3 = \frac{3}{8}x + \frac{1}{8}z.$$

Putting that in expression for k_2 we get:

$$k_2 = \frac{1}{4}x - \frac{1}{4}z.$$

Finally, from second equality, $k_1 = y - 3k_2$, this gives us:

$$k_1 = \frac{9}{8}x + y - \frac{3}{8}z.$$

Therefore, B_1 spans S_1, is linearly independent, meaning it is base for S_1. (b) Let $S_2 = \{(x, y, z) : \ (x + y - z = 0) \wedge (2x - y + z = 0)\}$ and B_2 be basis of S_2. The two equations imply $x + y - z = 2x - y + z$, i.e. $x - 2y + 2z = 0$. Let $(a_i, b_i, c_i) \in B_2$, for $i \in \{1, 2, 3\}$. Then, it follows, due to also $B_2 \subseteq S_2$ that $a_i - 2b_i + 2z_i = 0$, for $i \in \{1, 2, 3\}$. If we choose $a_1 = b_2 = c_3 = 0$, we get:

$$\begin{aligned} -2b_1 + 2c_1 &= 0, \\ a_2 + 2c_2 &= 0, \\ a_3 - 2b_3 &= 0. \end{aligned}$$

From first equation we have $c_1 = b_1$, from second $a_2 = -2c_2$ and from third $a_3 = 2b_3$. Let us choose $(0, 1, 1)$ as first vector for B_2, and $(2, 0, -1)$ as the second. It is obvious they are linearly independent, due to difference in zeros. Now, let us consider a third vector. For the third vector to be linearly dependent, it needs to be $(2b_3, b_3, c_3) = k_1(0, 1, 1) + k_2(2, 0, -1)$, for some $k_1, k_2 \in \mathbb{R}$. We have $2b_3 = 2k_2$ (i.e. $b_3 = k_2$), $b_3 = k_1$ and $c_3 = k_1 - k_2$. Thus, we have $k_1 = k_2 = b_3$, meaning $c_3 = 0$. So, if we choose $c_3 = 0$, it must not be that first two coordinates are of the form $2b_3$ and b_3. Let us choose $(1, 1, 0)$. Then, assume $k_1(0, 1, 1) + k_2(2, 0, -1) + k_3(1, 1, 0) = \mathbf{0}$. We have:

$$\begin{aligned} 2k_2 + k_3 &= 0, \\ k_1 + k_3 &= 0, \\ k_1 - k_2 &= 0. \end{aligned}$$

From third equation we get $k_2 = k_1$ and from second $k_3 = -k_1$. If we put that into the first equation, we obtain $2k_1 - k_1 = 0$, i.e. $k_1 = 0$. That implies that $k_2 = k_3 = 0$, i.e. B_2 is linearly independent. Now, let us observe equation $(x, y, z) = k_1(0, 1, 1) + k_2(2, 0, -1) + k_3(1, 1, 0)$, where $(x, y, z) \in S_2$. Then we get:

$$\begin{aligned} x &= 2k_2 + k_3, \\ y &= k_1 + k_3, \\ z &= k_1 - k_2. \end{aligned}$$

From second and third equations we get $k_3 = y - k_1$ and $k_2 = k_1 - z$. Putting that into first equation yields $x = 2k_1 - 2z + y - k_1$, i.e. $k_1 = x - y + 2z$. Then, second equation gives us $k_3 = -x + 2y - 2z$, and third $k_2 = x - y + z$. Therefore, B_2 is basis of S_2.

Problem. Find a basis for the subspace of $\mathbb{R}^3$ spanned by the set of vectors (x, y, z) such that $x^2 + y^2 + z^2 = 1$.

Solution. Let B denote basis of $S = \{(x, y, z) \in \mathbb{R}^3 : \ x^2 + y^2 + z^2 = 1\}$. We can see that $(1, 0, 0), (0, 1, 0), (0, 0, 1) \in S$. Seeing that these vectors are linearly independent is trivial, and if they span S it must be that $(x, y, z) = k_1(1, 0, 0) + k_2(0, 1, 0) + k_3(0, 0, 1)$. Is trivial to see that B spans S, i.e. it is basis of S.

Problem. Let U be the subspace of $\mathcal{F}(\mathbb{R})$ spanned by $V = \{\cos x^2, \sin x^2, \cos(2x)\}$. Find the dimension of U, and then find a basis of U.

Solution. Let $O(x) = 0$, for all $x \in [0, 2\pi\rangle$. As $\cos(2x) = \cos^2 x - \sin^2 x$, it is obvious that V is linearly dependent. Throwing out $\cos(2x)$, it is easy to show that V will be linearly independent. Assume that it is not linearly independent. Then, $k_1 \cos^2 x + k_2 \sin^2 x = O(x)$, for all $x \in [0, 2\pi\rangle$, and $k_1 \neq 0$ or $k_2 \neq 0$. Assume $k_1 \neq 0$. Now, $k_2 = 0$ or $k_2 \neq 0$. Assume $k_2 = 0$. Then, $k_1 \cos^2 x = O(x)$, for all $x \in [0, 2\pi\rangle$. But, if we take $x = 0$, then $k_1 \cdot 1 = 0$, i.e. $k_1 = 0$, which is a contradiction to assumption that $k_1 \neq 0$. If $k_2 \neq 0$, then $k_1 \cos^2 x + k_2 \sin^2 x = O(x)$, for all $x \in [0, 2\pi\rangle$. But if we choose $x = \frac{\pi}{2}$, we have $k_1 \cdot 0 + k_2 \cdot 1 = 0$, i.e. $k_2 = 0$, which is a contradiction to

assumption that $k_2 \neq 0$. Therefore, $V - \{\cos(2x)\}$ is linearly independent and is a basis for V spanned by those three vectors (previous theorem).

Problem. Find a basis for the subspace of $\mathcal{P}(\mathbb{R})$ spanned by:

$$S = \{x^3 + x^2 + x + 1, x^2 + 1, x^3 - x^2 + x - 1, x^2 - 1\}.$$

Solution. S is linearly dependent because:

$$x^2 + 1 = \frac{1}{2}\left(x^3 + x^2 + x + 1\right) - \frac{1}{2}\left(x^3 - x^2 + x - 1\right).$$

But, set $S - (x^2 + 1)$ is linearly independent which can be easily checked. Let $k_1, k_2, k_3 \in \mathbb{R}$. Then, let $O(x)$ be a null-polynomial and:

$$k_1\left(x^3 + x^2 + x + 1\right) + k_2\left(x^3 - x^2 + x - 1\right) + k_3\left(x^2 - 1\right) = O(x).$$

Then, from that we have following equations:

$$\begin{aligned} k_1 + k_2 &= 0, \\ k_1 - k_2 + k_3 &= 0, \\ k_1 + k_2 &= 0, \\ k_1 - k_2 - k_3 &= 0. \end{aligned}$$

From first equation we have $-k_2 = k_1$, and putting that in the second one gives us $-k_3 = 2k_1$. If we put expressions for $-k_2$ and $-k_3$ in the third equation we get $k_1 + k_1 + 2k_1 = 0$. That gives $4k_1 = 0$, i.e. $k_1 = 0$. Then, also $k_2 = k_3 = 0$, meaning $S - \{x^2 + 1\}$ is linearly independent. By previous theorem, $S - \{x^2 + 1\}$ is basis of subspace spanned by S.

Proposition. Let V be a finite dimensional vector space. Then:

1. If U is a subspace of V, then $\dim(U) \leq \dim(V)$.
2. If U is a subspace of V, and $\dim(U) = \dim(V)$, then $U = V$.

Proof. Ad 1. Assume B_V is basis of V. Then, $\dim(V) = |B_V|$, by definition. Choose any vector $\mathbf{a} \in U$. Then, as $U \subseteq V$, also $\mathbf{a} \in V$. That means that $\mathbf{a}$ can be represented

by vectors in B_V. In other words, B_V spans U. By previous lemma, that means that there exists $B_U \subseteq B_V$ such that B_U is basis of U. That means $\dim(U) = |B_U|$ and $|B_U| \leq |B_V|$, i.e. $\dim(U) \leq \dim(V)$.

Ad 2. We follow the same proof as in 1, but, when we arrive at $\dim(U) = \dim(V)$, we have $|B_U| = |B_V|$. That, along with $B_U \subseteq B_V$ gives $B_U = B_V$. Assume $U \neq V$, i.e. $U \subset V$. Then there exists $\mathbf{v} \in V$ such that $\mathbf{v} \notin U$. As $\mathbf{v} \in V$, then $\mathbf{v}$ can be shown as a linear combination of vectors in B_V. But, as $B_V = B_U$, $\mathbf{v}$ can also be shown as a linear combination of vectors in B_U, meaning it is also in U, which is a contradiction to our assumption. Therefore, it must be that $U = V$.

□

Proposition. Let V be a finite vector space. Any subset of an independent set in V is independent.

Proof. Let $S \subseteq V$ be linearly independent. Let $T \subseteq S$ such that $S, T \neq \emptyset, \{\mathbf{0}\}$. Let us prove that T is linearly independent. If $S = T$, we are done. Let $T = \{\mathbf{v_1}, \ldots, \mathbf{v_m}\}$ and $S = \{\mathbf{v_1}, \ldots, \mathbf{v_m}, \mathbf{v_{m+1}}, \ldots, \mathbf{n}\}$, where $m \leq n$. Let $\mathbf{v_i} \in T$. Assume T is linearly dependent, i.e. there exist $k_2, \ldots, k_m \in \mathbb{R}$ such that $\mathbf{v_1} = k_2\mathbf{v_2} + \cdots + k_m\mathbf{v_m}$. But, as $\mathbf{v_1} \in S$, that would mean that $\mathbf{v_1}$ can be shown as a linear combination of vectors in S in the following way:

$$\mathbf{v_1} = k_2\mathbf{v_2} + \cdots + k_m\mathbf{v_m} + 0\mathbf{v_{m+1}} + \cdots + 0\mathbf{v_n}.$$

We assumed that not all $k_i = 0$, so our assumption that $\mathbf{v_1}$ is a linear combination of vectors in S holds. That means that S is not linearly independent, which is a contradiction to our assumption that it actually is. Therefore, it must be that T is linearly independent also.

□

Proposition. Let V be a finite vector space. Any set of vectors containing a dependent set in V is dependent.

Proof. Let $T \subseteq S \subseteq V$ be a set in V such that $S, T \neq \emptyset, \mathbf{0}$. For $S, T = \mathbf{0}$ proof is trivial. Assume T is linearly dependent. Let us prove that S is then also linearly dependent. Assume contrary, assume that S is linearly independent. By previous proposition, then it must also be that T is linearly independent, which is a contradiction to our assumption. Therefore, it must be that S is linearly dependent.

□

Proposition. Let V be a vector space such that $\dim(V) = m$. If $U \subseteq V$ such that $|U| > m$, then U is linearly dependent.

Proof. Assume that $\mathcal{B}(V) = \{\mathbf{v_1}, \ldots, \mathbf{v_m}\}$ and that $U = \{\mathbf{u_1}, \ldots, \mathbf{u_n}\}$ is linearly independent, where $n > m$. Let us take $U_m = \{\mathbf{u_1}, \ldots, \mathbf{u_m}\}$ (we throw out $\mathbf{u}_{m+1}, \ldots, \mathbf{u_n}\}$). Then, U_m is linearly independent, by previous proposition. Also, by previous proposition, as $|U_m| = m = \dim(V)$, we have that U_m is a basis of V. That also implies that U_m spans V. As $U_m \subseteq U$, then U also spans V. That means that U is also a basis of V and then it must be $n = |U| = \dim(V) = m$, which is impossible because $n > m$.

□

Problem. Prove that if $U = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ is linearly independent, so is $V = \{\mathbf{a} + \mathbf{b}, \mathbf{b} + \mathbf{c}, \mathbf{c} + \mathbf{a}\}$.

Solution. Assume V is linearly dependent and F be a field over which vector space in this problem is defined. Then there exist $k_1, k_2, k_3 \in F$, not all equal to zero, such that the equality $\mathbf{0} = k_1(\mathbf{a} + \mathbf{b}) + k_2(\mathbf{b} + \mathbf{c}) + k_3(\mathbf{c} + \mathbf{a})$ holds. Then, $\mathbf{0} = k_1\mathbf{a} + k_1\mathbf{b} + k_2\mathbf{b} + k_2\mathbf{c} + k_3\mathbf{c} + k_3\mathbf{a}$. That can be regrouped so that $\mathbf{0} = (k_1 + k_3)\mathbf{a} + (k_1 + k_2)\mathbf{b} + (k_2 + k_3)\mathbf{c}$. As $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c}$ are linearly independent by assumption, it must be that $k_1 + k_3 = k_1 + k_2 = k_2 + k_3 = 0$. From that we have $k_1 = -k_3$ and $k_2 = -k_3$. Putting that into $k_1 + k_2 = 0$ we have $-2k_3 = 0$, i.e. $k_3 = 0$. This also implies $k_1 = k_2 = 0$. But, that is a contradiction to assumption that k_1, k_2 and k_3 are not all zero.

Proposition. If $B = \{\mathbf{a_1}, \ldots, \mathbf{a_m}\}$ is a basis of vector space V over F, so is $B' = \{k_1\mathbf{a_1}, \ldots, k_m\mathbf{a_m}\}$ for any nonzero scalars $k_1, \ldots, k_m \in F$.

Proof. Let us show that B' is linearly independent V. Let $l_1, \ldots, l_m \in F$ and $\mathbf{0} = l_1(k_1\mathbf{a_1}) + \cdots + l_m(k_m\mathbf{a_m})$. This can be regrouped so that $\mathbf{0} = (k_1l_1)\mathbf{a_1} + \cdots + (k_ml_m)\mathbf{a_m}$. But, as $\mathbf{a_1}, \ldots, \mathbf{a_m}$ are linearly independent by assumption, it must be that $k_1l_1 = \ldots = k_ml_m = 0$. Now, as $k_1, \ldots, k_m$ are non-zero, it must be that all $l_1, \ldots, l_m$ are zero, meaning B' is linearly independent. Now, let us show that B' spans V. Assume that for some $\mathbf{v} \in V$ we have $\mathbf{v} = l_1\mathbf{a_1} + \cdots + l_m\mathbf{a_m}$. Then, as k_i are non-zero, they have inverses in F, and for $\mathbf{v} = q_1(k_1\mathbf{a_1}) + \cdots + q_m(k_m\mathbf{a_m})$ we can take $q_i = l_ik_i^{-1}$. Thus, we have shown how to obtain linear combination as vectors in B' for $\mathbf{v}$, meaning B' spans V. In other words, as it is also linearly independent, it is a basis of V.

□

Proposition. The space spanned by $A = \{\mathbf{a_1}, \ldots, \mathbf{a_m}\}$ is the same as the space spanned by $B = \{\mathbf{b_1}, \ldots, \mathbf{b_m}\}$ if and only if each $\mathbf{a_i}$ is a linear combination of $\mathbf{b_1}, \ldots, \mathbf{b_m}$, and each $\mathbf{b_j}$ is a linear combination of $\mathbf{a_1}, \ldots, \mathbf{a_m}$.

Proof. Let V_A be a space spanned by A and V_B be a space spanned by B. *Necessity.* Assume $V_A = V_B$. If we take some $\mathbf{a_i} \in A \subseteq V_A$, then also, due to $V_A = V_B$ we have $\mathbf{v} \in V_B$ such that $\mathbf{v} = \mathbf{a_i}$. As $\mathbf{v} \in V_B$, that means it can be shown as a linear combination of $\mathbf{b_j}$. As $\mathbf{v} = \mathbf{a_i}$, that means $\mathbf{a_i}$ can be shown as a linear combination of $\mathbf{b_j}$. Proof is the same if we take $\mathbf{b_j} \in B \subseteq V_B$ first. *Sufficiency.* Assume each $\mathbf{a_i}$ is linear combination of vectors in B, and vice versa. Take $\mathbf{v} \in V_A$. Then, $\mathbf{v}$ can be shown as a linear combination of $\mathbf{a_i}$:

$$\mathbf{v} = k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m}.$$

But, as each $\mathbf{a_i}$ is a linear combination of vectors in B, we have:

$$\mathbf{a_i} = k_1^{(i)}\mathbf{b_1} + k_2^{(1)}\mathbf{b_2} + \cdots + k_m^{(i)}\mathbf{b_m}.$$

Thus, each $\mathbf{a_i}$ can be substituted to get:

$$\mathbf{v} = k_1(k_1^{(1)}\mathbf{b_1} + k_2^{(1)}\mathbf{b_2} + \cdots + k_m^{(1)}\mathbf{b_m}) + \cdots + k_m(k_1^{(m)}\mathbf{b_1} + k_2^{(m)}\mathbf{b_2} + \cdots + k_m^{(m)}\mathbf{b_m}).$$

Then, it is easy to see that we can regroup vectors of linear combination of $\mathbf{v}$ and write:

$$\mathbf{v} = k_1(k_1^{(1)} + k_1^{(2)} + \cdots + k_1^{(m)})\mathbf{b_1} + \cdots + k_m(k_m^{(1)} + k_m^{(2)} + \cdots + k_m^{(m)})\mathbf{b_m}.$$

Therefore, $\mathbf{v}$ can be shown as a linear combination of $\mathbf{b_i}$ meaning $\mathbf{v} \in V_B$. Thus, as $\mathbf{v} \in V_A$ implies $\mathbf{v} \in V_B$ and same can be shown for vectors in V_B, we have $V_A = V_B$, meaning vector space spanned by A is the same as space spanned by B.

□

Proposition. Let U and V be non-empty finite dimensional vector spaces over a field F, and let $h : U \to V$ be a linear transformation. Then:

1. The range of h is a subspace of V. (It is called the range space of h.)
2. The kernel of h is a subspace of U. (It is called the null-space of h.)
3. h is injective if and only if the null space of h is equal to $\{\mathbf{0}\}$.

Proof. *Ad* 1. Let $\text{ran}\,(h) = \{\mathbf{v} \in V : (\exists \mathbf{u} \in U)(h(\mathbf{u}) = \mathbf{v})\}$. As h is a function, and U is non-empty, then it must be that at all $\mathbf{u}$ have at least one corresponding element $\mathbf{v}$ in V. So, we can safely say that $\text{ran}\,(h)$ is non-empty, and that it is a subset of V, by its very definition. Take $\mathbf{v_1}, \mathbf{v_2} \in \text{ran}\,(h)$. Then, there exist $\mathbf{u_1}, \mathbf{u_2} \in U$ such that $h(\mathbf{u_1}) = \mathbf{v_1}$ and $h(\mathbf{u_2}) = \mathbf{v_2}$. Adding those two equalities gives us $h(\mathbf{u_1}) + h(\mathbf{u_2}) = \mathbf{v_1} + \mathbf{v_2}$. As h is a linear transformation, by definition, that is equivalent to $h(\mathbf{u_1} + \mathbf{u_2}) = \mathbf{v_1} + \mathbf{v_2}$. But, that implies that $\mathbf{v_1} + \mathbf{v_2} \in \text{ran}\,(h)$, i.e. $\text{ran}\,(h)$ is closed with respect to vector addition. Take $\mathbf{v} \in \text{ran}\,(h)$ and $k \in F$. Then, there exists $\mathbf{u} \in U$ such that $h(\mathbf{u}) = \mathbf{v}$. If we multiply that by k, we get $kh(\mathbf{u}) = k\mathbf{v}$. As h is a linear transformation, that is equivalent to $h(k\mathbf{u}) = k\mathbf{v}$, meaning $k\mathbf{v} \in \text{ran}\,(h)$. As $\text{ran}\,(h)$ is closed with respect to scalar multiplication also, it is a subspace of V.

Ad 2. Let $\ker(h) = \{\mathbf{u} \in U : h(\mathbf{u}) = \mathbf{0}\}$ be a kernel of h. It is easy to see that by definition $\ker(h) \subseteq U$. If we take some $h(\mathbf{u}) = \mathbf{v}$, then $\mathbf{v} \in \text{ran}\,(h)$, by definition of range space. But, as range of h is a subspace of V, that means also $-\mathbf{v} \in \text{ran}\,(h)$ ($\text{ran}\,(h)$ with respect to addition is an Abelian group, by definition of vector space). That implies that there exists $\mathbf{u}' \in U$ such that $h(\mathbf{u}') = -\mathbf{v}$. This means $h(\mathbf{u}) + h(\mathbf{u}') = \mathbf{v} - \mathbf{v}$, i.e. $h(\mathbf{u} + \mathbf{u}') = \mathbf{0}$. Thus we have proved that $\mathbf{u} + \mathbf{u}' \in \ker(h)$; in other words, $\ker(h)$ is non-empty. Take $\mathbf{u_1}, \mathbf{u_2} \in \ker(h)$. Then, $h(\mathbf{u_1} + \mathbf{u_2}) = h(\mathbf{u_1}) + h(\mathbf{u_2})$ by definition of linear transformation. Also $h(\mathbf{u_1}) + h(\mathbf{u_2}) = \mathbf{0} + \mathbf{0} = \mathbf{0}$, as $\mathbf{u_1}, \mathbf{u_2} \in \ker(h)$. That implies $h(\mathbf{u_1} + \mathbf{u_2}) = \mathbf{0}$, i.e. $\mathbf{u_1} + \mathbf{u_2} \in \ker(h)$, which proves that $\ker(h)$ is closed with respect to vector addition. Let $\mathbf{u} \in \ker(h)$ and $k \in F$. Then, $h(k\mathbf{u}) = kh(\mathbf{u})$, by definition of linear transformation. As $\mathbf{u} \in \ker(h)$, then $kh(\mathbf{u}) = k\mathbf{0} = \mathbf{0}$, which implies $h(k\mathbf{u}) = \mathbf{0}$, i.e. $h(k\mathbf{u}) = \mathbf{0}$. That means $h(k\mathbf{u}) \in \ker(h)$, i.e. $\ker(h)$ is closed with respect to scalar multiplication. Therefore, $\ker(h)$ is a subspace of U.

Ad 3. *Necessity.* Assume h is injective. That means that if $h(\mathbf{u_1}) = h(\mathbf{u_2})$, then $\mathbf{u_1} = \mathbf{u_2}$. Assume that $\mathbf{u} \in \ker(h)$. We have $h(\mathbf{u}) = \mathbf{0}$. As $\mathbf{u} \in \ker(h)$, then also it must be $\mathbf{u}' \in \ker(h)$ such that $\mathbf{u}' = -\mathbf{u}$. Then, $h(\mathbf{u}) + h(\mathbf{u}') = h(\mathbf{u}')$. As h is a homomorphism we have $h(\mathbf{u} + \mathbf{u}') = h(\mathbf{u}')$ which implies $\mathbf{u} + \mathbf{u}' = \mathbf{u}'$. That is equivalent to $\mathbf{u} = \mathbf{0}$. Our choice of $\mathbf{u}$ was arbitrary, so it must be that $\ker(h) = \{\mathbf{0}\}$. *Sufficiency.* As we assume $\ker(h) = \{\mathbf{0}\}$, then $\mathbf{0} \in \ker(h)$ implies $h(\mathbf{0}) = \mathbf{0}$. That also implies that if we take $\mathbf{u}, -\mathbf{u} \in U$, we will have $h(-\mathbf{u} + \mathbf{u}) = h(\mathbf{0}) = \mathbf{0}$. That means $h(-\mathbf{u}) + h(\mathbf{u}) = \mathbf{0}$, i.e. $h(-\mathbf{u}) = -h(\mathbf{u})$. Take $h(\mathbf{u_1}) = h(\mathbf{u_2})$. Then, $h(\mathbf{u_1}) - h(\mathbf{u_2}) = \mathbf{0}$. But, $-h(\mathbf{u_2}) = h(-\mathbf{u_2})$ implies $h(\mathbf{u_1}) + h(-\mathbf{u_2}) = \mathbf{0}$, i.e. $h(\mathbf{u_1} - \mathbf{u_2}) = \mathbf{0}$. From that follows $\mathbf{u_1} - \mathbf{u_2} \in \ker(h) = \{\mathbf{0}\}$, i.e. $\mathbf{u_1} - \mathbf{u_2} = \mathbf{0}$. Thus, $\mathbf{u_1} = \mathbf{u_2}$, which was deduced from $h(\mathbf{u_1}) = h(\mathbf{u_2})$, means h is injective.

□

Proposition[95]**.** Let U, V be finite dimensional vector spaces such that U is a subspace

[95] This proposition is practically the stronger version of previous lemma. The purpose of this is showing another way of proving it.

of V. Let $B_U = \{\mathbf{u_1}, \ldots, \mathbf{u_m}\}$, where $m \in \mathbb{Z}^+$ be a basis of U. Then, either there exists $n > 0$ such that $B_V = \{\mathbf{u_1}, \ldots, \mathbf{u_m}, \mathbf{v_1}, \ldots, \mathbf{v_n}\}$ is a basis of V, or we simply have $B_U = B_V$.

Proof. Let U be a subspace of V and let B_U be defined as in proposition assumption. Take any $\mathbf{v_1} \in V - U$. If such $\mathbf{v_1}$ does not exist, we are done. If it were that $B_U \cup \{\mathbf{v_1}\}$ is linearly dependent, it would mean that $\mathbf{v_1}$ could be shown as a linear combination of B_U, i.e. $\mathbf{v_1} \in U$, which is contradiction to our assumption. If $B_U \cup \{\mathbf{v_1}\}$ spans V, we are done. If not, take $\mathbf{v_2} \in V - U$. If $B_U \cup \{\mathbf{v_1}, \mathbf{v_2}\}$ is linearly dependent, then we take $\mathbf{v_3}$ instead, until we find $\mathbf{v_i}$ which makes $B_U \cup \{\mathbf{v_1}, \mathbf{v_i}\}$ linearly independent. If such $\mathbf{v_i}$ does not exist, that would mean that all $\mathbf{v_2}, \ldots, \mathbf{v_j} \in V - U$ (where j is some natural number) can be shown as linear combination of $B_U \cup \{\mathbf{v_1}\}$, i.e. that $B_U \cup \{\mathbf{v_1}\}$ spans V (as the rest of V is in U, they are spanned by B_U), which is contradiction to assumption that it does not span V. Therefore such $\mathbf{v_i}$ must exist, and we have $B_U \cup \{\mathbf{v_1}, \mathbf{v_i}\}$. We repeat the process until $B_U \cup \{\mathbf{v_1}, \ldots, \mathbf{v_n}\}$ spans V and is linearly independent (this process guarantees both).

□

Theorem. Let U and V be finite-dimensional vector spaces over F, and let $h : U \to V$ be a linear transformation. Then $\dim(U) = \dim(\ker(h)) + \dim(\operatorname{ran}(h))$.

Proof. By previous theorem, if $\mathcal{B}(\ker(h)) = \{\mathbf{u_1}, \ldots, \mathbf{u_m}\}$ is basis of $\ker(h)$, then it can be extended to basis of U such that $\mathcal{B}(U) = \{\mathbf{u_1}, \ldots, \mathbf{u_m}, \mathbf{u_{m+1}}, \ldots, \mathbf{u_{m+n}}\}$. Let $S = \mathcal{B}(U) - \mathcal{B}(\ker(h))$. Let us take $\mathbf{v} \in \operatorname{ran}(h)$. As $\mathbf{v}$ is in range of h, then there exists $\mathbf{u} \in U$ such that $h(\mathbf{u}) = \mathbf{v}$. As $\mathbf{u} \in U$, it can be shown as a linear combination of vectors in $\mathcal{B}(U)$, i.e.

$$\mathbf{u} = k_1\mathbf{u_1} + \cdots + k_m\mathbf{u_m} + k_{m+1}\mathbf{u_{m+1}} + \cdots + k_{m+1}\mathbf{u_{m+1}}.$$

As h is a well-defined function, from equality above, we can get:

$$h(\mathbf{u}) = h(k_1\mathbf{u_1} + \cdots + k_m\mathbf{u_m} + k_{m+1}\mathbf{u_{m+1}} + \cdots + k_{m+1}\mathbf{u_{m+1}}).$$

As h is a homomorphism that is equivalent to:

$$h(\mathbf{u}) = h(k_1\mathbf{u_1}) + \cdots + h(k_m\mathbf{u_m}) + h(k_{m+1}\mathbf{u_{m+1}}) + \cdots + h(k_{m+1}\mathbf{u_{m+1}}).$$

As $\mathbf{u_1}, \ldots, \mathbf{u_m} \in \ker(h)$ we have $h(\mathbf{u_1}) = \ldots = h(\mathbf{u_m}) = \mathbf{0}$. Also, as $h(\mathbf{u}) = \mathbf{v}$ we have:

$$\mathbf{v} = h(k_{m+1}\mathbf{u_{m+1}}) + \cdots + h(k_{m+1}\mathbf{u_{m+1}}).$$

In other words, we can show any $\mathbf{v} \in \text{ran}\,(h)$ as a linear combination of vectors in $h(S)$, where $S = \mathcal{B}\,(U) - \mathcal{B}\,(\ker\,(h))$. Now assume $h(S) = \{h(\mathbf{u_{m+1}}), \ldots, h(\mathbf{u_{m+n}})\}$ is linearly dependent. That means that some $\mathbf{u_{m+i}}$ can be shown as a linear combination of other vectors in $h(S)$. Assume $i = 1$, for simplicity. Then:

$$h(\mathbf{u_{m+1}}) = k_2 h(\mathbf{u_{m+2}}) + \cdots + k_n h(\mathbf{u_{m+n}}).$$

We can rearrange that to get:

$$k_2 h(\mathbf{u_{m+2}}) + \cdots + k_n h(\mathbf{u_{m+n}}) - h(\mathbf{u_{m+1}}) = \mathbf{0}.$$

As h is a homomorphism, expression above is equivalent to:

$$h(k_2\mathbf{u_{m+2}} + \cdots + k_n\mathbf{u_{m+n}} - \mathbf{u_{m+1}}) = \mathbf{0}.$$

But, that would mean that $\mathbf{u} = k_2\mathbf{u_{m+2}} + \cdots + k_n\mathbf{u_{m+n}} - \mathbf{u_{m+1}} \in \ker\,(h)$. As it is in $\ker\,(h)$, it can be shown as a linear combination of vectors in $\mathcal{B}\,(\ker\,(h)) = \{u_1, \ldots, u_m\}$, that is,

$$k_2\mathbf{u_{m+2}} + \cdots + k_n\mathbf{u_{m+n}} - \mathbf{u_{m+1}} = l_1\mathbf{u_1} + \cdots + l_m\mathbf{u_m}.$$

If we rearrange elements in above equality to get expression for $\mathbf{u_{m+1}}$, we have:

$$\mathbf{u_{m+1}} = k_2\mathbf{u_{m+2}} + \cdots + k_n\mathbf{u_{m+n}} - l_1\mathbf{u_1} - \cdots - l_m\mathbf{u_m}.$$

That would imply that $\mathbf{u_{m+1}}$ can be shown as a linear combination of vectors:

$$\{\mathbf{u_1}, \ldots, \mathbf{u_m}, \mathbf{u_{m+2}}, \ldots, \mathbf{u_{m+n}}\} = \mathcal{B}\,(U) - \{\mathbf{u_{m+1}}\}.$$

That would mean that $\mathcal{B}\,(U)$ is not linearly independent, which is a contradiction to assumption that $\mathcal{B}\,(U)$ is a basis of U. Therefore, set $h(S)$ must be linearly independent. As $h(S)$ spans $\text{ran}\,(h)$ and is linearly independent, it is a basis of $\text{ran}\,(h)$, i.e. $\mathcal{B}\,(\text{ran}\,(h)) = h(\mathcal{B}\,(U) - \mathcal{B}\,(\ker\,(h)))$. By definition of $\text{ran}\,(h)$, every element has an original in U. Let $h(\mathbf{u_i}) = h(\mathbf{u_j})$ and assume $i \neq j$, for some $\mathbf{u_i}, \mathbf{u_j} \in S$. We will have $h(\mathbf{u_i}) - h(\mathbf{u_j}) = \mathbf{0}$. As h is a homomorphism that would imply $h(\mathbf{u_i} - \mathbf{u_j}) = \mathbf{0}$,

i.e. $\mathbf{u_i} - \mathbf{u_j} \in \ker(h)$. That would mean $\mathbf{u_i} = \mathbf{u_j} + k_1\mathbf{u_1} + \cdots + k_m\mathbf{u_m}$. But, as $\mathbf{u_i} \in S = \mathcal{B}(U) - \mathcal{B}(\ker(h))$, i.e. $\mathbf{u_i}$ is in basis of U, just as $\mathbf{u_j}$, that would mean $\mathbf{u_i}$ can be shown as a linear combination of vectors in $\mathcal{B}(U)$, i.e. $\mathcal{B}(U)$ is not linearly independent. Therefore, it must be $\mathbf{u_i} = \mathbf{u_j}$, i.e. $\dim(\mathrm{ran}(h)) = |h(S)| = |S| = \dim(U) - \dim(\ker(h))$.

□

Proposition. Let U and V be finite-dimensional vector spaces over F such that $\dim(U) = \dim(V)$ and let $h : U \to V$ be a linear transformation. Then, h is injective if and only if h is surjective.

Proof. *Necessity.* Assume h is injective. Then, by previous proposition, we have $\dim(\ker(h)) = 0$. So, from previous theorem we have $\dim(U) = \dim(\ker(h)) + \dim(\mathrm{ran}(h)) = 0 + \dim(\mathrm{ran}(h)) = \dim(\mathrm{ran}(h))$. From assumption we have:

$$\dim(\mathrm{ran}(h)) = \dim(U) = \dim(V).$$

Then, $\dim(\mathrm{ran}(h)) = \dim(V)$ implies that h is surjective. *Sufficiency.* Assume h is surjective. Then, $\dim(V) = \dim(\mathrm{ran}(h))$ and we have $\dim(U) = \dim(V) = \dim(\mathrm{ran}(h))$. From previous theorem we have:

$$\dim(\mathrm{ran}(h)) = \dim(\ker(h)) + \dim(\mathrm{ran}(h)).$$

In other words, $\dim(\ker(h)) = 0$. Previous proposition then implies that h is injective.

□

Proposition. Let U and V be vector spaces over F. Let $h : U \to V$ be a homomorphism and let h be injective. If S is a linearly independent subset of U, then $h(S)$ is a linearly independent subset of V.

Proof. Assume that S is linearly independent subset of U. Let us assume $h(S)$ is linearly dependent, i.e. $k_1h(\mathbf{a_1}) + \cdots + k_mh(\mathbf{a_m}) = \mathbf{0}$ and not all k_i are equal to zero. As h is a homomorphism that is equal to $h(k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m}) = \mathbf{0}$. That means that $k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m} \in \ker(h)$. But, as h is injective, due to the previous proposition, $\ker(h) = \{\mathbf{0}\}$, and so it must be that $k_1\mathbf{a_1} + \cdots + k_m\mathbf{a_m} = \mathbf{0}$. But, as $\mathbf{a_1}, \ldots, \mathbf{a_m} \in U$ and $k_1, \ldots, k_m \in F$, and not all equal zero, we have that vectors $\mathbf{a_1}, \ldots, \mathbf{a_m} \in U$ are linearly dependent. If U contains linearly dependent set, it cannot be linearly independent, which is a contradiction to our assumption. Therefore, $h(S)$ must be linearly independent also.

□

Proposition. Let U and V be vector spaces over F. Let $h : U \to V$ be a homomorphism. Then, h is injective if and only if $\dim(U) = \dim(h(U))$.

Proof. *Necessity.* Assume h is injective. Then, by previous proposition we have $\dim(\ker(h)) = 0$. From previous theorem, $\dim(U) = \dim(\ker(h)) + \dim(\text{ran}(h))$, and, as $\text{ran}(h) = h(U)$ by definition, we have $\dim(U) = \dim(h(U))$. *Sufficiency.* Assume $\dim(U) = \dim(h(U))$. As $h(U) = \text{ran}(h)$, from previous theorem we have, $\dim(h(U)) = \dim(\ker(h)) + \dim(h(U))$, meaning $\dim(\ker(h)) = 0$. In other words, $\ker(h) = \{\mathbf{0}\}$. So, it must be that h is injective, by previous proposition.

□

Definition. Let U and V be vector spaces over the field F, and let $h : U \to V$ be a homomorphism. We say that h is an **isomorphism** if h is bijective.

Proposition. Let U and V be vector spaces over F such that $\dim(U) = \dim(V)$. Let $h : U \to V$ be a homomorphism. Then, following statements are equivalent:

- h is injective;
- h is surjective;
- h is an isomorphism.

Proof. By previous proposition we have that h is injective if and only if h is surjective. So, if h is surjective, it is also injective, and then it follows that it is an isomorphism. If it is an isomorphism, it implies that h is both injective and surjective. If h is injective, it is also surjective, which implies it is an isomorphism.

□

Lemma. Let V be a finite dimensional vector space over F. Then, each vector in V can be uniquely written as a linear combination of vectors in $\mathcal{B}(V)$.
Proof. Assume $\mathbf{v} \in V$ and $\mathcal{B}(V) = \{\mathbf{v_1}, \ldots, \mathbf{v_m}\}$. That means $\dim(V) = m$. As $\mathcal{B}(V)$ is basis of V, then $\mathbf{v}$ can be shown as a linear combination of vectors in V, i.e.

$$\mathbf{v} = k_1\mathbf{v_1} + \cdots + k_m\mathbf{v_m},$$

where $k_1, \ldots, k_m \in F$. Assume it can also be written as:

$$\mathbf{v} = l_1\mathbf{v_1} + \cdots + l_m\mathbf{v_m},$$

where $l_1, \ldots, l_m \in F$. Subtracting latter and former equalities we get

$$\mathbf{0} = (k_1 - l_1)\mathbf{v_1} + \cdots + (k_m - l_m)\mathbf{v_m}.$$

But, as $\mathbf{v_1}, \ldots, \mathbf{v_m} \in \mathcal{B}(V)$, they are linearly independent, so it must be $k_1 - l_1 = \ldots = k_m - l_m = 0$, i.e. $k_1 = l_1, \ldots, k_m = l_m$. In other words, each vector $\mathbf{V} \in V$ can be uniquely written as a linear combination of vectors in $\mathcal{B}(V)$.

□

Lemma. Let V be a vector space over F and $\dim(V) = m$. Then, F^m is also a vector space over F with $\dim(F^m) = m$.

Proof. As $(F, +, \cdot)$ is a field, then $(F, +)$ is an abelian group. Then, by previous proposition, $(F, +)^m = (F^m, +_m)$ is also an Abelian group. Let us show $(F^m, +_m, \cdot_m)$, which we will designate as F^m with $+$ and $\cdot$, over F is a vector space. Note that $k \cdot_m (k_1, \ldots, k_m) = (kk_1, \ldots, kk_m) \in V$. Take $(k_1, \ldots, k_m), (l_1, \ldots, l_m) \in F^m$ and $k, l \in F$. Then,

$$k((k_1, \ldots, k_m)+(l_1, \ldots, l_m)) = (kk_1+kl_1, \ldots, kk_m+kl_m) = k(k_1, \ldots, k_m)+k(l_1, \ldots, l_m).$$

Similarly, we have:

$$\begin{aligned}(k + l)(k_1, \ldots, k_m) &= ((k + l)k_1, \ldots, (k + l)k_m) \\ &= (kk_1 + lk_1, \ldots, kk_m + lk_m) = k(k_1, \ldots, k_m) + l(k_1, \ldots, k_m).\end{aligned}$$

It is easy to see that:

$$(k(l(k_1, \ldots, k_m))) = k(lk_1, \ldots, lk_m) = (klk_1, \ldots, klk_m) = (kl)(k_1, \ldots, k_m).$$

Finally,

$$1(k_1, \ldots, k_m) = (1k_1, \ldots, 1k_m) = (k_1, \ldots, k_m).$$

Therefore F^m over F is a vector space. Take any $k_1, \ldots, k_m \in F - \{0\}$ such that $k_i \neq k_j$ for $i \neq j$. Then let:

$$B = \{(k_1, 0, \ldots, 0), (0, k_2, \ldots, 0), \ldots, (0, 0, \ldots, k_m)\}.$$

Take $l_1, \ldots, l_m \in F$. If $\mathbf{0} = (l_1k_1, l_2k_2, \ldots, l_mk_m)$, we have $l_ik_i = 0$, and as F is a field and by that also an integral domain, there are no zero divisors and it must be $l_i = k_i = 0$, due to surely $k_i \neq 0$. Therefore, B is linearly independent. Now take $(l_1, \ldots, l_m) \in F^m$. We can take $(l_1, \ldots, l_m) = h_1(k_1, 0, \ldots, 0) + \cdots + h_m(0, 0, \ldots, k_m)$, where $h_i = k_i^{-1}l_i$ (as F is field there exists such k_i^{-1}). Thus, $\mathcal{B}(F^m) = B$ and $\dim(F^m) = m$.

□

Theorem. Let V be a vector space such that $\dim(V) = m$. Then, there exists an isomorphism $h : V \to F^m$.

Proof. We have shown that F^m is a vector space over F and $\dim(F^m) = m$. Now, let $\mathcal{B}(V) = \{\mathbf{v_1}, \ldots, \mathbf{v_m}\}$. Take any $\mathbf{v} \in V$, and it can be, by previous lemma, uniquely represented as $\mathbf{v} = k_1\mathbf{v_1} + \cdots + k_m\mathbf{v_m}$ Now, define $h(\mathbf{v}) = (k_1, \ldots, k_m)$. Assume $h(\mathbf{v}) = h(\mathbf{w})$, where $\mathbf{w} = l_1\mathbf{v_1} + \cdots + l_m\mathbf{v_m}$. That implies $(k_1, \ldots, k_m) = (l_1, \ldots, l_m)$, i.e. $k_i = l_i$, and by that $\mathbf{v} = \mathbf{w}$. Therefore, h is injective and by previous proposition, it is an isomorphism.

□

Definition. Let U and V be subspaces of vector space T. The **sum of vector spaces** U and V, denoted by $U + V$, is the set of all vectors $\mathbf{u} + \mathbf{v}$, where $\mathbf{u} \in U$ and $\mathbf{v} \in V$.

Proposition. Let U and V be subspaces of T over F. Then, $U + V$ and $U \cap V$ are subspaces of T.

Proof. Take $\mathbf{u} + \mathbf{v} \in U + V$. As $\mathbf{u} \in U \subseteq T$, and $\mathbf{v} \in V \subseteq T$, then $\mathbf{u} + \mathbf{v} \in T$, meaning $U + V \subseteq T$. Let us take $\mathbf{u_1} + \mathbf{v_1}, \mathbf{u_2} + \mathbf{v_2} \in U + V$. Adding those two vectors yields $\mathbf{w} = (\mathbf{u_1} + \mathbf{u_2}) + (\mathbf{v_1} + \mathbf{v_2})$. As $\mathbf{u_1} + \mathbf{u_2} \in U$ (as U is closed with respect to addition), and same holds for $\mathbf{v_1} + \mathbf{v_2}$ and V, then, $\mathbf{w} \in U + V$. Take $k \in F$. Then $k(\mathbf{u} + \mathbf{v}) = (k\mathbf{u}) + (k\mathbf{v})$. But, as U and V are subspaces of T over field F then $k\mathbf{u} \in U$ and $k\mathbf{v} \in V$. Therefore $k(\mathbf{u} + \mathbf{v}) \in U + V$. All summed up, $U + V$ is a subspace of T. Let us take $\mathbf{w} \in U \cap V$. That means $\mathbf{w} \in U$ and $\mathbf{w} \in V$. Both are subsets of T, so $\mathbf{w} \in T$, meaning $U \cap V \subseteq T$. Take $\mathbf{w_1}, \mathbf{w_2} \in U \cap V$. Then, as $\mathbf{w_1}, \mathbf{w_2} \in U$, it is also that $\mathbf{w_1} + \mathbf{w_2} \in U$, as U is closed with respect to vector addition. Same reasoning leads to $\mathbf{w_1} + \mathbf{w_2} \in V$. Therefore, $\mathbf{w_1} + \mathbf{w_2} \in U \cap V$. Also $k\mathbf{w} \in U$ as $\mathbf{w} \in U$, because U is closed with respect to scalar multiplication. Also, $k\mathbf{w} \in V$, meaning $k\mathbf{w} \in U \cap V$, meaning $U \cap V$ is a subspace of T.

□

Definition. T is said to be the **direct sum of vector spaces** U and V, if $T = U + V$ and $U \cap V = \{\mathbf{0}\}$. In that case, we write $T = U \oplus V$.

Proposition. Let U and V be subspaces of T. Then, $U \oplus V = T$ if and only if every $\mathbf{t} \in T$ can be uniquely written as $\mathbf{t} = \mathbf{u} + \mathbf{v}$, where $\mathbf{u} \in U$ and $\mathbf{v} \in V$.

Proof. *Necessity.* Assume $U \oplus V = T$. Then, choose $\mathbf{t} = \mathbf{u} + \mathbf{v} \in U \oplus V$. Assume $\mathbf{t} = \mathbf{u}' + \mathbf{v}' \in U \oplus V$. That means $\mathbf{u}' + \mathbf{v}' = \mathbf{u} + \mathbf{v}$, i.e. $\mathbf{u}' - \mathbf{u} = \mathbf{v} - \mathbf{v}'$, As $\mathbf{w} = \mathbf{u}' - \mathbf{u} \in U$, and $\mathbf{w} = \mathbf{v} - \mathbf{v}' \in V$, it must be that $\mathbf{w} \in U$ and $\mathbf{w} \in V$. But, by assumption $U \cap V = \{\mathbf{0}\}$, meaning $\mathbf{w} = \mathbf{0}$. That implies $\mathbf{0} = \mathbf{u}' - \mathbf{u}$ and $\mathbf{0} = \mathbf{v} - \mathbf{v}'$; in other words $\mathbf{u} = \mathbf{u}'$ and $\mathbf{v} = \mathbf{v}'$. *Sufficiency.* Assume that each $\mathbf{t} \in T$ can be uniquely written as $\mathbf{u} + \mathbf{v} \in U + V$. That means $T \subseteq U + V$. Take $\mathbf{u} + \mathbf{v} \in U + V$. It is obvious that, as $U \subseteq T$ and $V \subseteq T$, that $\mathbf{u} + \mathbf{v} \in T$. Therefore, $U + V \subseteq T$, implying $U + V = T$. Assume there exists $\mathbf{t} \in T$ such that $\mathbf{t} \in U \cap V$. Assume that $\mathbf{t} = \mathbf{u} + \mathbf{v}$. But, we can write $\mathbf{t} = \mathbf{0} + \mathbf{t}$, as $\mathbf{0} \in U$ and $\mathbf{t} \in V$. That means it must be that $\mathbf{u} = \mathbf{0}$. Similarly, we can write $\mathbf{t} = \mathbf{t} + \mathbf{0}$, because $\mathbf{t} \in U$ and $\mathbf{0} \in V$, but that implies $\mathbf{v} = \mathbf{0}$. Therefore, $\mathbf{t} = \mathbf{0} + \mathbf{0} = \mathbf{0}$ and $U \cap V = \{\mathbf{0}\}$.

□

Proposition. Let U be a subspace of finite dimensional vector space T. Then, there exists subspace V of T such that $\dim(V) = \dim(T) - \dim(U)$ and $T = U \oplus V$.

Proof. Assume $\mathcal{B}(T) = \{\mathbf{t_1}, \ldots, \mathbf{t_m}\}$, where $\dim(T) = m$. As U is subspace of T then $\mathcal{B}(U) = \{\mathbf{t_1}, \ldots, \mathbf{t_n}\}$, where $\dim(U) = n$. Let V be a subspace generated by $B = \{\mathbf{t_{n+1}}, \ldots, \mathbf{t_m}\}$. Then, $\dim(V) = m - n$. Now, let us take $\mathbf{t} \in T$. Then, we can write $\mathbf{t}$ uniquely as:

$$\mathbf{t} = k_1\mathbf{t_1} + \cdots + k_n\mathbf{t_n} + k_{n+1}\mathbf{t_{n+1}} + \cdots + k_m\mathbf{t_m}.$$

It is easy to see that:

$$\begin{aligned} k_1\mathbf{t_1} + \cdots + k_n\mathbf{t_n} &= \mathbf{u} \in U \\ k_{n+1}\mathbf{t_{n+1}} + \cdots + k_m\mathbf{t_m} &= \mathbf{v} \in V. \end{aligned}$$

That means $\mathbf{t} = \mathbf{u} + \mathbf{v}$, where $\mathbf{u} \in U$ and $\mathbf{v} \in V$, and as writing down $\mathbf{t}$ as linear combination of vectors in $\mathcal{B}(T)$ is unique, then $\mathbf{t}$ is also uniquely written as sum of $\mathbf{u}$ and $\mathbf{v}$. By previous proposition, that implies $T = U \oplus V$, and at the same time we have $\dim(V) = \dim(T) - \dim(U)$.

□

Proposition. If U and V are subspaces of finite dimensional vector space T, then:

$$\dim(U+V) = \dim(U) + \dim(V) - \dim(U \cap V).$$

Proof. Let $\mathbf{u}+\mathbf{v} \in U+V$. Then, if we consider $\dim(U) = m$ and $\dim(V) = n$, we can show $\mathbf{u}$ as a linear combination of m vectors in $\mathcal{B}(U)$ and $\mathbf{v}$ as linear combination of n vectors in $\mathcal{B}(V)$. But, as some of these base vectors can be both in $\mathcal{B}(U)$ and $\mathcal{B}(V)$, assume k of them, adding $\mathbf{u}$ and $\mathbf{v}$ would mean that $\mathbf{u}+\mathbf{v}$ is written in $m+n-k$ number of vectors, in a unique manner. Those vectors, defining $\mathbf{u}+\mathbf{v}$, are also linearly independent (as vectors in $\mathcal{B}(U)$ and $\mathcal{B}(V)$ are), and they span $U+V$ (as taking any $\mathbf{u}+\mathbf{v}$, we can show it as linear combination of vectors from $\mathcal{B}(U)$ and $\mathcal{B}(V)$), so they form $\mathcal{B}(U+V)$. The dimension of this basis is $m+n-k = \dim(U) + \dim(V) - \dim(U \cap V)$.

□

Degrees of field extensions

Proposition. Let E be a field, $F \leq E$ and $c \in E$. If c is algebraic over F, then $F(c)$ is a vector space over F.

Proof. As $F(c)$ is a field, it is also an abelian group with respect to addition. If we take $k, l \in A$, $a(c), b(c) \in F(c)$, then it is obvious that $ka(c) = k(a_m c^m + \cdots + a_1 c + a_0) = (ka_m)c^m + \cdots + (ka_1)c + (ka_0) \in F(c)$, as $ka_i \in F$. Also, it is easy to see that $k(a(c)+b(c)) = ka(c)+kb(c)$, $(k+l)a(c) = (k+l)(a_m c^m+\cdots+a_1 c+a_0) = (k+l)a_m c^m+\cdots+(k+l)a_1 c+(k+l)a_0 = ka_m c^m+la_m c^m+\cdots+ka_1 c+la_1 c+ka_0+la_0 = ka(c)+la(c)$. Also, $k(la(c)) = k(la^m c_m+\cdots+la_1 c+la_0) = (kl)a^m c_m+\cdots+(kl)a_1 c+(kl)a_0 = (kl)a(c)$. Finally, $1a(c) = a(c)$ is trivial.

□

Definition. If extension E of field F is a vector space over F with $\dim(E) = m$, we say that E is an **extension of degree** m over F, which we symbolize by writing $[E : F] = m$. If the dimension of vector space E over F is finite, we say that E is a **finite extension** of F.

Theorem. Let E be a finite field, $F \leq E$ and let $c \in E$ be algebraic over F. Then the degree of $F(c)$ is equal to the degree of the minimum polynomial of c over F.

Proof. Let $p(x) \in F[x]$ be a minimum polynomial of c over F. Minimal polynomial (of finite degree) exists (by definition) due to assumption that c is algebraic over F. That means that $p(x)$ is monic, $p(c) = 0$ and there exist no polynomial of lesser degree satisfying same conditions. Assume $p(x) = c^{m+1} + p_m c^m + \cdots + p_1 c + p_0$. Then, $\deg p(x) = m + 1$. We will prove that $B = \{1, c, \ldots, c^m\}$ is basis of $F(c)$ and that $\dim(F(c)) = m + 1$. Let us take $a(c) = a_n c^n + \cdots + a_1 c + a_0 \cdot 1 \in F(c)$. Then there exists $a(x) \in F[x]$ with same coefficients a_i. Assume $\deg a(x) = n > m$. Using division algorithm we get $a(x) = p(x)q(x) + r(x)$, where $0 \leq \deg r(x) < \deg p(x) = m + 1$. But, as $p(c) = 0$, then $a(c) = 0q(c) + r(c)$, i.e. $a(c) = r(c)$. That implies $n = \deg a(x) < \deg r(x) = m + 1$, i.e. $n \leq m$, which is a contradiction. Therefore, it must be that $\deg a(x) < \deg r(x)$, and $a(c)$ is of form $a(c) = a_m c^m + \cdots + a_1 c + a_0$. In other words, $a(c)$ is a linear combination of elements in B. Assume B is linearly dependent, i.e. $k_m c^m + \cdots + k_1 c + k_0 = 0$ and not all k_i are equal to zero. Let $k(x) = k_m x^m + \cdots + k_1 x + k_0$. We do not know if k_m, k_{m-1} and so on are equal to zero, so we can say at best $\deg k(x) \leq m$. As $k(c) = 0$ and because $p(x)$ is minimal polynomial of c over F, it must be that $m + 1 = \deg p(x) \leq \deg k(x) \leq m$, which is a contradiction. It can only be that degree of $k(x)$ is undefined, i.e. that $k(x) = 0$. That

of course implies $k_m = \ldots = k_1 = k_0 = 0$, i.e. B is linearly independent. Therefore, $B = \mathcal{B}(F(c))$. The number of elements in $\mathcal{B}(Fc)$ is $m + 1$, the same as degree of minimum polynomial of c over F.

□

Theorem. Let $H \trianglerighteq G \trianglerighteq F$ be finite fields. Then, $[H : F] = [H : G][G : F]$.

Proof. Let $\{a_1, \ldots, a_m\}$ be a basis of G over F and $\{b_1, \ldots, b_n\}$ be a basis of H over G. Then, $[G : F] = m$ and $[H : G] = n$. We will show that the set $B = \{a_i b_j : \ i \in \{1, \ldots, m\}, \ j \in \{1, \ldots, n\}\}$ is a basis of H over F. Assume B is linearly dependent. Then, $\sum k_{i,j} a_i b_j = 0$ and not all $k_{i,j}$ are equal to zero. We have:

$$a_1(k_{1,1}b_1 + \cdots + k_{1,n}b_n) + \cdots + a_m(k_{m,1}b_1 + \cdots + k_{m,n}b_n) = 0.$$

But, as $a_1, \ldots, a_m$ are linearly independent, it must be that:

$$\begin{aligned} k_{1,1}b_1 + k_{1,2}b_2 + \cdots + k_{1,n}b_n &= 0, \\ k_{2,1}b_1 + k_{2,2}b_2 + \cdots + k_{2,n}b_n &= 0, \\ &\vdots \\ k_{m,1}b_1 + k_{m,2}b_2 + \cdots + k_{m,n}b_n &= 0. \end{aligned}$$

But, as $b_1, \ldots, b_n$ are also linearly independent, then all coefficients $k_{i,j}$ are equal to zero, meaning $a_i b_j$ are linearly independent. Let us take $\mathbf{h} \in H$. As H is a vector space over G, then we can write $\mathbf{h} = b_1 k_1 + \cdots + b_n k_n$, where $k_j \in G$. But, as G is a vector space over F, we can write $k_j = l_1^{(j)} a_1 + \cdots + l_m^{(j)} a_m$. It is obvious that putting these expressions in $\mathbf{h}$ we will get:

$$\mathbf{h} = b_1(l_1^{(1)}a_1 + \cdots + l_m^{(1)}a_m) + \cdots + b_n(l_1^{(n)}a_1 + \cdots + l_m^{(n)}a_m) = \sum l_i^{(j)} a_i b_j.$$

That proves that B spans H over F, meaning B is a basis of H over F. It is easy to see that $[H : F] = mn = [G : F][H : G]$.

□

Definition. If c is algebraic over F, we say that $F(c)$ is obtained by **adjoining** c to F. An extension $F(c)$ formed by adjoining a single element to F is called a **simple**

extension of F. An extension $F(c_1, \ldots, c_m)$, formed by adjoining a finite number of elements $c_1, \ldots, c_m$ is called an **iterated extension**.

Proposition. Let F be a field and let $c_1, \ldots, c_m$ be algebraic over F. Then, iterated extension $F(c_1, \ldots, c_m)$ is the smallest field containing $c_1, \ldots, c_m$ and F.

Proof. We have that, by previous proposition, $F(c_1)$ is a smallest field containing c_1 and F. Now, $F(c_1)$ itself being a field, $F(c_1, c_2)$ is smallest field containing $F(c_1)$ and c_2. Assume G is smallest field containing F, c_1 and c_2. Then it must be that $F \subseteq G$ and $c_1, c_2 \in G$. But, as F and c_1 are in G, it must be that $F(c_1) \subseteq G$. Now, as $F(c_1)$ and c_2 are also in G, then, it must be that $F(c_1, c_2) \subseteq G$. But, by definition, $F(c_1, c_2)$ is the smallest field containing F, c_1 and c_2, so it must be $F(c_1, c_2) = G$ (due to are assumption that G is smallest field containing F, c_1 and c_2). The rest of proof follows inductively.

□

Proposition. Let F be a finite field. If $c_1, \ldots, c_m$ are algebraic over F, then iterated extension $F(c_1, \ldots, c_m)$ is a finite extension of F.

Proof. By previous theorem, as c_1 is algebraic over F, and as F is finite, then dimension of $F(c_1)$ is finite. So, by definition, $F(c_1)$ is a finite extension of F. Again, as c_2 is algebraic over F, it is certainly algebraic over $F(c_1)$. Let us elaborate: as c_2 is algebraic over F, there exists polynomial $p(x)$ with coefficients in F such that $p(c_2) = 0$. But, coefficients of F are also in $F(c_1)$, so c_2 is also algebraic over $F(c_1)$. Then, using previous theorem, dimension of $F(c_1, c_2)$ is finite. The rest of the proof goes inductively.

□

Proposition[96]**.** Every finite extension is an iterated extension.

Proof. Assume that E is a finite extension of F. That means that, taking E as a vector space over F, $\dim(E) = m$, where $m \in \mathbb{Z}^+$. Then, $\mathcal{B}(E) = \{\mathbf{v_1}, \ldots, \mathbf{v_m}\}$ and each $\mathbf{v} \in E$ can be written as $\mathbf{v} = k_1\mathbf{v_1} + \cdots + k_m\mathbf{v_m}$. So, E contains both F and $\mathbf{v_1}, \ldots, \mathbf{v_m}$. Let us observe $F(\mathbf{v_1}, \ldots, \mathbf{v_m})$. It is obvious that $\mathbf{v} \in E$, written as above, implies $\mathbf{v} \in F(\mathbf{v_1}, \ldots, \mathbf{v_m})$. In other words, $E \subseteq F(\mathbf{v_1}, \ldots, \mathbf{v_m})$ and also $\mathbf{v_1}, \ldots, \mathbf{v_m} \in F(\mathbf{v_1}, \ldots, \mathbf{v_m})$. But, as $F(\mathbf{v_1}, \ldots, \mathbf{v_m})$ is the smallest field containing F and $\mathbf{v_1}, \ldots, \mathbf{v_m}$, then $E \subseteq F(\mathbf{v_1}, \ldots, \mathbf{v_m})$ implies $E = F(\mathbf{v_1}, \ldots, \mathbf{v_m})$. I.e. E is an iterated extension of F.

[96] Converse of former proposition.

□

Theorem. If E is a finite extension of F, every element in E is algebraic over F.

Proof. Let $\mathbf{v} \in E$ and $\dim(E) = m$. Then, $V = \{\mathbf{1}, \mathbf{v}, \mathbf{v}^2, \ldots, \mathbf{v}^m\}$ is linearly dependent by previous proposition, because $|V| = m + 1 > m = \dim(E)$ and $V \subseteq E$ (easy to see, as E is closed with respect to multiplication of vectors, so also $\mathbf{v}^i$ are also in E). That means that $k_m\mathbf{v}^m + \cdots + k_1\mathbf{v} + k_0\mathbf{1} = \mathbf{0}$, where not all $k_0, k_1, \ldots, k_m$ are equal to zero. Note that $k_0, k_1, \ldots, k_m \in F$ (as E is a vector space over F). If we take $p(x) = k_m x^m + \cdots + k_1 x + k_0$, we see that $p(\mathbf{v}) = \mathbf{0}$, i.e. $\mathbf{v}$ is the root of polynomial $p(x) \in F[x]$. That means that $\mathbf{v}$ is algebraic over F.

□

Remark. It is easy to see that elements in $F(c_1, \ldots, c_m)$ are of the form:

$$\sum_{i_1,\ldots,i_m} k_{i_1,\ldots,i_m} c_1^{i_1} \cdots c_m^{i_m}.$$

Problem. Find a basis for $\mathbb{Q}(i\sqrt{2})$ over $\mathbb{Q}$ and describe the elements of $\mathbb{Q}(i\sqrt{2})$.

Solution. Take $x = i\sqrt{2}$. By squaring this equality, we get $x^2 = -2$, i.e. $x^2 + 2 = 0$. Is $x^2 + 2$ irreducible over $\mathbb{Q}$? There exists $2 \in P$ such that $2 \nmid 1$ (the leading coefficient) and $2^2 = 4 \nmid 2$ (the free member), while $2|2$ (the free member) and $2|0$ (the coefficient in x), so by Eisenstein's criterion, $x^2 + 2$ is irreducible over $\mathbb{Q}$. From previous theorem, we showed that, if $p(x) = x^2 + 2$ is minimum polynomial of $i\sqrt{2}$ over $\mathbb{Q}$, then $B = \mathcal{B}\left(Q(i\sqrt{2})\right) = \{1, i\sqrt{2}\}$. If we take $\mathbf{v} \in \mathbb{Q}(i\sqrt{2})$, then, as B spans $\mathbb{Q}(i\sqrt{2})$, we have that $\mathbf{v}$ is a linear combination of elements in B, i.e. $\mathbf{v} = a \cdot i\sqrt{2} + b \cdot 1 = ai\sqrt{2} + b$, where $a, b \in \mathbb{Q}$.

Problem. Show that every element of $\mathbb{R}(2 + 3i)$ can be written as $a + bi$, where $a, b \in \mathbb{R}$.

Solution. Let $x = 2 + 3i$. Then, $x - 2 = 3i$, and by squaring this equality, we get $x^2 - 4x + 4 = -9$, i.e. $x^2 - 4x + 13 = 0$. Is $p(x) = x^2 - 4x + 13$ irreducible over $\mathbb{R}$? One of the roots is $2 + 3i$, which means that $p(x)$ is irreducible over $\mathbb{R}$. Therefore $p(x)$ is minimum polynomial of $2 + 3i$ over $\mathbb{R}$. Now, from previous theorem, $B = \mathcal{B}(\mathbb{R}(2 + 3i)) = \{\mathbf{1}, \mathbf{2 + 3i}\}$. Take $\mathbf{v} \in \mathbb{R}(2 + 3i)$ which can be shown as a linear combination of vectors in B, i.e. $\mathbf{v} = k + (2 + 3i)l$, where $k, l \in \mathbb{R}$. Thus, every $\mathbf{v}$ can be written as $(k + 2l) + 3li$. If we take $a, b \in \mathbb{R}$ such that $a = k + 2l$ and $b = 3l$, we have $\mathbf{v} = a + bi$. That means that $\mathbb{R}(2 + 3i) \subseteq \mathbb{C}$. Also, if we take $a + bi \in \mathbb{C}$, we can easily write it down using k and l from former equalities.

Problem. If $a = \sqrt{1+\sqrt[3]{2}}$ show that $\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}, a, 2^{\frac{1}{3}}a, 2^{\frac{2}{3}}a\}$ is a basis of $\mathbb{Q}(a)$ over $\mathbb{Q}$. Describe the elements of $\mathbb{Q}(a)$.

Solution. Let $x = \sqrt{1+\sqrt[3]{2}}$. Then, $x^2 = 1+\sqrt[3]{2}$, which is again equivalent to $x^2-1 = \sqrt[3]{2}$. If we cube the equation, we get $x^6-3x^4+3x^2-1 = 2$, which is the same as $x^6-3x^4+3x^2-3 = 0$. If we consider $p(x) = x^6-3x^4+3x^2-3$, we can see that for $3 \in P$, as 3 divides each coefficient, except the leading one, and as $9 \nmid -3$, by Eisenstein's criterion, $p(x)$ is irreducible over $\mathbb{Q}$, and by that minimal polynomial of $a = \sqrt{1+\sqrt[3]{2}}$. We have $\mathcal{B}(\mathbb{Q}(a)) = \{1, a, 1+\sqrt[3]{2}, a(1+\sqrt[3]{2}), 1+2\sqrt[3]{2}+\sqrt[3]{4}, a(1+2\sqrt[3]{2}+\sqrt[3]{4})\}$, and each $\mathbf{v} \in \mathbb{Q}(a)$ can be written as:

$$\begin{aligned}\mathbf{v} &= k_1 + k_2 a + k_3(1+\sqrt[3]{2}) + k_4 a(1+\sqrt[3]{2}) \\ &\quad + k_5(1+2\sqrt[3]{2}+\sqrt[3]{4}) + k_6 a(1+2\sqrt[3]{2}+\sqrt[3]{4}) \\ &= (k_1+k_3+k_5) + a(k_2+k_4+k_6) + \sqrt[3]{2}(k_3+2k_5) + \sqrt[3]{2}a(k_4+2k_6) \\ &\quad + k_5\sqrt[3]{4} + k_6 a(\sqrt[3]{4}).\end{aligned}$$

Thus we have shown that $B = \{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}, a, 2^{\frac{1}{3}}a, 2^{\frac{2}{3}}a\}$ spans $\mathbb{Q}(a)$, for choosing any $\mathbf{v}$, it can be rewritten as linear combination of vectors in B. By previous proposition, as $|B| = \dim(\mathbb{Q}(a)) = 6$, and as it spans $\mathbb{Q}(a)$, it is a basis of $\mathbb{Q}(a)$. Elements of $\mathbb{Q}(a)$ can be written as:

$$\mathbf{v} = k_1 + k_2\sqrt{1+\sqrt[3]{2}} + k_3\sqrt[3]{2} + k_4\sqrt[3]{2}\left(\sqrt{1+\sqrt[3]{2}}\right) + k_5\sqrt[3]{4} + k_6\sqrt[3]{4}\left(\sqrt{1+\sqrt[3]{2}}\right).$$

Problem. Find a basis of $\mathbb{Q}(\sqrt{2}+\sqrt[3]{4})$ over $\mathbb{Q}$, and describe the elements of $\mathbb{Q}(\sqrt{2}+\sqrt[3]{4})$.

Solution. Let $x = 2^{\frac{1}{2}} + 2^{\frac{2}{3}}$. Then, from $x - 2^{\frac{1}{2}} = 2^{\frac{2}{3}}$, by cubing, we get $x^3 - 3x^2 2^{\frac{1}{2}} + 6x - 2^{\frac{3}{2}} = 4$. This can be written as $x^3 + 2(3x-2) = 2^{\frac{1}{2}}(3x^2+2)$. By squaring this equation we get $x^6 + 4x^3(3x-2) + 4(9x^2-12x+4) = 2(9x^4+12x^2+4)$. This can be written nicely as $p(x) = 0$ where $p(x) = x^6 - 6x^4 - 8x^3 + 12x^2 - 48x + 8$. Now, such polynomial does not satisfy Eisenstein's criterion, so we need a different approach. If $a = \sqrt{2}+\sqrt[3]{4}$, then $a - \sqrt{2} = \sqrt[3]{4}$. After cubing this equality we get $a^3 - 3a^2\sqrt{2} + 6a - 2\sqrt{2} = 4$, i.e. $a^3 - 3a^2\sqrt{2} + 6a - 2(\sqrt{2}+2) = 0$. We can see that $q(x) \in \mathbb{Q}(\sqrt{2})[x]$, where $q(x) = a^3 - 3a^2\sqrt{2} + 6a - 2(\sqrt{2}+2)$. Before we return to a and $p(x)$, let us observe $b = \sqrt{2}$. That implies $b^2 - 2 = 0$. Minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $r(x) = x^2 - 2$ (it is obviously irreducible). Then, by previous theorem,

$\mathcal{B}(\mathbb{Q}(b)) = \{1, b\}$, i.e. $\mathcal{B}\left(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right) = \{1, \sqrt{2}\}$, and we have $\dim\left(\mathbb{Q}(\sqrt{2})\right) = 2$. The elements $\mathbf{v} \in \mathbb{Q}(\sqrt{2})$ can be written as $\mathbf{v} = k_0 \cdot 1 + k_1\sqrt{2} = k_0 + k_1\sqrt{2}$, for some $k_0, k_1 \in \mathbb{Q}$. Now let us return to $p(x)$ and a. We can see that $p(x) \in \mathbb{Q}(\sqrt{2})$, as coefficients of $p(x)$ are 1, -3, $\sqrt{2}$,6 and $-2\sqrt{2} - 4$, and all are in $\mathbb{Q}(\sqrt{2})$. But, is $p(x)$ minimal polynomial of a over $\mathbb{Q}(\sqrt{2})$? Assume there exist $p_2(x)$ and $p_1(x)$ such that $\deg p_2(x) = 2$, $\deg p_1(x) = 1$ and $p_2(a) = p_1(a) = 0$. Polynomial $p_1(x)$ cannot be minimal as it would have to be $p_1(x) = x - a$, and $a \notin \mathbb{Q}\sqrt{2}$. If $p_2(x)$ is minimal, then $p(a) = a^2 + ca + d = 0$, i.e. $(\sqrt{2} + \sqrt[3]{4})^2 + c(\sqrt{2} + \sqrt[3]{4}) + d = 0$. From that we have $2+2\sqrt{2}\sqrt[3]{4}+\sqrt[3]{16}+c\sqrt{2}+c\sqrt[3]{4}+d = 0$. So, we would need to have $2+\sqrt[3]{16}+c\sqrt[3]{4}+d = 0$ and $2\sqrt{3}[4]+c = 0$. Thus, we would get $c = -2\sqrt{3}[4]$, which is impossible as $c \in \mathbb{Q}(\sqrt{2})$ and $\sqrt{3}[4] \notin \mathbb{Q}(\sqrt{2})$. We know that, because $\sqrt{3}[4] = e + f\sqrt{2}$, cubed, would yield $4 = e^3+e^2f\sqrt{2}+2ef^2+2f^3\sqrt{2}$. From that we could get $\sqrt{2}(2f^3+e^2f) = 4-e^3+2ef^2$, i.e.

$$\sqrt{2} = \frac{4 - e^3 + 2ef^2}{2f^3 + e^2f}.$$

As e and f are in $\mathbb{Q}$, that would imply that the right-hand side of equality is also in $\mathbb{Q}$, which is impossible, as that would imply $\sqrt{2} \in \mathbb{Q}$. Thus, it must be that $\sqrt{3}[4] \notin \mathbb{Q}(\sqrt{2})$, and $p_1(x)$ and $p_2(x)$ cannot be minimal polynomials. Now, a is root of $p(x)$, and there are no polynomials of lesser degrees, so $p(x)$ has to be minimum polynomial of a over $\mathbb{Q}(\sqrt{2})$. Therefore, basis of $\mathbb{Q}(a)$ over $\mathbb{Q}(\sqrt{2})$ is $\mathcal{B}\left(\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})\right) = 1, a, a^2$ and $\dim\left(\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})\right) = 3$. Finally, it has to be $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 3 \cdot 2 = 6$. We can see that, by previous proposition:

$$\mathcal{B}(\mathbb{Q}(a) : \mathbb{Q}) = \{1, a, \sqrt{2}, a\sqrt{2}, a^2, a^2\sqrt{2}\}.$$

So, if we take $\mathbf{v} \in \mathbb{Q}(a)$ we have:

$$\begin{aligned} \mathbf{v} &= k_0 + k_1(\sqrt{2} + \sqrt[3]{4}) + k_2\sqrt{2} + k_3(\sqrt{2} + \sqrt[3]{4})\sqrt{2} \\ &\quad +k_4(\sqrt{2} + \sqrt[3]{4})^2 + k_5(\sqrt{2} + \sqrt[3]{4})^2\sqrt{2}. \end{aligned}$$

This can be reduced to:

$$\mathbf{v} = l_0 + l_1 2^{\frac{1}{2}} + l_2 2^{\frac{2}{3}} + l_3 2^{\frac{4}{3}} + l_4 2^{\frac{7}{6}}.$$

Problem. Find a basis of $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ over $\mathbb{Q}$, and describe the elements of $\mathbb{Q}(\sqrt{5}, \sqrt{7})$.

Solution. Let us observe $\mathbb{Q}(\sqrt{5}) : \mathbb{Q}$. If $\sqrt{5} = x$, we get $x^2 - 5 = 0$. By Eisenstein's

criterion it is easy to see that $p(x) = x^2 - 5$ is irreducible over $\mathbb{Q}$, and is therefore the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}$. Thus, $\mathcal{B}\left(\mathbb{Q}(\sqrt{5}) : \mathbb{Q}\right) = \{1, \sqrt{5}\}$ and we have $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Each element in $\mathbb{Q}(\sqrt{5}) : \mathbb{Q}$ can be shown as $a + b\sqrt{5}$. Then, let us see if $\sqrt{7} \in \mathbb{Q}(\sqrt{5})$. That would mean $a + b\sqrt{5} = \sqrt{7}$. Squaring this expression gives us $a^2 + 2ab\sqrt{5} + b^2\sqrt{5} = 7$. After some rearrangement that is equivalent to $\sqrt{5}(2ab + b^2) = 7 - a^2$, i.e. $\sqrt{5} = \frac{2ab+b^2}{7-a^2}$. Now, as a, b and 7 are all rational, then whole right-hand side of equality is also rational, which is impossible as $\sqrt{5}$ is irrational. Now, we have $x = \sqrt{7}$ which gives us $x^2 - 7 = 0$. Is $q(x) = x^2 - 7$ minimum polynomial of $\sqrt{7}$ over $\mathbb{Q}$? If it was $Q(x) = ax + b$, a polynomial of lesser degree, and $Q(\sqrt{7}) = 0 = a\sqrt{7} + b$ we would have $-b = a\sqrt{7}$, for some $a, b \in \mathbb{Q}(\sqrt{5})$. Taking $a^{-1} \in \mathbb{Q}(\sqrt{5})$ (as it is a field such element exists) gives us $-ba^{-1} = \sqrt{7}$. But, $-ba^{-1} \in \mathbb{Q}(\sqrt{5})$, while we just have shown that $\sqrt{7} \notin \mathbb{Q}(\sqrt{5})$. So, as $\sqrt{7}$ is root of $q(x)$, and there does not exist any polynomial of lesser degree whose root is $\sqrt{7}$, as we have shown, then it must be that $q(x)$ is indeed minimum polynomial of $\sqrt{7}$ over $\mathbb{Q}(\sqrt{5})$. So, $\mathcal{B}\left(\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})\right) = \{1, \sqrt{7}\}$ and $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})] = 2$. From that, using previous proposition, we get $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$, and $\mathcal{B}\left(\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}\right) = \{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$. That means that if $\mathbf{v} \in \mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}$, then $\mathbf{v} = k_0 + k_1\sqrt{5} + k_2\sqrt{7} + k_3\sqrt{35}$.

Problem. Find a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$ and describe $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Solution. We have $p(x) = x^2 - 2$ as minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ (obviously irreducible). Then, $\mathcal{B}\left(\mathbb{Q}(\sqrt{2})\right) = \{1, \sqrt{2}\}$, by previous proposition, and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Each element in $\mathbb{Q}(\sqrt{2})$ is of the form $a + b\sqrt{2}$. Now, we know that $\sqrt{3}$ is the root of $q(x) = x^2 - 3$, but is $q(x)$ minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. First, we will show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. If it were so, then there would exist $a, b \in \mathbb{Q}$ such that $a + b\sqrt{2} = \sqrt{3}$. Squaring this equality would give us $a^2 + 2ab\sqrt{2} + 2b^2 = 3$, i.e. $\sqrt{2} = \frac{3-2b^2-a^2}{2ab}$. But, as the right-hand side is rational, so it would mean that $\sqrt{2}$ is rational, which is a contradiction. Therefore, $\sqrt{3} \notin \mathbb{Q}$. Assume $q(x)$ is not minimal, and that there exists some $Q(x)$ such that $\deg Q(x) < \deg q(x)$. That would mean that only possibility is $Q(x) = ax + b$, where $a, b \in \mathbb{Q}(\sqrt{2})$. So, it also must be $Q(\sqrt{3}) = a\sqrt{3} + b = 0$. That is equivalent to $\sqrt{3} = -ba^{-1}$, where $-ba^{-1} \in \mathbb{Q}(\sqrt{2})$ which is a contradiction. So, as $q(\sqrt{3}) = 0$ and $q(x)$ has rational coefficients, which are in turn also in extension field, then $q(x)$ must be minimal polynomial. Therefore, $\mathcal{B}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\right) = \{1, \sqrt{3}\}$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. By previous proposition, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$ along with $\mathcal{B}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\right) = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Assume $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let us observe that as vector space over $\mathbb{Q}(\sqrt{2})$, with basis vectors 1 and $\sqrt{3}$. That would mean that $\sqrt{5} = a + b\sqrt{3}$, where $a, b \in \mathbb{Q}(\sqrt{2})$. Squaring this would yield $5 = a^2 + 2ab\sqrt{3} + 3b^2$, i.e. $\sqrt{3} = (5 - a^2 - 3b^2)(2ab)^{-1}$. But, as right-hand side

is obviously again in $\mathbb{Q}(\sqrt{2})$, it cannot be that it is equal to $\sqrt{3}$, as we have already shown $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. So it must be that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have $r(x) = x^2 - 5$ which is a minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. If it was not minimal, there would exist $R(x) = ax + b$, where $a, b \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. That would imply $R(\sqrt{5}) = a\sqrt{5} + b = 0$, i.e. $\sqrt{5} = -ba^{-1}$, so the right-hand side is again in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, while we have just shown $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. By previous proposition, it must be that $\mathcal{B}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})\right) = \{1, \sqrt{5}\}$ with $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$. Thus, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 4 = 8$ and $\mathcal{B}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}\right) = \{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$. Each $\mathbf{v} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ can be written as $\mathbf{v} = k_0 + k_1\sqrt{2} + k_2\sqrt{3} + k_3\sqrt{5} + k_4\sqrt{6} + k_5\sqrt{10} + k_6\sqrt{15} + k_7\sqrt{30}$.

Problem. Name an extension of $\mathbb{Q}$ over which π is algebraic of degree 3.

Solution. Let us observe π over $\mathbb{Q}(\pi^3)$. We have $p(x) = x^3 - \pi^3$, which is a polynomial in $\mathbb{Q}(\pi^3)[x]$, due to $\pi^3 \in \mathbb{Q}(\pi^3)$. Also, $p(\pi) = \pi^3 - \pi^3 = 0$. Then, $\mathbb{Q}(\pi)$ over $\mathbb{Q}(\pi^3)$ has basis $\{1, \pi, \pi^2\}$ and $[\mathbb{Q}(\pi) : \mathbb{Q}(\pi^3)] = 3$.

Proposition. Let F be a field and $\text{char}\,(F) \neq 2$. Let $a, b \in F - \{0\}$ be non-squares and $a \neq b$. Then,

1. $F\left(\sqrt{a} + \sqrt{b}\right) = F\left(\sqrt{a}, \sqrt{b}\right)$;
2. If $b \neq x^2 a$, for all $x \in F$, then $\sqrt{b} \notin F\left(\sqrt{a}\right)$ and $[F\left(\sqrt{a}, \sqrt{b}\right) : F] = 4$;
3. $F\left(\sqrt{a + b + 2\sqrt{ab}}\right) = F\left(\sqrt{a}, \sqrt{b}\right)$.

Proof. *Ad* 1. By previous proposition we have $F(\sqrt{a} + \sqrt{b}) \subseteq F(\sqrt{a}, \sqrt{b})$. Let us take $\sqrt{a} + \sqrt{b} \in F(\sqrt{a} + \sqrt{b}) = G$. Then, $(\sqrt{a} + \sqrt{b})^2 \in G$. But, $(\sqrt{a} + \sqrt{b})^2 = a + 2\sqrt{ab} + b$, and as $a, b \in F \subseteq G$, then $2\sqrt{ab} = (\sqrt{a} + \sqrt{b})^2 - a - b \in G$. Notice that $2\sqrt{ab} = \sqrt{ab} + \sqrt{a+b} = 1\sqrt{ab} + 1\sqrt{ab} = (1+1)\sqrt{ab} = (2 \cdot 1)(\sqrt{ab})$. As $1 \in G$ (neutral element), then $(2 \cdot 1) \in G$, and so it must be that $(2 \cdot 1)^{-1} \in G$ (as $\text{char}\,(F) \neq 2$, then $2 \cdot 1 \neq 0$ and so such inverse exists). Therefore, $(2 \cdot 1)^{-1}(2 \cdot 1)\sqrt{ab} \in G$, which implies $\sqrt{ab} \in G = F(\sqrt{a} + \sqrt{b})$. So it also must be that $\sqrt{ab}(\sqrt{a} + \sqrt{b}) = \sqrt{a^2 b} + \sqrt{b^2 a} = a\sqrt{b} + b\sqrt{a} \in G$. So, also $\sqrt{ab}(\sqrt{a} + \sqrt{b}) - b(\sqrt{a} + \sqrt{b}) = a\sqrt{b} + b\sqrt{a} - b\sqrt{a} - b\sqrt{b} = a\sqrt{b} - b\sqrt{b} \in G$, i.e. $\sqrt{b}(a - b) \in G$. As $(a - b) \in F$, then $(a - b)^{-1}$ is also in F. Thus, $\sqrt{b}(a - b)(a - b)^{-1} = \sqrt{b} \in G = F(\sqrt{a} + \sqrt{b})$. In the same way we can show $\sqrt{a} \in F(\sqrt{a} + \sqrt{b})$. Thus, as $F(\sqrt{a} + \sqrt{b})$ contains F, $\sqrt{a}$ and $\sqrt{b}$, and $F(\sqrt{a}, \sqrt{b})$ is smallest such field, it must be that $F(\sqrt{a}, \sqrt{b}) \subseteq F(\sqrt{a} + \sqrt{b})$, and that implies, along with the first result, that $F(\sqrt{a}, \sqrt{b}) = F(\sqrt{a} + \sqrt{b})$.

Ad 2. Let $b \neq x^2a$, for all $x \in F$, but $\sqrt{b} \in F(\sqrt{a})$. That implies $\sqrt{b} = k + l\sqrt{a}$, for some $k, l \in F$. Squaring this equality gives us $b = k^2 + 2kl\sqrt{a} + l^2a$, i.e. $0 = (k^2 + l^2a - b) \cdot 1 + (2kl)\sqrt{a}$. As $\{1, \sqrt{a}\}$ is basis of $F(\sqrt{a})$, then 1 and $\sqrt{a}$ are linearly independent, and it must be that $(k^2 + l^2a - b) = 0$ and $2kl = 0$, i.e. $kl = 0$. We have three cases. First, if $k = l = 0$. Then we simply have $0^2 + 0^2a - b = 0$ which would mean $b = 0$, contrary to our assumption that $a, b \neq 0$. Assume $k = 0$ and $l \neq 0$. Then, $0^2 + l^2a - b = 0$ gives us $l^2a = b$, which is contrary to assumption that $b \neq x^2a$, for all $x \in F$. Assume $k \neq 0$ and $l = 0$. Then, $k^2+0^2a-b = 0$ gives us $b = k^2$, which is contrary to assumption that a and b are non-squares. Thus it must be that $\sqrt{b} \notin F(\sqrt{a})$. But, there does exist $p(x) = x^2 - b$ such that $p(\sqrt{b}) = b - b = 0$, and it is obviously irreducible, as $q(x) = kx + l$, for $q(\sqrt{b}) = 0 = k\sqrt{b} + l$ would imply $-lk^{-1} = \sqrt{b}$, i.e. that $\sqrt{b} \in F(\sqrt{a})$ (we have just shown it is not the case). Thus, $p(x)$ is minimal polynomial of $\sqrt{b}$ over $F(\sqrt{a})$. So, $\mathcal{B}\left(F(\sqrt{a}, \sqrt{b}) : F(\sqrt{a})\right) = \{1, \sqrt{b}\}$, and by previous proposition, $\mathcal{B}\left(F(\sqrt{a}, \sqrt{b}) : F\right) = \{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$, i.e. $[F(\sqrt{a}, \sqrt{b}) : F] = 4$.

Ad 3. Let $u = \sqrt{a + b + 2\sqrt{ab}}$. Then, $u^2 = a + b + 2\sqrt{ab}$, i.e. $u^2 - (a + b) = 2\sqrt{ab}$. Squaring that gives us $u^4 - 2u^2(a + b) + a^2 - 2ab + b^2 = 0$. That is equivalent to $u^4 - 2u^2(a+b) + (a-b)^2 = 0$. If we took $v = \sqrt{a} + \sqrt{b}$ we would get $v^2 = a + 2\sqrt{ab} + b$. It is easy to see that by squaring $v^2 - (a + b) = 2\sqrt{ab}$, we would get $v^4 - 2v^2(a + b) + (a - b)^2 = 0$. So, both u and v are roots of $p(x) = x^4 - 2x^2(a + b) + (a - b)^2$. As $p(u) = p(v)$, it must be that $u^4 - 2(a+b)u^2 + (a-b)^2 = v^4 - 2(a+b)v^2 + (a-b)^2$, i.e. $u^4 - 2(a + b)u^2 = v^4 - 2(a + b)v^2$. That implies $u^4 - v^4 - (2(a + b)u^2 - 2(a + b)v^2) = 0$, or simplified as $u^4 - v^4 - 2(a + b)(u^2 - v^2) = 0$. Further simplification gives us $(u^2 - v^2)(u^2 + v^2) - 2(a + b)(u^2 - v^2) = 0$ and $(u^2 - v^2)(u^2 + v^2 - 2(a + b)) = 0$. Now, using elementary algebra we get $(u - v)(u + v)(u^2 + v^2 - 2(a + b)) = 0$. From this, $u - v = 0$ or $u + v = 0$ or $u^2 + v^2 - 2(a + b) = 0$. Let us examine the latter case. We would have $(a + b + 2\sqrt{ab}) + (a + b + 2\sqrt{ab}) - 2(a + b) = 0$, which amounts to $4\sqrt{ab} = 0$. But that would imply $ab = 0$, i.e. $a = 0$ or $b = 0$, both of which are contradictory to assumption that $a, b \neq 0$. So, it must be $u - v = 0$ or $u + v = 0$. If $u - v = 0$, then obviously $F(u) = F(v)$. If $u + v = 0$, then $u = -v$, which would mean $v \in F(u)$. As $F(v)$ is the smallest field containing F and v, and also $F \subseteq F(u)$, then it must be that $F(v) \subseteq F(u)$. Also as $v = -u$, we have $u \in F(v)$, which in same way implies $F(u) \subseteq F(v)$. In other words, we have proved that $F(u) = F(v)$, that is $F(\sqrt{a + b + 2\sqrt{ab}}) = F(\sqrt{a} + \sqrt{b})$. But, $F(\sqrt{a} + \sqrt{b}) = F(\sqrt{a}, \sqrt{b})$ by a previous proposition, so $F(\sqrt{a + b + 2\sqrt{ab}}) = F(\sqrt{a}, \sqrt{b})$. Previous problem tells us of how the field $F(\sqrt{a + b + 2\sqrt{ab}})$ looks like, if $a \neq x^2b$ for all $x \in F$.

□

Problem. Find an uncomplicated basis for $\mathbb{Q}(d) : \mathbb{Q}$ where d is a root of $x^4 - 14x^2 + 9$.

Solution. Notice that $-14 = -2(a+b)$, that is $7 = a+b$ and $9 = (a-b)^2$, i.e. $3 = a-b$.

This gives us $a = 5$ and $b = 2$, as in previous proposition. Thus, $d = \sqrt{7 + 2\sqrt{10}}$ and we have $\mathbb{Q}(d) = \mathbb{Q}(\sqrt{7 + 2\sqrt{10}}) = \mathbb{Q}(\sqrt{5}, \sqrt{2})$, by previous proposition. Then, $\mathcal{B}\left(\mathbb{Q}(\sqrt{5}, \sqrt{2}) : \mathbb{Q}\right) = \{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$.

Proposition. Let F be a field, and let c be algebraic over F with $[F(c) : F] = m$. Then, each element of $F(c)$ can be written uniquely as $a_0 + a_1 c + \cdots + a_{m-1}c^{m-1}$, for some $a_0, a_1, \ldots, a_{m-1} \in F$.

Proof. As $[F(c) : F] = m$, then $p(x) = c^m + k_{m-1}c^{m-1} + \ldots + k_1 c + k_0$, and so, by previous theorem, $\mathcal{B}\left(F(c) : F\right) = \{1, c, c^2, \ldots, c^{m-1}\}$. Now, assume $\mathbf{v} = a_{m-1}c^{m-1} + \ldots + a_1 c + a_0$ and $\mathbf{v} = b_{m-1}c^{m-1} + \ldots + b_1 c + b_0$. Then, $a_{m-1}c^{m-1} + \ldots + a_1 c + a_0 = b_{m-1}c^{m-1} + \ldots + b_1 c + b_0$ and we have $c^{m-1}(a_{m-1} - b_{m-1}) + \ldots + c(a_1 - b_1) + (a_0 - b_0) = \mathbf{0}$. As $\{1, c, c^2, \ldots, c^{m-1}\}$ is basis of $F(c) : F$, they are linearly independent, implying $a_{m-1} - b_{m-1} = \ldots = a_1 - b_1 = a_0 - b_0 = 0$, i.e. $a_i = b_i$ for all $i \in \{0, 1, \ldots, m-1\}$. Thus, each $\mathbf{v}$ can be written in a unique manner as $\mathbf{v} = a_{m-1}c^{m-1} + \ldots + a_1 c + a_0$.

□

Problem. Construct a field of four elements as an extension of $\mathbb{Z}/2\mathbb{Z}$. Describe its elements, and supply its addition and multiplication tables.

Solution. Notice that $\overline{0} + \overline{0} + \overline{1} = \overline{1}$ and $\overline{1} + \overline{1} + \overline{1} = \overline{1}$. Thus, $p(x) = x^2 + x + \overline{1}$ has no roots, and, as it is of degree 2, it is irreducible, and also monic. Let c be such element that $c^2 + c + \overline{1} = \overline{0}$. Then, $\mathcal{B}\left(\mathbb{Z}/2\mathbb{Z}(c) : \mathbb{Z}/2\mathbb{Z}\right) = \{1, c\}$ and if $\mathbf{v} \in \mathbb{Z}/2\mathbb{Z}(c)$, then $\mathbf{v} = \overline{k}c + \overline{l}$. We can see that $\mathbb{Z}/2\mathbb{Z}(c)$ has four elements (two for $\overline{k}$ and two for $\overline{l}$). Addition table for $\mathbb{Z}/2\mathbb{Z}(c)$ is:

$+$	$\overline{0}$	$\overline{1}$	c	$\overline{1} + c$
$\overline{0}$	$\overline{0}$	$\overline{1}$	c	$\overline{1} + c$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1} + c$	c
c	c	$\overline{1} + c$	$\overline{0}$	$\overline{1}$
$\overline{1} + c$	$\overline{1} + c$	c	$\overline{1}$	$\overline{0}$

For multiplication table, notice that $c^2 = c + \overline{1}$ and $c^2 + c = \overline{1}$ which we get from definition $c^2 + c + \overline{1} = \overline{0}$. Multiplication table for $\mathbb{Z}/2\mathbb{Z}(c)$ is as follows:

$\cdot$	$\overline{0}$	$\overline{1}$	c	$\overline{1} + c$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	c	$\overline{1} + c$
c	$\overline{0}$	c	$\overline{1} + c$	$\overline{1}$
$\overline{1} + c$	$\overline{0}$	$\overline{1} + c$	$\overline{1}$	c

Problem. Construct a field of eight elements as an extension of $\mathbb{Z}/2\mathbb{Z}$.

Solution. We have seen that $|\mathbb{Z}/2\mathbb{Z}(c)| = 4$, where $c^2 + c + \overline{1} = \overline{0}$. Now, if we take some $p(x) \in \mathbb{Z}/2\mathbb{Z}(c)$ such that it is irreducible and of degree 2, we can construct a field of eight elements based upon the former field. Notice that $x^2 \in \{\overline{1}, \overline{1} + c, c\}$, for all $x \in \mathbb{Z}/2\mathbb{Z}(c)$. Using this, we can think of an irreducible polynomial of degree two. Let us observe also $p(x) = x^2 + x$. We have $p(\overline{1}) = \overline{1} + \overline{1} = \overline{0}$, $p(c) = c + \overline{1} + c = \overline{1}$ and $p(c + \overline{1}) = c + c + \overline{1} = \overline{1}$. Of course, $p(\overline{0}) = \overline{0}$. As $p(c) = p(\overline{1} + c) = \overline{1}$, adding $\overline{1}$ to $p(x)$ would make it zero, but adding c would make all $p(x) \neq \overline{0}$. So, we are looking for $p(x) = x^2 + x + c$, which is monic and irreducible (it is of degree two and has no roots in $\mathbb{Z}/2\mathbb{Z}(c)$). Now, taking for a rule $d^2 + d + c = \overline{0}$, we arrive at $\mathcal{B}(\mathbb{Z}/2\mathbb{Z}(c, d) : \mathbb{Z}/2\mathbb{Z}(c)) = \{\overline{1}, d\}$, but by previous proposition, $\mathcal{B}(\mathbb{Z}/2\mathbb{Z}(c, d) : \mathbb{Z}/2\mathbb{Z}) = \{\overline{1}, c, d, cd\}$. Thus, every $\mathbf{v} \in \mathbb{Z}/2\mathbb{Z}(c, d)$ can be shown as $\mathbf{v} = k_0\overline{1} + k_1 c + k_2 d + k_3 cd$, for some $k_i \in \mathbb{Z}/2\mathbb{Z}$, where $i \in \{0, 1, 2, 3\}$. We can see that, we have 2 choices for each k_i, and therefore, all in all, 8 possible elements in $\mathbb{Z}/2\mathbb{Z}(c, d)$.

Proposition. Let F be a finite field such that $|F| = n$. If c is algebraic over F with $[F(c) : F] = m$, then $|F(c)| = n^m$.

Proof. As $[F(c) : F] = m$, then minimal polynomial of c over F is of degree m and $\mathcal{B}(F(c)) = \{1, c, c^2, \ldots, c^{m-1}\}$. Then every $\mathbf{v} \in F(c)$ can be shown as $\mathbf{v} = k_0 + k_1 c + k_2 c^2 + \ldots + k_{m-1} c^{m-1}$. For each choice of k_i we have n possibilities, as $k_i \in F$ and $|F| = n$. Also, due to previous proposition, this can be done in unique manner. Therefore, in total, we have n^m vectors in $F(c) : F$.

□

Proposition. For every $p \in P$ there exists a field with p^2 elements.

Proof. We have already shown the case for $p = 2$. Now, we know that $\mathbb{Z}/p\mathbb{Z}$ is a field. So, if we took $q(x) = x^2 + \overline{c}$, where $\overline{c} \in \mathbb{Z}/p\mathbb{Z}$, then $q(x)$ would be irreducible if and only if it had no roots in $\mathbb{Z}/p\mathbb{Z}$. How many elements in $\mathbb{Z}/p\mathbb{Z}$ are squares? Well, setting aside $\overline{0}$, it leaves $p-1$ elements to consider. As $(\overline{m - a})^2 = \overline{m}^2 - 2\overline{ma} + \overline{a}^2 = \overline{a}^2$, it is evident that there are $\overline{p - 1}2$ squares (if not exactly, then surely less than that) in $\mathbb{Z}/p\mathbb{Z}$. Adding $\overline{0}$ makes it $\overline{p + 1}2$ squares. Thus, there exist $\overline{p - 1}2$ elements that are not squares, and that much elements we can choose for $\overline{c}$ so $q(x)$ will have no roots, and thus irreducible. Assume $d^2 = -\overline{c}$. Extension $\mathbb{Z}/p\mathbb{Z}(d)$ is then of degree 2 (due to $q(x)$ being of degree 2). By previous proposition, as $|\mathbb{Z}/p\mathbb{Z}| = p$ and $[\mathbb{Z}/p\mathbb{Z}(d) : \mathbb{Z}/p\mathbb{Z}] = 2$, we have $|\mathbb{Z}/p\mathbb{Z}(d)| = p^2$.

□

Summa Summarum

Let $C, D \neq \emptyset$.

Relation $\mathcal{R} = \{(x, y) : \ x \in D, \ y \in C\} \subseteq D \times C$ (we write $x\mathcal{R}y$ if $(x, y) \in \mathcal{R}$) is:

- **left-total** if $(\forall x \in D)(\exists y \in C) : \ (x, y) \in \mathcal{R}$;
- **right-total** if $(\forall y \in C)(\exists x \in D) : \ (x, y) \in \mathcal{R}$;
- **one-to-many** if $(\forall y \in C)(\forall x_1, x_2 \in D) : \ (x_1, y) \in \mathcal{R}, (x_2, y) \in \mathcal{R} \to x_1 = x_2$;
- **many-to-one** if $(\forall x \in D)(\forall y_1, y_2 \in C) : \ (x, y_1) \in \mathcal{R}, (x, y_2) \in \mathcal{R} \to y_1 = y_2$;
- **one-to-one** if one-to-many and many-to-one.

Domain of relation $\mathcal{R} \subseteq D \times C$ is set D.

Codomain of relation $\mathcal{R} \subseteq D \times C$ is set C.

Function $f : D \to C$ is a *left-total*, *many-to-one* relation $f \subseteq D \times C$ called

- **injective** if one-to-many;
- **surjective** if right-total;
- **bijective** if injective and surjective.

Domain of function $f : D \to C$ is set D.

Codomain of function $f : D \to C$ is set C.

Image of function $f : D \to C$ is set $\mathrm{Im}(f) = \{y \in C : \ y = f(x)\}$.

Partial binary operation $*$ is a many-to-one relation $* \subseteq (D^2 \times D)$.

Binary operation $*$ is a function $* : D^2 \to D$.

A **partition** of a set A is a family $\{A_i : \ i \in I\}$ of nonempty subsets of A such that:

1. $(\forall x \in A)\,(\forall i, j \in I)\,(x \in A_i \wedge x \in A_j) \Rightarrow A_i = A_j$;

2. $(\forall x \in A)\,(\exists i \in I)\,(x \in A_i)$.

Let S be a non-empty set. We say that $\mathcal{R} = \{(a, b) :\ a, b \in S\}$ is an **equivalence relation**, if:

- $(\forall a \in S) :\ a\mathcal{R}a$ (**reflexivity**);
- $(\forall a, b \in S) :\ a\mathcal{R}b \to b\mathcal{R}a$ (**symmetry**);
- $(\forall a, b, c \in S) :\ (a\mathcal{R}b \wedge b\mathcal{R}c) \to a\mathcal{R}c$ (**transitivity**).

Let $\sim$ be an equivalence relation on A and $x \in A$. **Equivalence class** of x is $[x] = \{y \in A :\ y \sim x\}$.

Ordered pair $(S, *)$ with $S \neq \emptyset$ is called:

- **partial magma** if $*$ is a partial binary operation;
- **magma** (groupoid) if $* : S^2 \to S$ is a binary operation;
- **semigroup** if $(S, *)$ is magma and $(\forall x, y, z \in S) :\ x * (y * z) = (x * y) * z$;
- **monoid** if $(S, *)$ is semigroup and $(\exists e \in S)(\forall x \in S) :\ e * x = x * e = x$;
- **group** if $(S, *)$ is monoid and $(\forall x \in S)(\exists x^{-1} \in S) :\ x^{-1} * x = x * x^{-1} = e$;
- **Abelian group** if $(S, *)$ is group and $(\forall x, y \in S) :\ x * y = y * x$.

Let G be a group and $S \neq \emptyset$. S is a **subgroup** of G if:

- $S \subseteq G$,
- $(\forall x, y \in S) :\ x * y \in S$,
- $(\forall x \in S) :\ x^{-1} \in S$.

Center of a group G is a subgroup $C = \{a \in G :\ xa = ax,\ \forall x \in G\}$.

Subgroup of G **generated by** $\{a_1, \ldots, a_n\} \subseteq G$ is a subgroup S such that:

- $a_1, \ldots, a_n, a_1^{-1}, \ldots, a_n^{-1} \in S$;
- $(\forall a \in S) :\ a$ is expressible as an arbitrary product of $a_1, \ldots, a_n, a_1^{-1}, \ldots, a_n^{-1}$.

Cyclic subgroup $\langle a \rangle$ of G is a subgroup of G generated by $\{a\} \subseteq G$.

Permutation is any bijection of the form $f : A \to A$.

Group of permutations S_A on A is called **symmetry group** on A.

Let $p(x_1, \ldots, x_n) = \sum \prod_{j=1}^{n} x_j^{y_j}$, where $0 \leq y_j \leq m$, be a polynomial. The **symmetries of a polynomial** p are all the permutations of subscripts of x_j that leave p unchanged.

Cycle is a permutation $f : A \to A$ (where A is finite) such that $[\underbrace{f \circ f \circ \cdots \circ f}_{n+1 \text{ times}}](a) = a$ and $[f \circ f](a) \neq a$ for some $a \in A$ and $[f \circ f](x) = x$ for all $x \in A \backslash \{a\}$. Number n is called the **length of the cycle** f. Cycle of length 2 is called a **transposition**.

Subgroup A_n of even permutations in S_n is called **alternating group**.

Let $(G_1, \odot)$ and $(G_2, \otimes)$ be groups. If there exists a bijection $f : G_1 \to G_2$ such that $f(a \odot b) = f(a) \otimes f(b)$, for all $a, b \in G_1$, we say that group G_1 is **isomorphic** to group G_2 and write $G_1 \cong G_2$. Such function f is called an **isomorphism** from G_1 to G_1.

Let G be a group and $G^* = \{\pi_a : \ a \in G\}$, where $\pi_a : G \to G$ is a permutation on G. We say that G^* is:

- **left regular representation** of G if $\pi_a(x) = ax$;
- **right regular representation** of G if $\pi_a(x) = xa$;
- **regular representation** of G if G is commutative.

If G is a group, an **automorphism** of G is an isomorphism from G to G.

Let G be a group and H a subgroup of G. Let $a \in G$. A **left coset** of H in G is defined as $aH = \{y \in G : \ (\forall h \in H)(y = ah)\}$. A **right coset** of H in G is $Ha = \{y \in G : \ (\forall h \in H)(y = ha)\}$.

If $a \in G$, a **conjugate** of a is any element of the form xax^{-1}, where $x \in G$.

Let $a \in G$ and $\sim$ an equivalence relation on G such that $a \sim b$ if and only if $a = xbx^{-1}$ for some $x \in G$. **Conjugacy class** of a is the set $[a]_c = \{xax^{-1} : \ x \in G\}$.

For any element $a \in G$, the **centralizer** of a is the set $C_a = \{x \in G : \ xa = ax\} = \{x \in G : \ xax^{-1} = a\}$.

Let A be a set, and G a subgroup of S_A (group of all the permutations of A). We say that G is a **group acting on the set** A.

Let G be a finite group acting on the set A. If $a \in A$, then the **orbit** of a, with respect to G, is the set $O(a) = \{g(a) \in A : \ g \in G\}$.

Let G be a group acting on the set A. The **stabilizer** of $a \in A$, with respect to G, is the set $G_a = \{g \in G : \ g(a) = a\}$.

Let G and H be groups. Function $f : G \to H$ is called a **homomorphism** from G to H if $f(ab) = f(a)f(b)$, for all $a, b \in G$. Then, H is called a **homomorphic image** of G.

Let $f : G \to H$ be a homomorphism from group G to group H. Then, the **kernel** of f is the set $\ker(f) = \{a \in G : \ f(a) = e\}$. The **range** of f is the set $\text{ran}(f) = \{f(a) \in H : \ a \in G\}$.

Let G be a group and H a subgroup of G. If $xyx^{-1} \in H$, for all $y \in H$ and $x \in G$, then H is called a **normal subgroup** of G.

Let G be a group. A **commutator** is any product of the form $aba^{-1}b^{-1}$, where $a, b \in G$.

Let G be a group, H a subgroup of G and $a \in G$. Set $aHa^{-1} = \{aha^{-1} : \ h \in H\}$ is a **conjugate** of H.

Let G be a finite group and H a subgroup of G. Set

$$N(H) = \left\{a \in G : \ (\forall h \in H)\left(aha^{-1} \in H\right)\right\}$$

is the **normalizer** of H.

Let G be a group and H a normal subgroup of G. Then, $G/H = \{Ha : \ a \in G\}$ with coset multiplication defined as $Ha \cdot Hb = H(ab)$ is a **quotient group** (sometimes a **factor group**).

Group G is called a p**-group** if the order of all elements of G is a power of p.

Appendix A. Kantian and Analytic Notions

Definition. A *proposition* is any statement whose truth value (true-false being the usual) can be determined. Proposition is composed of a *subject*, which determines what the proposition is about, and a *predicate* which describes the subject, i.e. tells us something about it. A proposition is said to be *analytic* if the predicate is contained in the subject; if the predicate is not contained in the subject, the proposition is said to be *synthetic*.

Definition. Knowledge can be thought of as a set of propositions to which an individual can ascribe a truth value. We can say that something is known *a priori* if it is known independent of the information derived from our senses; independent of experience. Something is known *a posteriori* if the information about it is derived from our senses, i.e. from experience. We can think about these terms in the absolute or in the relative sense. We have defined it so far in the absolute sense. Now, the *relative a priori* knowledge is actually something that *can* be known through the senses, but is not. *Relative a posteriori* knowledge is in opposition to relative a priori knowledge. It is something that *can* be and *is* known through the senses.

Definition. *Type* is the class of things in the universal, abstract sense. It is, actually, derived by considering properties in common to some set of objects. *Token* is a concrete incarnation of the class, i.e. type, in reality.

Clarification. Relative a priori knowledge is, furthermore, different from absolute a priori knowledge in the way that the referent of the former is type and of the latter token.

Definition. *Representation* is the collection of *phenomena* (the way we perceive outside objects). *Nomena* is the object-in-itself, as it is outside, not the way it is perceived.

Definition. A subject can be viewed from two different angles in *sense-reference categories*. It can be viewed as *sense*, in which case it tells us the way something is. If it is viewed from the point of *reference*, it tells us just what something is and nothing else.

Definition. A subject can be viewed from two different angles in *mention-use categories*. Through *mention* we are only talking about the subject in the context of denotation, representation, etc. I use it more broadly, to talk about notation in the more abstract sense, not completely as a string of symbols. Through *use* we are talking about what the subject really is; in the context of how it is used (colloquially speaking).

Definition. *Abstraction* is a negative movement, while *concretization* is a positive movement. Abstraction moves the point of thought from the subject by removing its properties. Concretization moves the point of thought to the subject by further defining and describing it through it's properties. *Deduction* is a method of *conclusion-making* through the use of concretization. *Induction* is an opposite of deduction; we conclude through the use of abstraction. *Abduction* is the combination of the both, we make a conclusion by concretization, observation and then by abstraction.

Appendix B. Critique of Classical Logic

On analytic a priori truths. Rationalists' main argument was that there do exist analytic a priori truths and that all analytic propositions were of the a priori class. The main example were tautologies, law of identity, etc. To contradict them would be irrational, as it would enforce a contradiction. For example, if we say that it is not $A = A$, that would mean that $A \neq A$, which is the breach of the law of non-contradiction. Therefore, some truths must be known independent of experience. Now, Kant has proved that there do exist synthetic a priori truths by using examples in mathematics (he considered mathematics to be a pure science). But, I do argue against rationalists by saying that the breach of non-contradiction does not enforce necessity of existence, for the law of non-contradiction is, as Schopenhauer similarly mentioned, based on our reason to believe that it is not otherwise. It is only an assumption-axiom, one would have to prove that it is absolute. But in order to prove that, one would have to use logic to do so, which is in turn based on the law of non-contradiction, and so it would go against the forbidance of circular reasoning.

On synthetic a priori truths. Now, Kant has argued against rationalists that there do exist some synthetic a priori truths, i.e. not all analytic propositions are a priori. One of the examples was that $5 + 2 = 7$ is a synthetic proposition. I have already defined what a synthetic proposition is; we cannot find the predicate in the subject. Now, for this expression one does not need empirical evidence from Kant's point of view. Therefore it is a priori. And one also cannot find 7 nor in 5 nor in 2, nor in the $5 + 2$. Therefore it must be synthetic. I, on the other hand say that this is true, considering only the semiotic sphere. We indeed, cannot find predicate in the subject, but it's only in the mention-sense, not in the use-sense. Therefore, altough I cannot see 7 nor in 5, nor in 2, I in fact do know, that the expression itself, as a process, yields 7. The result of the process of addition is 7. I may say that in the use-sense one can find predicate in this subject. For if we were to say that it is not, we would need to view $5 + 2$ as a process and 7 as a number. But, how can a process equal an object, in this case, a number? Then we would need to view the equal sign as "the result of the process on the left-hand side is". In that case, which would, in my opinion be final, one would see that one can see 7 in $5 + 2$. Knowing that equality is not the same in language as in mathematics, that it's only a short for the former expression, one could then argue against $A = A$, the law of identity. If A were the process, then how can the result of a process be a process itself, the same as the one before? It would indeed, not say that A equals A, but would in fact define A as a never-ending process, the one whose result is itself. The main confusion was in the fact that we usually say "is" or "equals" for short; much better would be "yields" or "gets us", if not the forementioned expression. Now, if Kantian view was indeed correct, then it would mean that $5 + 2$ is

in fact the number 7 itself. And for that, he would be right in the use-sense, which is incorrect, as the process cannot equal an object. The number 7 already hides in that process, whose result we do indeed know, but it's as if we were waiting for it to be finished, and can't see the number 7 inside. But if we already, beforehand, a priori, know the result is 7, then we indeed must know what the result of the $5+2$ process was. Therefore, in my opinion, there do not exist nor analytic a priori truths, nor synthetic a priori truths. In fact, I would argue against any a priori knowledge, for $5 + 2 = 7$ is something that is actually learned from experience. But, the long-use of that fact in our society has led to its absolute acceptance, as something that was obvious. That is true in the mention sense. But, the very values themselves cannot be learned. One cannot learn that 5 rocks plus 2 rocks yields 7 rocks (where numbers now should not be viewed in the mention sense). It also cannot be seen, for we do not know beforehand that 7 in the mention-sense is actually what is in use-sense. It is our agreement, that we used to denote use-7 by symbol "7" and to think of it as an abstraction of the use-7 as the mention-7. That process cannot be learned. Only an agreement of the symbols can be learned. Therefore, if we do indeed view $5 + 2$ as a process, then it really is a priori. But then cannot be synthetic.

Appendix C. On Formulaic Mention-Sense

Now, the motivation for the distinction about to be made more clear is due to, what I believe, true misunderstanding of Bertrand Russell's paradox. It's a sort of a magic trick, that allows us to believe that everything goes according to some sort of plan, the magician shows us step by step necessary actions, assuring us that they are valid, but then comes the prestige which reveals something unexpected, leaving us in awe and misbelief into the very prestige itself; yet the point is not contained within the prestige, it is in the misinterpretation of the steps. And one of the crucial steps that were misinterpreted in Russell's paradox is that the formula itself is valid. Not through axiomatics, but through our own interpretation. We would never consider a formula $ab* = \langle x :\leftarrow$ valid, as it contains nothing of the sort that we got used to through our experience in mathematics. In addition, it contains symbols that don't have a meaning in standard arithmetic at all, leaving us to not even try to interpret such a formula and we are forced to call it *noise*. Now, the fluctuation itself, the deviation from this pattern of thought, is hidden in Russell's paradox. As we are used to, in set-theoretic area and sense, all of the symbols and their combinations in the definition of the set used in paradox, we do not even try to not interpret formula at all, rather believing it to be meaningful, due to interesting outcome, than dismissing it a priori. This further led to one of the most ugly concepts in mathematics and that is ZFC axiomatic system. We are forced to view mathematics as a strict game with strict rules, we are forced to dismiss our intuition in favor of an axiomatic system, and we forget that it was intuition in the first place that brought us ZFC axioms. Modern mathematician is sort of a Jewish analogue; Moses brought ten commandments and they are not questioned but obeyed without hesitation. And, in the age of "raving nihilism" as Zizek called it, one fails to see that this point of view, glorified by modern pseudophilosophers, is actually nihilism. Now, with Putnam's non-sensical thought experiments and with such axiomatics, one fails to see that in both systems, there is a great negation of more aspects of reality that appear to be positive, but are rather negative in nature. If in philosophy, one chooses to replace the idea of God and transcendetality with some vague notion of other-immortality and transcendentality of human mind, then one is negating, not only God, but the opposite fact, and that is that everything is contained without infinity restriction. One is able to speak about philosophical zombies, and that two straight lines intersect, but under condition that it happens in infinity (p-zombie problem is a thought experiment, and I am bound to say that every thought experiment is real in a point in infinity). And, saying that something happens or does not happen at a point in infinity is the equivalent of saying that it does not happen at all. For then, we can talk about Gods of Olympus as everything is true beyond infinity, it is not verifiable. One is led to believe that in mathematics, operations with infinity are absolute, as one of the most misleading facts that one over zero is infinity, or that one

over infinity is zero. Here comes the punchline, and it is in misinterpretation of the copula. We must say that it tends to infinity or that it tends to zero, respectively, and not use the copula at all. The notion of limits must be used with strict care, and through such semantical absolutists, mathematician has forgotten to think (like a social science through statistics) and to use expressions technicaly. In order to further my theories, I will use a function to distinguish an alphabetic expression, i.e. string from a meaningful mathematical expression. I can say that $R = \{x : \ x \notin X\}$ is a *string* and not a meaningful expression. The same thing goes for $ab* = \langle x :\leftarrow$. Now, let α be an alphabet consisting of symbols used within some theory. Then, α^* is a set of all possible symbols throught the use of concatenation from α. Now, we will say that $\xi \in \alpha*$ iff $\xi \in \alpha^n$, for some $n \in \mathbb{N}$. Now, let α_* be the set of all meaningful expressions. We define a partial function $\Xi : \alpha^* \to \alpha_*$, that is, a *conversion function* from a string to a meaningful mathematical expression. Furthermore, we will define a *breaking function* $B : \alpha^* \times \alpha \to \alpha_*$ such that, if $\xi = (\xi_1, \xi_2, \ldots, \xi_n) \in \alpha^*$ and $\odot \in \alpha$, then $B(\xi, \odot) = \Xi(\xi_1 \odot \xi_2 \odot \cdots \odot \xi_n)$.

For further explanations, examples and justifications... *Je n'ai pas le temps...* Yet the answer is in my head, clear as sky on a beautiful sunny day...