Berkeley Math 113: Abstract Algebra

Sohil Doshi

September 22, 2021

Contents

§1 Introduction

Chapter 1: Sets
Chapter 2: Groups
Chapter 3: Permutation Groups
Chapter 4: Rings
Chapter 5: Fields

The three main topics in this class will be groups, rings, and fields (permutation groups are a special type of group). The textbook for this class is I.N. Herstein, Abstract Algebra, Third Edition. When referring to problems in these notes, we will be referring to them from this book.

§2 Foreshadowing (Chapter 1)

Important note: We will not always be working in the real numbers ($\mathbb{R}$) all the time. It is important to know what you are working in because operations like addition and multiplication can possibly act differently in different sets of numbers like the complex numbers.

Question — Does $0 \cdot x = 0$ always?

Solution: If $x \in \mathbb{R}$, then the answer is yes but however if $x \notin \mathbb{R}$ then the answer is no because $0 \cdot \infty =$ undefined which is a counterexample. □

Question — Does $AB = BA$ always hold?

Solution: If $A, B \in \mathbb{R}$ and we are talking about the multiplication operator, then yes this holds. But if A, B are $2 \cdot 2$ matrices, then $AB = BA$ does not hold. □

Question — Does $AB = AC \longrightarrow B = C$ if $A \neq 0$?

Solution: If $A, B, C \in \mathbb{R}$, then yes this is true. However if A, B, C are $2 \cdot 2$ matrices, then this is not true because not all matrices have an inverse, specifically the matrices that have a determinant equal to 0 do not have an inverse. □

Question — If $AB = 0$ then does $A = 0$ or $B = 0$?

Solution: In $\mathbb{R}$, then yes this is true but in some other places like $2 \cdot 2$ matrices then this is no longer true as there are many counterexamples that we can find.

Consider $2 \cdot 2$ matrices over $\mathbb{R}$. Take the subset of $2 \cdot 2$ matrices over $\mathbb{Z}$ (set of integers). Very few will now have a multiplicative inverse because each element of the matrix has to be an integer. What if we talked about $2 \cdot 2$ matrices over the even integers? Note this is a subset of the set of $2 \cdot 2$ matrices over $\mathbb{Z}$. This subset wouldn't have an identity element so inverses wouldn't even make sense. □

Takeaway. Operations that work in the real numbers or identities that hold in the real numbers will not always hold when we work over different sets like the set of $2 \cdot 2$ matrices or the set of complex numbers.

Consider the following equation $f(x) = 0$ where $f(x) = x^2 - x - 1$. Can we say for sure whether $f(x)$ has a root in the interval $(1, 2)$ without solving the equation. Yes we are able to since we can use the intermediate value

theorem. Now consider the functions $g(x) = x^4 - x - 1$ and $h(x) = x^5 - x - 1$. Using the same logic, by the intermediate value theorem, both equations have a root in the interval $(1, 2)$. But are we able to explicitly find roots to $g(x)$ and $h(x)$ like we were able to find for $f(x)$. We are able to find solutions for $g(x)$ but we are not able to find solutions to $h(x)$ because there doesn't exist any formula for roots of a polynomial with degree 5 or higher while there do exist formulas for roots for quadratics, cubics, and quartics.

Question — What does $2^{\frac{1}{4}}$ mean?

Solution: Are there multiple values of $2^{\frac{1}{4}}$ over $\mathbb{R}$ or $\mathbb{C}$? This depends on the context. In calculus this is defined to be the positive real solution to $x^4 = 2$; we want it, in this context, to have only one value otherwise $f(x) = x^{\frac{1}{4}}$ would not be a function. Another way to define $2^{\frac{1}{4}}$ is all complex numbers z for which $z^4 = 2$. In this context, there are four distinct values for z. □

Question — Is $2^{\frac{2}{8}} = 2^{\frac{1}{4}}$?

Solution: We can rewrite $2^{\frac{2}{8}} = 4^{\frac{1}{8}}$ and we know that $4^{\frac{1}{8}}$ has 8 distinct solutions however $2^{\frac{1}{4}}$ has 4 distinct solutions. This again depends on the context. If it is defined using the calculus definition, then yes they are the same but if we are using the definition we used for complex numbers, then it gets a bit tricky. □

Let n, m be positive integers, then

$$x^{\frac{n}{m}} = (x^{\frac{1}{m}})^n$$

depends on the context.

Note that $x^n = x \cdot x \cdot ... \cdot x$ where there are n $x's$.

Consider $2 \cdot 2$ matrices over $\mathbb{R}$. Then we know that there is only one value of

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

But how would we define $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{\frac{1}{3}}$. Intuitively this means all $2 \cdot 2$ matrices A for which

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

In this context, we are not able to define A by the calculus definition (principle root) but we have to define it the second way as we did for the complex numbers.

Question — Now the big question is how many such $A \in \mathbb{R}$ are there such that

$$A^3 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}?$$

Solution: It is very hard to find all solutions to this equation. In the real numbers, we know that a 10th degree equation has at most 10 solutions but that is not the case everywhere as we can see for this example. □

Properties of $\cdot$ (multiplication) in $\mathbb{R}$ that we are used to:

– $\cdot$ is commutative
– There is an element 0 such that $0 \cdot r = 0 \ \forall \ r \in \mathbb{R}$.
– There is an element 1 such that $1 \cdot r = r \ \forall \ r \in \mathbb{R}$.
– $\forall \ r \neq 0$, $\exists \ r^{-1}$ such that $r^{-1} \cdot r = 1$.
– Exponent laws hold.
– An nth degree equation has at most n roots.

Example

For the set of $2 \cdot 2$ matrices over $\mathbb{R}$ and multiplication is defined as usual matrix multiplication. Then properties 1 and 4 do not hold while properties 2 and 3 do hold.

Example

Permutations are a reordering of a set. Say b and c are two permutations of a set S. What is $b \cdot c$?

Let us say b reverses order and c switches elements in the 3rd and 4th slot. And let $S = \{1, 2, 3, 4, 5\}$. Then $c(S) = 12435$ and $b(S) = 54321$. Then $c \cdot b = 54231$ and $b \cdot c = 53421$ (for $c \cdot b$, we apply b first then c). This is another example of "multiplication" which is not commutative.

In this context there is no "0" style element but there is a "1" style element such as $e = 12345$.

Question — How many solutions are there to

$$x^2 = e \text{ where } e = 12345 \text{ (the identity element).}$$

Solution: Both b and c are solutions to this equation and there are a finite number of solutions to this equation but there is definitely more than 2 solutions even though this is an equation with degree 2 which again differs from the real numbers. $\square$

Constructability: What can we construct with a straight edge and a compass if we have a segment of length 1? We can definitely construct a segment of length 2. Are we able to create a segment of length $\sqrt{2}$? Yes we can construct a segment of length $\sqrt{2}$ by creating a right triangle. However are we able to create a segment of length $\sqrt[3]{2}$? No, we are not able to construct a segment of such length but how do we prove this? We are able to prove this with abstract algebra.

Let $\mathbb{Q}$ is the set of rational numbers. Now consider the equation

$$x^2 - 2 = 0.$$

Does this equation have roots in $\mathbb{Q}$? No this equation doesn't have solutions in $\mathbb{Q}$ but it has solutions in $\mathbb{R}$ although its coefficients are in $\mathbb{Q}$. Similarly we can say that the equation

$$x^2 + 1 = 0$$

doesn't have solutions in $\mathbb{R}$ but does have solutions in $\mathbb{C}$.

To solve this issue, we can just work in a different set like the set of all real numbers but the set of real numbers is vastly more complicated than the set of rational numbers. Is there a way that we can resolve this issue? What if we just add $\sqrt{2}$ and create a smaller extension? This is possible and we call this a field extension and this is much simpler than just adding all the real numbers.

Takeaway. We will be working in different sets in abstract algebra and the properties of one set might be different than the properties of another set which can affect how we solve problems in abstract algebra.

§3 Sets and Functions

A set is a group or collection of elements. There is no requirement for the structure of a set.

Let S be a set of elements. We define an *operation* $*$ on S by $a * b$ for $a, b \in S$ (not necessarily distinct) where $a * b$ is a new element (not necessarily in S). Most of the time for $a * b$ we write that as $a \cdot b$ or ab which is even simpler. This of course assumes we are only dealing with one operation.

Definition

Let S be a set and let T be a *subset* of S if T is contained in S and is denoted by $T \subset S$. This does allow for $T = S$ as well according to this book, might be different for other books. We say that T is a *proper subset* of S if $T \subset S$ and $T \neq S$.

Definition

Say that $A, B \subset S$. Then $A \cup B$ (union) is all elements of S in at least one of A and B, $A \cap B$ (intersection) is all elements of S in both A and B, $A - B$ is elements which are in A but not in B, and $A' = A^c$ (A complement) is elements of S not in A, that is $S - A$. Note that $A - B = A \cap B'$.

Be careful with complement. Recall that $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Now what is $\mathbb{Q}'$? In order to answer this question, we would first need to specify what superset we are working with otherwise it would not be possible to fin the complement.

Definition

If A, B have no elements in common where $A, B \subset S$, then $A \cap B = \emptyset \longrightarrow$ empty set. We also have that $S' = \emptyset$. We also have that $A \times B$: Cartesian product $= \{(a, b) \mid a \in A, b \in B\}$.

Definition

We also have $|S| = m(S)$ which is the number of elements in S which is also known as cardinality of a set S.

What is $|A \cup B|$? This simply would be $|A| + |B| - |A \cap B|$ since we are overcounting the elements that are in both A and B so we can subtract the overcount which gives us the desired identity.

Problem (Section 1.2 #15)

What is $|A \cup B \cup C|$?

Solution: The answer is that $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$. We will now prove this fact.

Assume that $x \in A \cup B \cup C$. This implies that x is in at least one of A, B, or C.

Say that $x \in A$ only. Then if we plug it in the formula that we found, we can see that x is only counted once in $|A|$.

Say that $x \in A, B$ but $x \notin C$. Then x is counted in $|A|, |B|$, and $|A \cap B|$ but this is only counted once since we subtract $|A \cap B|$.

Say that $x \in A, B, C$. Then this is counted everywhere but it is added 4 times and subtracted 3 times which implies it is only counted once.

Hence this identity is true as x is counted only one time on both sides. □

Problem (Section 1.2 #16)
What is $|A_1 \cup A_2 \cup ... \cup A_n|$?

Solution: We have that

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i,j=1, i<j}^{n} |A_i \cap A_j| + \sum_{i=j=k=1, i<j<k}^{n} |A_i \cap A_j \cap A_k| + ...$$

Say x is in the union and x belongs to k of the n sets ($1 \leq k \leq n$). How many times is x counted on the right? This is how we would be able to prove the formula above. □

Definition
Let S, T be sets. Then $f : S \to T$ is a function from S to T. A *function* or *mapping* of this type assigns to each element of S, a *unique* element of T. For $f(x)$ to be a function, we must have that $f(x)$ has only one value for each value of x. For example, $f(x) = x$ is a function but $f(x) = \pm x$ is not a function. Going back to $f : S \to T$, we have that S is the *domain* of the function while T is the *codomain* and $f(s) \subset T$ is the *range*.

Definition
Let $f : S \to T$ be a function. Then f is *onto* or *surjective* if $f(S) = T$ (range = codomain). A function f is *one-to-one* or *injective* if $s_1 \neq s_2 \longrightarrow f(s_1) \neq f(s_2)$ or said differently $f(s_1) = f(s_2) \longrightarrow s_1 = s_2$. We say a function f is a *one-to-one correspondence* or *bijection* if it is one-to-one and onto.

If S and T are finite, then such an f can be onto only when $|S| \geq |T|$ and f an be one-to-one only when $|S| \geq |T|$ and therefore we have that f can only be a bijection if $|S| = |T|$.

Definition
Now let $g : S \to T$ and $f : T \to U$. Then we can define $f \circ g : S \to U$ by $(f \circ g)(s) = f(g(s)) \longrightarrow$ composition.

However, $g \circ f$ may not even be defined here. The only way that it is guaranteed that $g \circ f$ is defined is if $U \subset S$. Then we have that $g \circ f : T \to T$. So $f \circ g = g \circ f$ (not necessarily commutative) is not necessarily true, they likely don't even have the same domain or codomain.

Now suppose that we have a third function $h : P \to S$ with $g : S \to T$ and $f : T \to U$. Then we have that $(f \circ g) \circ h : P \to U$. We can also define $f \circ (g \circ h) : P \to U$. Now are these two the same? Yes these two are

the same and now we will prove this fact. Take $p \in P$. Then we have that $[(f \circ g) \circ h](p) = (f \circ g)(h(p)) = f(g(h(p)))$ and $[f \circ (g \circ h)](p) = f((g \circ h)(p)) = f(g(h(p)))$ so we have thus proven that $(f \circ g) \circ h = f \circ (g \circ h)$. We have also proven that the operation $\circ$ is *associative*, that is $(a \circ b) \circ c = a \circ (b \circ c)$.

Question — Say that the operation $*$ is not associative. Then what does $a * b * c * d$ mean?

Solution: This is unclear. We would need parenthesis. If not associative then is a^2b^3 even clear? Is it $aabbb$? We would not know for sure because we do not have associativity. Matrix multiplication and "multiplication" of permutations are both associative but neither of them is commutative. In $\mathbb{R}$, we have that $a * b = a \cdot b$ is associative while $a * b = \frac{a}{b}$ and $a * b = a^b$ are not associative. □

When dealing with composition, we often consider $f, g : S \to S$ to ensure $f \circ g$ and $g \circ f$ are both defined. When f, g are bijections, that means they are *permutations*. An important function is $i_S : S \to S$ which is the *identity function* on S, that is $\forall \ \ s_1 \in S$, we hve that $i_S(s_1) = s_1$.

Definition

Say that $f : S \to T$ is a bijection. Then we can define $f^{-1} : T \to S$ which is the *inverse function* of f. Then we have that $f^{-1} \circ f = i_S$ and $f \circ f^{-1} = i_T$.

Question — If $f^{-1} \circ f = i_S$, can we be sure that $f \circ f^{-1} = i_T$?

Solution: The answer is yes. Assume that $f^{-1} \circ f = i_S$. Consider $f \circ f^{-1}$. Say that $(f \circ f^{-1})(t_i) = t_2$. Then for some $t_1, t_2 \in T$, then $[f^{-1} \circ (f \circ f^{-1})](t_1) = f^{-1}(t_2)$ and $[(f^{-1} \circ f) \circ f^{-1}](t_1) = f^{-1}(t_2)$ and $(i_S \circ f^{-1})(t_1) = f^{-1}(t_2)$. Then we have that $i_S(f^{-1}(t_1)) = f^{-1}(t_2)$ which implies that $f^{-1}(t_1) = f^{-1}(t_2)$ which implies that $t_1 = t_2$. Therefore we have that $(f \circ f^{-1})(t_1) = t_1$ which implies that $f \circ f^{-1} = i_T$ and the proof is complete. □

Problem (Section 1.3 #23)

Let S be the set of all integers of the form $2^m 3^n$, $m \geq 0, n \geq 0$ and let $\mathbb{N}$ be the set of natural numbers. Show that there is a $1-1$ correspondence of S onto $\mathbb{N}$.

Solution: We can start by putting the elements of S in order (same as the "usual" order). Therefore we will have that $S = \{s_1, s_2, s_3, ...\}$. Now we can define f to be a function such that $f : S \to \mathbb{N}$ defined by $f(s_k) = k$. Will this be the desired bijection? Each element of S is mapped to a unique element of $\mathbb{N}$ so f is a function. We also have that f is onto because for any natural number k we can find s_k which means this is onto. This function is also $1-1$ (can be easily checked). Therefore the function f that we defined is a bijection. □

An interesting question is what is the value of $f(2^{100}3^{50})$ or in other words, where does f map $2^{100}3^{50}$. The only way we can find this is to find where in the list does the number $2^{100}3^{50}$ lie in. And this is obviously not easy to do by hand.

Takeaway. Bijections, especially between infinite sets, sometimes they are not as convenient to define explicitly even though we can prove that a bijection exists.

Problem (Section 1.3 #24)
Prove that there is a $1-1$ correspondence of the set of all positive integers ($\mathbb{N}$) onto the set of all positive rational numbers ($\mathbb{Q}^+$).

Could we use an order argument like we used in Question #23? No, we cannot because that type of argument will not work here because we cannot even find the smallest positive rational number. So how do we do this?

Solution: Define a function $g : \mathbb{Q}^+ \to S$ defined by if $\frac{m}{n}$ is in the lowest form then $g(\frac{m}{n}) = 2^m 3^n$. This is a function because no 2 y values correspond to 1 x value. Is this a $1-1$ function? Yes this a $1-1$ or injective function as if $f(x) = f(y)$ then it implies that $x = y$. However this function, g, is not onto.

We can create a function h with $h : g(\mathbb{Q}^+) \to \mathbb{N}$. Then $h \circ g$ will be a bijection between $\mathbb{Q}^+$ and $\mathbb{N}$. $\square$

§4 Permutations

Definition
Let S be any set. Then $A(S)$ is the set of permutations of S. If S is finite with $|S| = n$ for some positive integer n, then we denote $A(S)$ by S_n.

Two permutations can be "multiplied" via composition. This "set" of permutations with this operation is closed, has "1" style element, each element has inverse, and is associative. However, no "0" style permutation exists and it is not commutative.

Now what is $|S_n|$? We have that $| S_n |= n! = n \cdot (n-1) \cdot ... \cdot 2 \cdot 1$.

Question — We know that S_2 has 2 elements and S_3 has 6 elements. Now let us consider the following problem. How many solutions are there to the equation

$$x^2 = \text{ identity or } x^3 = \text{ identity?}$$

Solution: We have that $S = \{1, 2, 3\}$ and the 6 permutations are

$$123, 132, 213, 231, 312, 321.$$

The first three and the last permutation satisfy the equation $x^2 =$ identity. The fourth and the fifth permutations satisfy the equation $x^3 =$ identity. We have three elements of order 2 as we do not consider 123 to be of order 2 as it is already the identity so it is of order 1, and we have two elements of order 3. $\square$

What if we do the same with S_4? So how many elements are there in S_4 that are of order 2 (elements that satisfy the equation $x^2 =$ identity? How many elements are there in S_4 that are of order 3?

Problem (Section 1.4 #16)
Let S be an infinite set and let $M \subset A(S)$ be the set of all elements $f \in A(S)$ such that $f(s) \neq s$ for at most a finite number of $s \in S$. Prove that:

(a) $f, g \in M$ implies that $fg \in M$.
(b) $f \in M$ implies that $f^{-1} \in M$.

Solution: The problem is asking to prove that M is closed and that M contains inverses.

Say $f, g \in M$. Suppose that f moves : $\{s_1, s_2, ..., s_k\}$ and g moves : $\{s_1', s_2', ..., s_j'\}$ then fg can only move elements in the union of these two. That is, if $f(s) = s$ and $g(s) = s$, then $fg(s) = s$. Therefore $fg \in M$.

If $f \in M$ then is $f^{-1} \in M$? If $f \in M$ and f moves $\{s_1, s_2, ..., s_k\}$, then f^{-1} only moves these also. Therefore $f^{-1} \in M$. □

Question — Suppose we are working with the same conditions of the problem but now we have that $P \subset A(S)$, where P is the set of elements such that $f(s) = s$ for finitely many s only. Is P closed? Does P contain inverses?

Solution: First of all, the identity is not in P because if f is the identity then for all s we have that $f(s) = s$ which implies that the identity cannot be in P.

Assume that $S = \mathbb{N}$.

12345678...

Let f be the permutation that switches $2k - 1$ with $2k$ for all k. Is $f \in P$? Yes f is in P because f doesn't leave any element fixed. What is f^2? We have that $f^2 =$ identity. This implies that P is not closed as the identity is not in P.

Yes inverses do exist as f and f^{-1} both leave the same set of elements fixed. □

Problem (Section 1.4 #24)

If n is at least 3, show that for some g in S_n, $f = g$ cannot be expressed in the form $g = f^3$ for any f in S_n.

Solution: Take $h : S_n \to S_n$ defined by $h(x) = x^3$. Is this function $1 - 1$? Are there multiple permutations whose cube is equal to the identity? Yes there are. We had shown in S_3 there were at least two of them. Therefore this function cannot be $1 - 1$. Is this function onto? This function cannot be onto since the domain and the codomain have the same cardinality. Thus for some $g \in S_n$ not in the range of h which implies that there is no $f \in S_n$ such that $f^3 = g$. □

§5 The Integers

The symbol $\mathbb{Z}$ represents the integers and $\mathbb{N}$ represents the positive integers.

We have that $\mathbb{N}$ is *well ordered*. That is, every nonempty subset of $\mathbb{N}$ has a smallest element. On the contrary, $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are not well ordered.

Theorem (Euclid's Algorithm)

Let m be any integer and let n be any positive integer. Then we can write $m = qn + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Here we have that q is the quotient and r is the remainder.

Proof: Consider $S - \{m - t_n \mid t \in \mathbb{Z}\}$. For t small enough (big negative number), these entries are nonnegative. So S definitely contains nonnegative entries.

Take x to be the smallest nonnegative element in S which we can do so since S is well ordered. Say $x = m - t_1 n$. Then $m - (t_1 + 1)n < 0$ or otherwise that would contradict the fact that this x is the smallest. Therefore

$$0 \leq x = m - t_1 n < n \longrightarrow m = t_1 n + x \text{ where } 0 \leq x < n$$

which proves Euclid's algorithm.

Therefore we can write $m = qn + r$ where $0 \leq r < n$. We say that $n \mid m$ (n divides m) if $m = qn$, that is $r = 0$. □

Definition Greatest Common Divisor

Say that a, b are nonzero integers. Then the greatest common divisor (gcd) is defined to be $\gcd(a, b) = c$ has the property that $c > 0, c \mid a, c \mid b$ and if $d \mid a$ and $d \mid b$, then $d \mid c$.

Question — Why does the gcd of two nonzero, fixed integers a, b exist?

Solution: Consider the set $K = \{ma + nb \mid m, n \in \mathbb{Z}\}$. Then K will have positive entries. Now consider the smallest positive element, which exists since the set of positive integers is well ordered. This smallest element will be the $\gcd(a, b)$. If $d \mid a$ and $d \mid b$, then certainly $d \mid (ma + nb)$ for any $m, n \in \mathbb{Z}$. The complete proof of the existence of the gcd is in the textbook. □

Now when $\gcd(a, b) = 1$ then this means that a and b are *relatively prime*.

Definition

A *prime number* p is an integer for which every nonzero integer n has $\gcd(p, n) = 1$ when $p \nmid n$ and $\gcd(p, n) = p$ when $p \mid n$.

Question — Every positive integer n such that $n > 1$ is a product of primes.

Solution: We will prove this fact by contradiction. Suppose that we are not able to write every positive integer $n > 1$ as a product of primes. Let n be the smallest integer which is not a product of primes. Consider n. It cannot be prime because then it would be written as a product of just itself. Now write $n = n_1 \cdot n_2$ where $n_1, n_2 > 1$. Then n_1 and n_2 both are a product of primes since $n_1, n_2 < n$ and we had defined n to be the smallest possible number that could not be written as the product of primes. Therefore this immediately is a contradiction as it then implies that n can be written as the product of primes. □

Theorem (Unique Factorization Theorem)

Every integer $n > 1$ can be written as a product of primes in a unique way.

Proof: Say

$$x = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l} = q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}$$

is the smallest positive integer without unique factorization. Here the p_i and the q_i are prime and the a_i and b_i are positive integers. Also WLOG assume that $p_1 < p_2 < p_3 < ... < p_l$ and $q_1 < q_2 < q_3 < ... < q_k$. We claim that $p_1 = q_1$. If not, say that $p_1 < q_1$. Then we must have that $p_1 \mid q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}$ which implies that p_1 divides one of the q_i which is not possible since the p_i and q_i are all primes. The proof is similar if $p_1 > q_1$ So we must have that $p_1 = q_1$.

Now consider $\frac{n}{p_1}$. This number must have a unique prime factorization as we had defined x to be the smallest positive integer without a unique prime factorization. Therefore this implies that the two factorizations are the same. $\square$

Theorem

There are infinitely many primes.

Proof: We will do a proof by contradiction. Suppose that there are finitely many primes and the set of all primes is $\{p_1, p_2, \ldots, p_k\}$. Now consider the integer $q = p_1 p_2 \ldots p_k + 1$. Now q is not divisible by any of the p_i which implies that q is a new prime which is a contradiction. Therefore there are infinitely many primes. $\square$

This fact helps show that $\gcd(a, b)$ is the largest positive integer that divides both a and b. This is because if $c = \gcd(a, b)$ and some $d \mid a, d \mid b$ had $d \nmid c$, then some prime p has higher power in d than in c. But increase power of p in c to match the power in d and you have a larger integer dividing both a and b.

Problem (Section 1.5 #14)

Prove that there are infinitely many primes of the type $4n + 3$.

Solution: Suppose that there are only finitely many primes of the form $4n + 3$ and let them be $q_1, q_2, \ldots, q_k$. Take $n = 4q_1 q_2 \ldots q_k - 1$. Then m is of type $4n + 3$ but is not divisible by any of the q_i or in other words, it is not divisible by any of the set of primes that are of the form $4n + 3$. Thus m can only be divisible by primes in the form $4n + 1$. Since a product of primes of the $4n + 1$ produces a number of the form $4n + 1$ (we can see this by taking modulo 4), we have a contradiction as m is of the form $4n + 3$. Therefore there must be infinitely many primes of the type $4n + 3$. $\square$

Problem (Section 1.5 #15)

Show that no integer $u = 4n + 3$ can be written as $u = a^2 + b^2$ where a, b are integers.

Solution: If a is even, then a^2 is of type $4n$ and if a is odd, then a^2 is of type $4n + 1$. Therefore if we consider all the possible combinations of a, b being either even or odd, we can see that we can never produce an integer u that is of type $4n + 3$ such that $u = a^2 + b^2$. $\square$

§6 Induction

Definition

Suppose you have a statement $P(k)$ for each $k \in \mathbb{N}$. We start off by proving $P(k)$ for initial values of k. Then we prove that if $P(k)$ holds for all $k \leq n$ then it holds for $k = n + 1$ as well. If both of these are true, then $P(k)$ holds for all $k \in \mathbb{N}$.

Problem (Section 1.6 #13)

Prove that for all $n \in \mathbb{N}$ that $3 \mid (n^3 - n)$.

Solution: If $n = 1$ then $n^3 - n = 1^3 - 1 = 0$ and $3 \mid 0$. If $n = 2$, then $n^3 - n = 2^3 - 2 = 6$ and $3 \mid 6$. Therefore the base case is satisfied.

Suppose that $3 \mid (k^3 - k)$ for all $k \leq n$. Now consider $(n+1)^3 - (n+1)$. We want to prove that $3 \mid ((n+1)^3 - (n+1))$. Now note that

$$(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = (n^3 - n) + 3n^2 + 3n.$$

Now by the induction hypothesis, we know that $3 \mid (n^3 - n)$ and also $3 \mid 3n^2$ and $3 \mid 3n$ since both are 3 times an integer. Therefore $3 \mid (n^3 - n) + 3n^2 + 3n$ which is equivalent to saying $3 \mid (n+1)^3 - (n+1)$ and the induction is complete. □

Problem (Section 1.6 #14)
Prove that for any fixed prime p that $p \mid (k^p - k)$ for all $k \in \mathbb{N}$.

Solution: Here we will do a proof by induction. If $k = 1$, then $1^p - 1 = 0$ so $p \mid (1^p - 1)$. Therefore the base case is satisfied.

Say that $p \mid (k^p - k)$ for all $k \leq n$. Now consider the expression $(n+1)^p - (n+1)$. Therefore by expanding with the binomial theorem, we have that

$$\begin{aligned}(n+1)^p - (n+1) &= (n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n + \binom{p}{p}) - (n+1) \\ &= (n^p - n) + (\binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n).\end{aligned}$$

Note for $1 \leq j \leq p-1$, we have that $\binom{p}{j} = \frac{p!}{j! \cdot (p-j)!}$ is divisible by p since the numerator is divisible by p while the denominator is not divisible by p. Now $p \mid (n^p - n)$ due to the induction hypothesis and since p divides each of the $\binom{p}{j}$ terms for all $1 \leq j \leq p-1$, we have that

$$p \mid (n^p - n) + (\binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n)$$

which implies that $p \mid (n+1)^p - (n+1)$ and the induction is complete. □

§7 Complex Numbers

Definition
The symbol $\mathbb{C}$ represents the complex numbers. If $z \in \mathbb{C}$, then $z = a + bi$ where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$.

Consider the following equation $x^2 + 1$. This equation has no solutions in real numbers. This is one of the reasons complex numbers were introduced.

With the help of complex numbers, we showed that for any nth degree equation over $\mathbb{R}$, there are exactly n roots in $\mathbb{C}$ (counting repeated roots as separate).

Definition

For $z = a+bi$, we define $\overline{z} = a-bi$ to be the *complex conjugate* of z. One property of the complex conjugate is that both $z\overline{z}$ and $z+\overline{z}$ are real.

If $f(x)$ is a polynomial over $\mathbb{R}$ (coefficients of $f(x)$ are real), then the roots of $f(x) = 0$ are in conjugate pairs. That is, if z is a root of $f(x)$, then $\overline{z}$ is also a root of $f(x)$.

Definition

Let $z = a + bi$ for $a, b \in \mathbb{R}$ where $i = \sqrt{-1}$. Then the magnitude of z is defined as

$$|z| = \sqrt{a^2 + b^2}.$$

Theorem (Triangle Inequality)

Suppose that we have $z, w \in \mathbb{C}$ Then we have that

$$|z| + |w| \geq |z + w|.$$

Theorem (Polar Form)

We can write $z = r(\cos(\theta) + i\sin(\theta))$ where $r = |z|$. This is called the polar form of z. We often write

$$\cos(\theta) + i\sin(\theta) = \operatorname{cis}(\theta) = e^{i\theta}.$$

Theorem (DeMoivre's Theorem)

This theorem states that if $z = r \cdot \operatorname{cis}(\theta)$, then

$$z^n = r^n \cdot \operatorname{cis}(n\theta).$$

Proof: The most common way to prove this theorem is to use Euler's identity, which states that $\cos(\theta)+i\sin(\theta) = e^{i\theta}$. We will leave the details up to the reader as this is a fairly simple and straightforward proof. □

Question — Now consider the number $(\sqrt{3}+i)^{100}$. How do we evaluate such a number?

Solution: We will convert this number to polar form. Now the magnitude of the complex number is

$$|\sqrt{3}+i| = \sqrt{(\sqrt{3})^2 + 1^2} = 2.$$

We also have that

$$\sqrt{3}+i = 2(\frac{\sqrt{3}}{2} + \frac{1}{2}i) = 2 \cdot \operatorname{cis}(\frac{\pi}{6}).$$

Therefore our original number becomes

$$(2\operatorname{cis}(\frac{\pi}{6}))^{100} = 2^{100}\operatorname{cis}(\frac{100\pi}{6}) = 2^{100}\operatorname{cis}(\frac{4\pi}{6}) = 2^{100}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i).\square$$

Theorem

Say that $f(x)$ is a polynomial in $\mathbb{R}$ (all coefficients of $f(x)$ are real). Then if z is a root of $f(x)$, then so is $\overline{z}$.

Proof: We know that $f(x)$ is a polynomial in $\mathbb{R}$. Say that $z = r\,\mathrm{cis}\,(\theta)$ is a root of $f(x)$. Then $\overline{z} = r\,\mathrm{cis}\,(-\theta)$. Thus $z^n = r^n\,\mathrm{cis}\,(n\theta)$ while $\overline{z}^n = r^n\,\mathrm{cis}\,(-n\theta)$. Thus z^n and $\overline{z}^n$ have same real part but opposite imaginary part. Suppose we have that

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0.$$

Then we must have that

$$a_k z^k + a_{k-1}z^{k-1} + \cdots + a_1 z + a_0 = 0.$$

We are also curious if

$$a_k(\overline{z})^k + a_{k-1}(\overline{z})^{k-1} + \cdots + a_1\overline{z} + a_0 = 0$$

holds. If we add the two of these up, the imaginary parts will all cancel out and the sum of the two will be 0. Therefore we must have that

$$a_k(\overline{z})^k + a_{k-1}(\overline{z})^{k-1} + \cdots + a_1\overline{z} + a_0 = 0.$$

Therefore this proves that $\overline{z}$ is also a root of $f(x)$ if z is a root. □

Question — If n is a fixed positive integer, what are the solutions in $\mathbb{C}$ to $z^n = 1$?

Solution: We can find the solutions with the help of DeMoivre's theorem. Imagine working backwards in terms of power ($\frac{1}{n}$ power essentially). Note that

$$1 = \mathrm{cis}\,(0) = z^n.$$

Then $z = \mathrm{cis}\,(\frac{0}{n})$ also works as taking the nth power gives us that $z^n = \mathrm{cis}\,(0) = 1$. Instead of saying $\mathrm{cis}\,(0)$, suppose we say that

$$z^n = 1 = \mathrm{cis}\,(2\pi).$$

then we must have that

$$z = \mathrm{cis}\,(\frac{2\pi}{n})$$

by DeMoivre's and this also satisfies $z^n = 1$. Continuing like this, we have that for any integer k, $z = \mathrm{cis}\,(\frac{2\pi k}{n})$ is a root of $z^n = 1$. As a result, $z^n - 1$ has n distinct roots and these roots are

$$\{\mathrm{cis}\,(\frac{2\pi k}{n}) \mid 0 \leq k \leq n-1\}.$$

Each of the roots have a different position on the unit circle which implies that all of these n roots are distinct. We call these roots the nth roots of unity. □

Question — Will every point on the unit circle be an nth root of unity for some positive integer n?

Solution: The answer is actually no. To show this we will provide a counterexample. Note that $\mathrm{cis}\,(1)$ is not a root of unity as if we take this number to any power, it can never be of the form $\mathrm{cis}\,(2\pi kn)$ as π is irrational. □

Problem (Section 1.7 #21)

Consider the set $A = \{a + bi \mid a, b \in \mathbb{Z}\}$. Prove that there is a $1-1$ correspondence of A onto $\mathbb{N}$. (A is called the set of *Gaussian integers*.)

Solution: Define $f : A \to \mathbb{N}$ and let $f(a+bi) = 2^a \cdot 3^b$ if $a, b \geq 0$, $f(a+bi) = 5^a \cdot 7^{-b}$ if $a \geq 0, b < 0$, $f(a+bi) = 11^{-a} \cdot 13^b$ if $a < 0, b \geq 0$, and $f(a+bi) = 17^{-a} \cdot 23^{-b}$ if $a < 0, b < 0$. This is a one-to-one from A to $\mathbb{N}$. However this function is not onto. [finish this solution up] □

§8 Definitions and Examples of Groups (Chapter 2)

Definition

Let us define what a group is. A group, $(G, *)$, is a set G with an operation $*$ satisfying the following properties:

1. For all $a, b \in G$, we have that $a * b \in G$ (closure).

2. For all $a, b, c \in G$, we have that $(a * b) * c = a * (b * c)$ (associativity).

3. There exists an element $e \in G$ such that for all $a \in G$, we have that $a * e = e * a = a$ (identity, two-sided identity).

4. For all $a \in G$, there exists $a^{-1} \in G$ for which $a * a^{-1} = a^{-1} * a = e$ (inverse, two-sided inverse).

We do not necessarily have $a * b = b * a$ for all $a, b \in G$. Commutativity is not required in a group.

Definition

A group which has commutativity is called *abelian*.

Although groups have an identity element, they do not have a "0" style element. We cannot have a "0" style element in a group as it cannot have an inverse.

Say that we are in $\mathbb{R}$.

1. Does the operation $a * b = a^b$ form a group? No this doesn't as there is no closure as $(-5)^{\frac{1}{2}} \notin \mathbb{R}$.

2. Does the operation $a * b = a - b$ form a group? No this doesn't as there is no associativity.

3. Does the operation $a * b = a \cdot b$ form a group? No this doesn't as 0 has no inverse.

However $\mathbb{R} - \{0\}$ with the operation $a * b = a \cdot b$ is a group.

4. Does the operation $a * b = a + b$ form a group? Yes this does form a group as it meets all of the criterion of a group if this operation is over $\mathbb{R}$.

In a group G, for some $a \in G$, what does the element a^n mean for $n \in \mathbb{N}$. We have that

$$a^n = a * a * \cdots * a$$

where a is written n times and this is well defined due to associativity. Without associativity, we would not really know what a^n meant as it would represent a variety of things depending on how the parenthesis are.

Question — Now what does a^{-n} mean? Is it $(a^{-1})^n$ or is it $(a^n)^{-1}$?

Solution: Both of these options seem like reasonable interpretations. Now note that

$$(a^n)^{-1} * a^n = e$$

by definition and also

$$(a^{-1})^n * a^n = a^{-1}a^{-1}\dots a^{-1}aa\dots a$$

where each of the a^{-1} and a are written n times. Now note that $a^{-1} * a = e$ and if we keep repeating this process, we get that

$$(a^{-1})^n = e.$$

This implies that both $(a^{-1})^n$ and $(a^n)^{-1}$ are the same. □

Example

Consider 2×2 matrices with the multiplication operator over $\mathbb{R}$. Does this form a group? This is not a group because matrices with determinant equal to 0 do not have inverses and there are 2×2 matrices with determinant equal to 0.

Now if we say consider 2×2 matrices with nonzero determinant with the multiplication operator over $\mathbb{R}$ will be a group as it satisfies the group properties.

Example

Let $T_{a,b} : \mathbb{R} \to \mathbb{R}$ such that $T_{a,b}(r) = ar + b$ for $a, b \in \mathbb{R}$ and $a \neq 0$. This set of mappings is actually a group under composition $(T_{a,b} \circ T_{c,d})$.

Solution: This is true because

$$T_{a,b} \circ T_{c,d} = T_{a,b}(cr + d) = a(cr + d) + b = acr + (ad + b).$$

Obviously this is closed under composition as $a \neq 0$ and $c \neq 0$. We can also check for associativity as we already know that function composition is associative. The identity element is $T_{1,0}$ as we have that

$$T_{1,0} \circ T_{a,b} = T_{a,b} = T_{a,b} \circ T_{1,0}.$$

Now what about inverses. Note that $T_{a,b}^{-1} = T_{\frac{1}{a},-\frac{b}{a}}$ so inverses exist. Therefore this satisfies all the properties of a group and thus is a group. However this is a non-abelian group as functional composition is not commutative. This is also an infinite group as it has an infinite number of elements. □

Definition

For a finite group G, the number of elements in G is denoted by $|G|$ or $o(G)$ where the $o(G)$ means order of G.

Say $n \in \mathbb{N}$, usually $n > 2$. Now consider operations on the points of the plane:

$$f : \text{ reflect point in } y - \text{axis},$$

$$h : \text{ rotate the point counterclockwise by } \frac{2\pi}{n} \text{ in reference to the origin.}$$

Now the big question is what happens if we apply both f and h together or what happens if we apply h twice? Overall, how many different things that we can do to the points in the plane by applying f and h?

Note that for fh, we first rotate the point and then reflect it however for hf, we first reflect the point and then rotate it which implies that $fh \neq hf$ for any $n > 2$. If $n = 2$, then we have that $fh = hf$ so this is the

exception which is why we consider $n > 2$.

However what we do have is that $fh = h^{-1}f$. Now we also have that

$$f^2 = h^n = \text{identity mapping.}$$

Example

Therefore f, h generate a group. The elements of this group will be of the form

$$G = \{f^k h^l \mid k = 0, 1, l = 0, 1, \dots, n-1\}.$$

Now how do we know if this generates all of the possible mappings? We know that this is true because of the identity $fh = h^{-1}f$ which means that every possible mapping can be written in the form $f^k h^l$ for some $k = 0, 1$ and $l = 0, 1, \dots, n-1$. Therefore we must have that $|G| = 2n$ has k has 2 possibilities and l has n possibilities.

Definition

Therefore for $n > 2$, we have that G is a nonabelian group with the operation being composition of order $2n$. This group is called the *dihedral* group of order $2n$.

Problem (Section 2.1 #24)

If G is the dihedral group of order $2n$, then prove that:
(a) If n is odd and $a \in G$ is such that $a * b = b * a$ or all $b \in G$, then $a = e$.
(b) If n is even, show that there is an $a \in G$, $a \neq e$, such that $a * b = b * a$ for all $b \in G$.

Solution: (a) Consider fh^l where $l = \{0, 1, \dots, n-1\}$. Then we have that

$$fh^l = h^{-1}fh^{l-1} = h^{-2}fh^{l-2} = h^{-l}f = h^l f \longrightarrow h^{2l} = e.$$

Therefore this implies that $l = 0$. Therefore no nontrivial power of h commutes with f. Similarly fh^l won't commute with f for $l \neq 0$. Therefore we must have that a is the identity or $a = e$.

(b) From (a) we know that f will commute with $h^{\frac{n}{2}}$ so we have that $h^{\frac{n}{2}}$ will commute with all of G. And since $h^{\frac{n}{2}} \neq e$, we have shown that there exists $a \in G$ with $a \neq e$ such that $a * b = b * a$ for all $b \in G$. □

Problem (Section 2.1 #26)

If G is a finite group, prove that, given $a \in G$, there is a positive integer n, depending on a, such that $a^n = e$.

Solution: List the positive integer powers of a,

$$\{a, a^2, a^3, \dots\}.$$

Then there exists $k, j \in \mathbb{N}$ with $k < j$ such that $a^k = a^j$ as there are only finitely many powers that can be made but there are infinitely many powers which implies that the powers will eventually repeat. Then we have that

$$a^k = a^k \longrightarrow a^k = a^k a^{j-k} \longrightarrow e = a^{j-k}.$$

Therefore we have that there exists such a positive integer n such that $a^n = e$. □

Problem (Section 2.1 #27)

If G is a finite group and given $a \in G$, prove that there exists an integer $m > 0$ such that $a^m = e$ for *all* $a \in G$.

Solution: We can take the least common multiple of the powers such that $a^n = e$ for each of the elements $a \in G$ and this least common multiple will work because of the exponent laws. Therefore there exists such a positive integer m such that $a^m = e$ for all $a \in G$. $\square$

Problem (Section 2.1 #28)

Let G be a set with an operation $*$ such that:
1. G is closed under $*$.
2. $*$ is associative.
3. There exists an element $e \in G$ such that $e * x = x$ for all $x \in G$.
4. Given $x \in G$, there exists a $y \in G$ such that $y * x = e$.

Prove that G is a group.

Solution: Take $x \in G$ and say $y \in G$ is the left inverse of x and say that z is the left inverse of y and e is the left identity. Can we prove y is also the right inverse of x? We must have that

$$xy = e(xy) = (zy)(xy) = z(yx)y = z(ey) = zy = e$$

which implies that inverses are two sided.

Now can we prove that e is the right identity also? We must have that

$$xe = x(yx) = (xy)x = ex = x$$

which proves that e is a two sided identity.

Therefore we must have that G is a group as it is closed, associative, has two sided inverses, and has two sided identity. $\square$

However if $(G, *)$ is closed, associative, has left identity, and has right inverses, then G is not necessarily a group.

Consider $\mathbb{R} - \{0\}$ under the operation $a * b = |a| \cdot b$. This operation is obviously closed as $\mathbb{R} - \{0\}$ is closed under this operation and this is also associative which we can check. We also have that 1 is a left identity as $1 * b = b$ for all $b \in \mathbb{R} - \{0\}$ however $a * 1 = |a| \neq a$ for all $a \in \mathbb{R} - \{0\}$ which means it is not a right identity. Also notice that $a * \frac{1}{|a|} = 1$ for all $a \in \mathbb{R} - \{0\}$ which means each element has a right inverse but there are no left inverses because no negative number will have a left inverse. Therefore this is an example of the property above as it has all the properties listed but it isn't a group.

Problem (Section 2.1 #29)

Let G be a *finite* nonempty set with an operation $*$ such that:
1. G is closed under $*$.
2. $*$ is associative.
3. Given $a, b, c \in G$ with $a * b = a * c$, then $b = c$.
4. Given $a, b, c \in G$ with $b * a = c * a$, then $b = c$.

Prove that G must be a group under $*$.

Solution: Say that $G = \{a_1, a_2, \ldots, a_n\}$ where each of the a_i are distinct for $i = 1, 2, \ldots, n$. Consider the list

$$\{a_1^2, a_1a_2, a_1a_3, \ldots, a_1a_n\}.$$

Now the elements in this list are all distinct because of cancellation laws. Therefore one of them must be a_1 as the elements in the set are all distinct and there are n of these elements implying that they must all be elements of G as G is closed. Now suppose that

$$a_1a_i = a_1$$

for some i. Then for any $m \in [1, n]$, we have that

$$a_1a_m = a_1a_ia_m$$

and by cancellation, this means that $a_m = a_ia_m$ which implies that a_i is the left identity for every element in G.

For any m, consider the list

$$\{a_1a_m, a_2a_m, \ldots, a_na_m\}.$$

Again the elements in this list are distinct because of cancellation laws and again one of them must be equal to a_i. Therefore we have that

$$a_ka_m = a_i$$

for some k and we know that a_m has a left inverse of a_i, the left identity.

Now since we have the existence of left inverses and left identity, we can use Problem #28 from this section to conclude that G is a group. □

Problem (Section 2.1 #30)

However if G is an infinite set, then even if G has the same properties as #29, then it is not necessarily a group.

Solution: Consider the set $\mathbb{Z} - \{0\}$ under the usual multiplication operation. This set is closed, associative, and the cancellation laws hold. However this is not a group as we do not have the existence of inverses. □

§9 Some Simple Remarks

In a group G, the identity element is unique and each element has a unique inverse.

Why is this true? Say that e, f were both identity elements in G. Then we have that

$$e = e * f = f$$

which implies that there is only one identity element in G which means that the identity element is unique. Now why are inverses unique? Say that $a, b, c \in G$ and b, c are inverses of a. Then we have that

$$ab = ac = e \longrightarrow bab = bac \longrightarrow eb = ec \longrightarrow b = c$$

which implies that there is only one inverse for each element in G which means that each element has a unique inverse.

Problem (Section 2.2 #30)
Let G be a group in which $(ab)^n = a^n b^n$ for some fixed integer $n > 1$ for all $a, b \in G$. For all $a, b \in G$, prove that:
(a) $(ab)^{n-1} = b^{n-1}a^{n-1}$.
(b) $a^n b^{n-1} = b^{n-1}a^n$.
(c) $(aba^{-1}b^{-1})^{n(n-1)} = e$.

Solution: (a) Start with $(ab)^n = a^n b^n$ and cancel a from left and cancel b from right. Then once we finish doing this we get the following

$$(ba)^{n-1} = a^{n-1}b^{n-1}$$

and we can switch a, b to get the following identity that they want us to prove.

(b) Note that we have

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

which is exactly what we had wanted to prove and we had proved this using cancellation laws.

(c) Therefore for arbitrary $a, b \in G$, we want to prove that $((aba^{-1}b^{-1})^{n-1})^n$ is the identity element. Now we can consider (aba^{-1}) to be one element and have b^{-1} be the other element. Now using the identity $(ab)^{n-1} = b^{n-1}a^{n-1}$, we get that

$$((aba^{-1}b^{-1})^{n-1})^n = (b^{1-n}(aba^{-1})^{n-1})^n = (b^{1-n}ab^{n-1}a^{-1})^n.$$

Now we can let $(b^{1-n}ab^{n-1})$ be one element and let a^{-1} be the other element and we get that

$$(b^{1-n}ab^{n-1}a^{-1})^n = (b^{1-n}ab^{n-1})^n a^{-n} = b^{1-n}a^n b^{n-1}a^{-n}.$$

Now using $a^n b^{n-1} = b^{n-1}a^n$ on $a^n b^{n-1}$ term, we have that

$$b^{1-n}a^n b^{n-1}a^{-n} = b^{1-n}b^{n-1}a^n a^{-n} = e$$

which was what we wanted to prove. □

§10 Subgroups

In this section, we will be talking about subgroups.

Definition
Let $(G, *)$ be a group. For $H \subset G$, define $(H, *)$ to be a *subgroup* of G if H is a group in its own right. Note that the operation of G is also the operation of H.

Theorem
For groups H, G with $H \subset G$, we have that H is a subgroup of G if for all $a, b \in H$, we have that $ab^{-1} \in H$.

Example
An example of a subgroup ($H \subset G$) is when $G = \mathbb{Z}$ under the operation $+$ and $H = k\mathbb{Z}$ which is the multiples of k.

Definition

If H is a subgroup of G and $H \neq G$, then we say that H is a *proper subgroup* of G.

Definition

For any group G for fixed $a \in G$,

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is always a subgroup of G. This is the *cyclic subgroup* generated by a. The cyclic subgroup generated by a is denoted by (a).

Definition

For any G, we have that $\mathbb{Z}(G)$ is the set of elements in G which commute with all other elements, in other words, $a \in \mathbb{Z}(G)$ if $a * b = b * a$ for all $b \in G$. This is called the *center* of G.

For H being any subgroup of G, if $a \in G$ for fixed a, then

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

is also a subgroup of G. We should choose a such that $a \notin H$. Now why is this a subgroup? Take any ah_1a^{-1}, ah_2a^{-1} in the set aHa^{-1} where $h_1, h_2 \in H$. Note that

$$(ah_1a^{-1})(ah_2a^{-1})^{-1} = (ah_1a^{-1})(ah_2^{-1}a^{-1}) = ah_1h_2^{-1}a^{-1}$$

and we have that $ah_1h_2^{-1}a^{-1} \in aHa^{-1}$ as $h_1h_2^{-1} \in H$. Therefore this proves that this set is a subgroup of G.

Problem (Section 2.3 #18)

If S is a nonempty set and $X \subset S$, show that $T(X) = \{f \in A(S) \mid f(X) \subset X\}$ is a subgroup of $A(S)$ if X is *finite*.

Solution: Take $f, g \in T(X)$. Now what we want to find out is whether fg^{-1} has to be in $T(X)$?

For any $x \in X$, consider $(fg^{-1})(x) = f(g^{-1}(x))$. Since X is finite, we have that $g(x) = x$ and thus $g^{-1}(x) = x$. Hence $g^{-1}(x) \in X$. Therefore

$$f(g^{-1}(x)) = f(x') \text{ where } x' \in X \text{ which implies that } f(x') \in X \text{ since } f \in T(x).$$

Thus fg^{-1} maps anything in X inside X, so $fg^{-1} \in T(X)$ which implies that $T(X)$ is a subgroup. $\square$

Problem (Section 2.3 #25)

Let $S, X, T(X)$ be as in Problem 18 (but X no longer finite). Give an example of a set S and an infinite subset X such that $T(X)$ is *not* a subgroup of $A(S)$.

Solution: Let $S = \mathbb{Z}$. Consider the function $f(z) = z+1$. Take $X = \mathbb{Z}^+$. Here $f(x) \subset X$. However $f^{-1}(z) = z-1$ does not satisfy this property, in other words, $f^{-1}(x) \not\subset X$. Therefore $T(X)$ is not a subgroup. $\square$

Problem (Section 2.3 #29)
If M is a subgroup of G such that $x^{-1}Mx \subset M$ for all $x \in G$, prove that $x^{-1}Mx = M$.

Solution: For some fixed x, we have that $xMx^{-1} \subset M$ (using a^{-1}). Now we also have that $x^{-1}(xMx^{-1})x \subset x^{-1}Mx$ which simplifies to $M \subset x^{-1}Mx$. Now since each of them are subsets of one another, this implies that $x^{-1}Mx = M$. $\square$

§11 Lagrange's Theorem

Definition (Cyclic Group)
A group G is cyclic if it is generated by a single element. That is,

$$G = \{b^n \mid n \in \mathbb{Z}\}$$

which might be finite or infinite. Cyclic groups are always abelian.

Definition (Relations)
For a set S, define a relation on S by $b, c \in S$, $b \sim c$ means b is "related" to c. We can also say that a relation is a collection of ordered pairs in S.

1. A relation on S is *reflexive* if $b \sim b$ for all $b \in S$.
2. A relation on S is *symmetric* if whenever $b \sim c$ then $c \sim b$ as well.
3. A relation on S is *transitive* if $a \sim b$ and $b \sim c$ implies that $a \sim c$.

A relation that satisfies all three of these rules is called an *equivalence relation*.

Example
Common example in $\mathbb{Z}$. For a fixed nonzero integer, we say that $a \sim b$ if $n \mid (b - a)$. We say that $a \equiv b \pmod{n}$ if $n \mid (a - b)$.

If there is an equivalence relation on S, for $a \in S$, $[a]$ is the equivalence class of a which contains all elements related to a.

Importantly, these equivalence classes break S into a collection of pairwise disjoint subsets.

Definition
Say G is a group with $H \subset G$ as a subgroup. For fixed $b \in G$, define

$$Hb = \{hb \mid h \in H\}.$$

This is called a *right coset* of H in G. Similarly

$$bH = \{bh \mid h \in H\}$$

is called a *left coset* of H in G.

For any $b, c \in G$, we have that $Hb = Hc$ or $Hb \cap Hc = \emptyset$. In essence, we can define an equivalence relation on G via $b \sim c$ if $Hb = Hc$.

Say that Hb and Hc overlap for some $h_1, h_2 \in H$ so that $h_1 b = h_2 c$. Then $bc^{-1} = h_1^{-1} h_2 \in H$. Therefore $bc^{-1} \in H$ and we can say that $b = h_3 c$ for some $h_3 \in H$.

So then for $h'c \in Hc$, we have that $h' h_3^{-1} b \in Hb$ since $h' h_3^{-1} \in H$. Thus $Hc \subset Hc$. Similarly we can prove that $Hb \subset Hc$. Therefore since we have proven that they are subsets of one another, we must have that $Hb = Hc$.

With this in mind, partition G into $Ha_1, Ha_2, \ldots, Ha_k$ pairwise disjoint cosets. Say that G is finite. Then each of the Ha_i has cardinality $o(H)$ and $Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k = G$. This proves that $o(H) \mid o(G)$. This is known as Lagrange's Theorem.

Theorem (Lagrange's Theorem)

For any group G having a subgroup H, the order of H must divide the order of G, $(o(H) \mid o(G))$.

The number of distinct (right) cosets that H has in G is $i_G(H)$ where i represents index.

This leads the way to proving that every group of prime order is cyclic.

Say that $|G| = p$ for prime p. Then for any $a \in G$ with $a \neq e$, consider the cyclic subgroup generated by a, (a). We must have that $G = (a)$ as the subgroup must divide p and since $a \neq e$, the subgroup cannot have order 1 which means it has to have order p which means that it has to be the entire group. Therefore we have that G is cyclic.

Definition

For group G for any $b \in G$, let the smallest positive integer k (if such a k exists) for which $b^k = e$ is the *order* of b in G and is denoted as $o(b)$. If G is finite, then $o(b) \mid o(G)$. This is because $(b) = \{e, b, b^2, \ldots, b^{k-1}\}$ so $|(b)| = k$. Since this is a subgroup, by Lagrange's theorem we have that $k \mid o(G)$ which means that $o(b) \mid o(G)$.

This also means if $|G| = n$, for any $b \in G$, we have that $b^n = e$ where e is the identity.

Let n be a positive integer such that $n \geq 2$. Then $\mathbb{Z}_n$ is the nonnegative integers $< n$ under addition $\pmod n$. The operation boils down to $[a] + [b] = [a + b]$ where these are equivalence classes. Therefore we have that $\mathbb{Z}_n$ is the cyclic group of order n.

What if we try to take the same collection of integers under multiplication $\pmod b$? No this is not a group because 0 has no inverse and [1] is the identity.

Say we remove 0. Then would it be a group? No it is not necessarily a group. For example, consider 12. Then $[4] \cdot [3] = 0$ but 0 is no longer there. Therefore it is not necessarily a group.

In multiplication mod n, $u < k < n$ has an inverse if and only if $\gcd(k, n) = 1$, that is if k and n are relatively prime.

For any $n > 1$, the set of positive integers $< n$ which are relatively prime to n form a group under multiplication $\pmod n$. This is denoted by U_n.

Let $\phi(n) = n\Pi_{p|n}(1 - \frac{1}{p})$. Then we have that $o(U_n) = \phi(n)$.

For n being any positive integer, if b is relatively prime to n, then

$$b^{\phi(n)} \equiv 1 \pmod{n}.$$

In special case where n is prime, p, for any b, $p \nmid b$, we have that

$$b^p \equiv b \pmod{p}, b^{p-1} \equiv 1 \pmod{p}.$$

Problem (Section 2.4 #12)

If aH and bH are distinct left cosets of H in G, are Ha and Hb distinct right cosets of H in G? Prove that this is true or give a counterexample.

Solution: If $Ha = Hb$, then we have that $ab^{-1} \in H$. If $aH = bH$, then we have that $b^{-1}a \in H$. Is it possible to have $ab^{-1} \in H$ but $b^{-1}a \notin H$.

Now consider the dihedral group for large n. Let this group be denoted by G. Let K be the subgroup such that $K = \{e, f\}$. Then $Kh = \{h, fh\}$ and $K(fh) = \{fh, f^2h\} = \{fh, h\}$ since $f^2 = e$.

Now we have that $hK = \{h, hf\} = \{h, fh^{-1}\}$ as $fh = h^{-1}f$. We also have that $(fh)K = \{fh, fhf\} = \{fh, h^{-1}\}$.

Now $hK \neq Kh$ unless $h = h^{-1}$ but that only happens when n is one of the initial cases and not for large n. Therefore for large n, we have that $hK \neq Kh$ which is a counterexample so even though the left cosets are distinct, this doesn't imply that the right cosets are distinct. $\square$

Problem (Section 2.4 #26)

Let G be a group, H a subgroup of G, and let S be the set of all distinct right cosets of H in G, T the set of all left cosets of H in G. Prove that there is a $1-1$ mapping of S onto T.

Solution: The natural try is to let $f(Ha) = aH$. However this does not work. Say that $Ha = Hb$, but $aH \neq bH$. Then $f(Ha) = aH$ and $f(Hb) = bH$ but $aH \neq bH$ so this won't be a function.

You have to do this instead. We map $f(Ha) = a^{-1}H$. Because if $Ha = Hb$ then this implies that $ab^{-1} \in H$ which implies that $ba^{-1} \in H$. This forces that $a^{-1}H = b^{-1}H$. Therefore $Ha = Hb$ implies that $a^{-1}H = b^{-1}H$. Therefore this is a $1-1$ mapping of S onto T. $\square$

Problem (Section 2.4 #24)

If p is a prime number of the form $4n + 3$, show that we *cannot* solve

$$x^2 \equiv -1 \pmod{p}.$$

Solution: Note that $p - 1 = 4n + 2$. Thus for any x, $p \nmid x$, we have that

$$x^{p-1} \equiv 1 \pmod{p} \xrightarrow[25]{} x^{4n+2} \equiv 1 \pmod{p}.$$

Suppose that if $x^2 \equiv 1 \pmod{p}$, then we have that $(x^2)^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{p}$. This would imply that $x^{4n+2} \equiv -1 \pmod{p}$ which is a contradiction. Therefore if p is of the form $4n+3$, then we cannot solve $x^2 \equiv -1 \pmod{p}$. $\square$

Problem

Prove that there are an infinite number of primes in the form $4n+1$.

Solution: Suppose that there are finitely many $4n+1$ primes and call them $q_1, q_2, \ldots, q_m$.

Consider the number

$$b = 4q_1^2 q_2^2 \ldots q_n^2 + 1$$

which is still in the form $4n+1$.

Note that b is also in the form x^2+1 for some positive integer x. Therefore by using the problem above, we know that b is not divisible by any prime in the form $4n+3$. Therefore we must have that b is divisible by primes in the form $4n+1$. However b cannot be divisible by $q_1, q_2, \ldots, q_m$ as b leaves a remainder of 1 when divided by any of them. This is the desired contradiction which means there must be an infinite number of primes in the form $4n+1$. $\square$

Problem (Section 2.4 #43)

Let G be an abelian group of order n, and $a_1, \ldots, a_n$ its elements. Let $x = a_1 a_2 \ldots a_n$. Show that:
(a) If G has exactly one element $b \neq e$ such that $b^2 = e$, then $x = b$.
(c) If n is odd, then $x = e$.
(b) If G has more than one element $b \neq e$ such that $b^2 = e$, then $x = e$.

Solution: (a) Pair each element with its inverse. Leave b and e aside. Then the product of all elements excluding b and e would simply just be e. Then we have that $x = ebe = b$.

(c) Pair each element with its inverse again and leave e aside. Then the product of all elements excluding e would simply just be e. Then we have that $x = ee = e$.

(b) Consider $H \subset G$ which is the subgroup of elements of order ≤ 2. The product of elements outside H is simply e. Therefore we just need to prove that the product of elements inside H is also e.

Take $a, b \in H$ with $a \neq b$ such that $a \neq e$ and $b \neq e$. Now consider

$$K = \{e, a, b, ab\}$$

which is a subgroup of H. The product of elements in K is also e. For any coset Kc in H will be

$$\{c, ac, bc, abc\}$$

and the product of all elements will still be e. So now break H into its cosets of K. Therefore the product of all the elements of H will be e which means that the product of all the elements $x = e$. $\square$

§12 Homomorphisms and Normal Subgroups

Let G be a group with subgroup H. Say that we take $f : H \to M$ where M is a subset of G and f is a bijection. Is M also a subgroup of G?

Definition

Say that G and G' are groups. A function $f : G \to G'$ is a *homomorphism* if for all $b, c \in G$, we have that $f(bc) = f(b)f(c)$. When we mean bc, we mean bc with the operation of G whereas $f(b)f(c)$ is with the operation of G'.

Definition

If such an f is $1-1$, it is called a *monomorphism*. If such an f is a bijection, it is called an *isomorphism*. If $f : G \to G$ is an isomorphims, then it is called an *automorphism*.

Let $G_1 = \mathbb{Z}_7 = \{0, 1, \ldots, 6\}$ with the operation addition modulo 7. Let $G_2 = \{1, a, a^2, \ldots, a^c\}$ with $a^7 = 1$. Are G_1 and G_2 the same group? While G_1 and G_2 use different notation, they are isomorphic, that is $G_1 \cong G_2$.

Any two groups of same prime order are isomorphic.

Example

For any group G and fixed $b \in G$, take $T_b : G \to G$ defined by

$$T_b(x) = bx, T_b \text{ left multiplies by } b.$$

The key is that $T_b \in A(G)$.

Consider $f : G \to A(G)$ defined by $f(b) = T_b$. This will be a monomorphism because $f(bc) = T_{bc} = T_b \circ T_c = f(b)f(c)$. This function is also $1-1$ as

$$f(b) = f(c) \longrightarrow T_b = T_c \longrightarrow bx = cx \longrightarrow b = c$$

through cancellation laws which means this function is $1-1$. Thus G is isomorphic to a subgroup of $A(G)$.

Say $|G| = 100$. Then G is isomorphic to some subgroup of S_{100}. However can we find a smaller n for which G is isomorphic to a subgroup of S_n. What is the smallest n for which S_n contains a copy of $\mathbb{Z}_k$?

Example

Let $f : G \to G$. Say that $b \in G$ is fixed. Then

$$f(x) = b^{-1} \times b$$

is always an automorphism of G. This is because we have that

$$f(x) = b^{-1}xyb = (b^{-1}xb)(b^{-1}yb) = f(x)f(y)$$

so this is a homomorphism. This is also a bijection, which we can easily check, and since it is from G to itself, it must be an automorphism.

Definition

Say $f : G \to G'$ is a homomorphism where G and G' are groups. Then the kernel of f ($\text{Ker}(f)$) is the set

$$\text{Ker}(f) = \{g \in G \mid f(g) = e'\}$$

where e' is the identity in G'.

Note that $\text{Ker}(f)$ is always a subgroup of G. We will call $\text{Ker}(f)$ as K for short. Say that $a, b \in K$, that is $f(a) = f(b) = e'$. Then $f(e) = e'$ which implies that $f(bb^{-1}) = e' = f(b)f(b^{-1})$ which implies that $f(b^{-1}) = (f(b))^{-1}$. Therefore we have that

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = e'(e')^{-1} = e'$$

which means that $ab^{-1} \in K$. Consequently we must have that K is a subgroup of G.

Let $f : G \to G'$ be a homomorphism with kernel K. It turns out that for all $b \in G$, we have that $b^{-1}ab \subset K$. This is because for any $k_1 \in K$ we have that

$$f(b^{-1}k_1b) = f(b^{-1})f(k_1)f(b) = f(b^{-1})e'f(b) = f(b^{-1})f(b) = e'$$

which implies that $b^{-1}k_1b \in K$.

We showed that if $b^{-1}Kb \subset K$ for all $b \in G$, then $b^{-1}Kb = K$ for all $b \in G$. Thus if H is a subgroup of G and there exists some $b \in G$ for which $b^{-1}Hb \not\subset H$, then H cannot be the kernel of any homomorphism on G.

Definition

For any group G with subgroup N, N is what we call the *normal subgroup* of G if for all $b \in G$, we have that $b^{-1}Nb \subset N$ which is equivalent to saying that $b^{-1}Nb = N$ for all $b \in G$. We can also say $N \lhd G$ if $Nb = bN$ for all $b \in G$, that is, every left coset is a right coset ($N \lhd G$ means N is a normal subgroup of G).

Example

Take dihedral group such that the number of elements is ≥ 6. Let $M = \{e, f\}$ where f is the reflection and e is the identity. Is $M \lhd G$?

We have that

$$hM = \{h, hf\} = \{h, fh^{-1}\}$$

and we also have that

$$Mh = \{h, fh\}$$

which means that $hM \neq Mh$. Thus, M not a normal subgroup of G.

For an abelian group, all subgroups are normal subgroups. However, most non-abelian groups have non-normal subgroups like S_3 and the dihedral group with 6 elements.

Example

The quoternion group (Q_8) is the group

$$Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$$

where $i^2 = j^2 = k^2 = -1$, $ij = k, ji = -k, jk = i, kj = -i, ki = j$, and $ik = -j$. This is defintely a group as it is closed, associative, has an identity element which is 1, and has inverses. We also have that $|Q_8| = 8$ and Q_8 is not abelian.

There is only one two element subgroup which is $\{1, -1\}$ but since every element in this subgroup commutes with every element in Q_8, this will be a normal subgroup.

A subgroup with four elements will be $\{1, -1, i, -i\}$ (we can replace i with j or k and $-i$ with $-j$ or $-k$ respectively) and this will be a normal subgroup also.

Therefore all proper subgroups of this non-abelian group are all normal subgroups.

If $N \triangleleft G$, that means that all $b \in G$ satisfy $b^{-1}Nb = N$ but it does not necessarily mean that $b^{-1}nb = n$.

Problem (Section 2.5 #12)

Prove that if $Z(G)$ is the center of G, then $Z(G) \triangleleft G$.

Solution: We will write $Z(G)$ as Z for short. For any $b \in G$, we have that $b^{-1}Zb = Z(b^{-1}b) = Z$ which proves that Z is a normal subgroup.

It is easier to check that $b^{-1}Nb \subset N$ compared to checking that $b^{-1}Nb = N$. $\square$

Problem (Section 2.5 #17)

If $M \triangleleft G$, $N \triangleleft G$, prove that $M \cap N \triangleleft G$.

Solution: For all $b \in G$, we have that $b^{-1}Mb \subset M$ and $b^{-1}Nb \subset N$. Now take any $p \in M \cap N$. Then $b^{-1}pb \in M$ since $p \in M$ and $b^{-1}pb \in N$ since $p \in N$. Thus $b^{-1}pb \in M \cap N$. Therefore since p was an arbitrary element in $M \cap N$, we have that $b^{-1}(M \cap N)b \subset M \cap N$ which proves that $M \cap N \triangleleft G$. $\square$

Problem (Section 2.5 #37)

If G is a non-abelian group of order 6, prove that $G \cong S_3$.

Solution: Any non-identity element of G has order 2 or 3 because the order cannot be 1 as it is not the identity and the order cannot be 6 otherwise it would be cyclic and therefore it would be abelian.

Take $a, b \in G$ such that a has order 2 and b has order 3. Then a, b generate G. We also have that $\{e, b, b^2\}$ is a subgroup of G. Then we have that

$$G = \{e, b, b^2, a, ab, ab^2\}$$

and now we look for what is ba? So the only way that G is non-abelian is if $ba = ab^2$. Therefore there is only 1 non-abelian group of order 6. $\square$

Problem (Section 2.5 #50)
Suppose that $M \subset N \subset G$ where G is a group. If $N \lhd G$ and $M \lhd N$, must $M \lhd G$?

Solution: For all $g \in G$ and $m \in M$, must $g^{-1}mg \in M$? We will prove that $M \lhd G$ is not forced. We will now found a counterexample.

Let G be the dihedral group with 8 elements. Then

$$G = \{e, f, h, fh, h^2, fh^2, h^3, fh^3\}$$

where $f^2 = h^4 = e$ and $hf = fh^{-1}$. Take the subgroup

$$N = \{e, f, h^2, fh^2\}.$$

We can easily verify this is a subgroup of G. Since (index) $i_G(N) = 2$, we have that $N \lhd G$. Take the subgroup

$$M = \{e, f\}$$

which is well known to be a subgroup. Since (index) $i_N(M) = 2$, we have that $M \lhd N$. However M is not normal in G since $hM \neq Mh$ since $hM = \{h, hf\}$ and $Mh = \{hfh\}$. Therefore this is a counterexample which means that even if $N \lhd G$ and $M \lhd N$, it is not necessary that $M \lhd G$. $\square$

§13 Factor Groups

Definition
Let G be any group and let $N \lhd G$. We define a new group called the *quotient group* or *factor group* of G over N, which is denoted by G/N.

Definition
What is G/N? This is the collection of cosets of N in G. What is the operation? The operation is if you have two cosets Na and Nb, then $(Na)(Nb) = N(ab)$.

Is this well defined? That is, if $Na_1 = Na_2$ and $Nb_1 = Nb_2$, does that imply that $N(a_1b_1) = N(a_2b_2)$?

If $Na_1 = Na_2$ and $Nb_1 = Nb_2$, then this implies that $a_1a_2^{-1} \in N$ and $b_1b_2^{-1} \in N$. We need to show that $(a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} \in N$. Suppose that $b_1b_2^{-1} = n_1$ which implies that $b_2^{-1} = b_1^{-1}n_1$. Also suppose that $a_1a_2^{-1} = n_2$ which implies that $a_2^{-1} = a_1^{-1}n_2$. Now note that

$$a_1b_1b_2^{-1}a_2^{-1} = a_1n_1a_2^{-1} = a_1n_1a_1^{-1}n_2.$$

Now notice that $a_1n_1a_1^{-1} \in N$ since $N \lhd G$. Therefore since $a_1n_1a_1^{-1} \in N$ and $n_2 \in N$, then that implies that $a_1n_1a_1^{-1}n_2 = a_1b_1b_2^{-1}a_2^{-1} \in N$ which implies that $N(a_1b_1) = N(a_2b_2)$.

Now we will verify that it is a group. Closure is obvious since $(Na)(Nb) = N(ab)$. This operation is associative since G is associative. The identity element is Ne. Also notice that $(Na)(Na^{-1}) = N(aa^{-1}) = Ne$ which implies that $(Na)^{-1} = Na^{-1}$. Therefore inverses also exist. Therefore this is a group.

Say that G is a group and H is not normal in G. Then there exists some element $a \in G$ and $h \in H$ for which $aha^{-1} \notin H$. Then we have that $(Ha)(Ha^{-1}) = H$. However we can rewrite it as $H(aHa^{-1}) = H$ but we said $aHa^{-1} \notin H$ which means that $H(aHa^{-1})$ cannot equal H. Therefore this operation is only valid in normal subgroups.

Theorem

In G/N, we denote $[g]$ as the coset Ng. Now consider $f : G \to G/N$ defined by $f(g) = [g] = Ng$. Then notice that

$$f(g_1g_2) = N(g_1g_2) = (Ng_1)(Ng_2) = f(g_1)f(g_2)$$

which implies that f is a homomorphism. We have that $\text{Ker}(f) = N$.

Remember that $o(G/N) = i_G(N)$, assuming that the order is finite. We can also say that $o(G/N) = \frac{o(G)}{o(N)}$, again assuming that the order of G is finite.

Theorem (Cauchy's Theorem (not generalized))

If G is a finite abelian group and p is a prime such that $p \mid o(G)$, then G has an element of order p.

Proof: Suppose this is true for all groups of order $< |G|$. Take N to be a proper normal subgroup of G. If $p \mid o(N)$, then N has an element of order p since $o(N) < |G|$ and we are done.

Say this is not the case. Then $p \mid o(G/N)$ since $p \nmid o(N)$. Therefore G/N has an element $[a]$ or Na of order p since $o(G/N) < o(G)$. Then since Na has order p, we must have that $(Na)^p = N$ which implies that $N(a^p) = N$. Therefore $a^p \in N$ but $a \notin N$. Thus $(a^p)^{o(N)} = e \longrightarrow (a^{o(N)})^p = e$. So maybe $a^{o(N)}$ is the element of order p in G. The only way not is if $a^{o(N)} = e$. However we then have that $a^{o(N)} = e \in N$ and since $a^p \in N$, we have that $a^{\gcd(p,o(N)} \in N$. However since we said that $p \nmid o(N)$, we must have that $a \in N$ which is a contradiction. Therefore we must have that $a^{o(N)}$ has order p.

Therefore in both cases, we have shown that if there exists a prime $p \mid o(G)$, then G has an element of order p. □

Problem (Section 2.6 #7)

If G is a cyclic group and N is a subgroup of G, show that G/N is a cyclic group.

Solution: Say that $G = \{e, a, a^2, \dots, a^{n-1}\}$ and let $N = \{a, a^k, a^{2k}, \dots\}$ where a^k is the smallest positive power of a in n. Then we have that

$$G/N = \{N, Na, Na^2, \dots, Na^{k-1}\}$$

where all of the cosets here are distinct. Therefore we can clearly see that G/N is cyclic. □

Problem (Section 2.6 #10)

Let G be a finite abelian group and say p is a prime such that $p \mid o(G)$ and p^b is the highest power of p dividing $o(G)$. Prove G has a following subgroup with p^b elements.

Solution: Let S be all elements in G whose order is p^n for some nonnegative integer n. Then $S \neq \{e\}$ by Cauchy's Theorem.

Note that S is a subgroup of G because if $a, b \in S$, then $a^{p^{n_1}} = b^{p^{n_2}} = e$. Then $(ab)^{p^{n_3}} = e$ where $n_3 = \max(n_1, n_2)$. How large is S? If $|S| = p^b$, we are done. Note that we have $|S| = p^n$ for some non-negative integer n since if q is a prime such that $q \mid o(S)$, then S has an element of order q.

Now suppose that $|S| \neq p^b$. Now consider the group G/S. We have that $p \mid o(G/S)$. Thus G/S has an element, Sx, of order p. Then $x^p \in S$ but $x \notin S$. We also have that $(x^p)^{o(S)} = e$ since $x^p \in S$. However $p \cdot o(S)$ is still a power of p which implies that $x \in S$ which is a contradiction. Thus the only conclusion is that $|S| = p^b$ which is the desired result. □

§14 The Homomorphism Theorems

Theorem (First Homomorphism Theorem)

Say that G and G' are groups and $f : G \to G'$ is an onto homomorphism. Then if $K = \text{Ker}(f)$, we have

$$G/K \cong G'.$$

Proof: Take $\phi : G/K \to G'$ defined by $\phi([b]) = \phi(Kb) = f(b)$. We need to show that this is a function. That is, $Kb = Kc$ implies that $f(b) = f(c)$ must be shown. If $Kb = Kc$, then we have that $bc^{-1} \in K$. So we have that

$$f(bc^{-1}) = e' \longrightarrow f(b)f(c^{-1}) = e' \longrightarrow f(b)[f(c)]^{-1} = e'$$

which implies that $f(b) = f(c)$. Therefore this is well defined and it is a function.

Now we must show that it is a homomorphism. Notice that

$$\phi([b][c]) = \phi(Kb \cdot Kc) = \phi(Kbc) = f(bc) = f(b)f(c) = \phi([b])\phi([c])$$

which implies that it is a homomorphism. Since f is onto, we have that ϕ is also onto.

We will now show that ϕ is $1-1$. Say that $\phi([b]) = \phi([c])$ which implies that $f(b) = f(c)$. Therefore we have that $bc^{-1} \in K$ which implies that $Kb = Kc$ which implies that $[b] = [c]$. Therefore we have that ϕ is $1-1$. Therefore since ϕ is $1-1$,onto, and is a homomorphism, we have that ϕ is an isomorphism. □

Theorem (Correspondence Theorem)

Let $f : G \to G'$ be an onto homomorphism. Say that $H' \subset G'$ is a subgroup. Then we have that

$$H = \{h \in G \mid f(h) \in H'\}$$

is a subgroup of G, $H/K \cong H'$, and if $H' \lhd G'$, then $H \lhd G$. (Here $K = \text{Ker}(f)$.)

Proof: Say $b, c \in H$, that is $f(b), f(c) \in H'$. Then $f(b)[f(c)]^{-1} \in H'$ since H' is a subgroup which implies that

$$f(b)f(c^{-1}) \in H' \longrightarrow f(bc^{-1}) \in H' \longrightarrow bc^{-1} \in H$$

which implies that H is a subgroup of G.

Say $H' \lhd G'$. Take arbitrary $b \in G$ and $h \in H$. We wish to prove that $b^{-1}hb \in H$. Note that since f is a homomorphism, we have that

$$f(b^{-1}hb) = f(b^{-1})f(h)f(b) = [f(b)]^{-1}f(h)f(b)$$

where $f(h) \in H'$. Now we must have that $[f(b)]^{-1}f(h)f(b) \in H'$ because $H' \lhd G'$. Therefore since $f(b^{-1}hb) = [f(b)]^{-1}f(h)f(b) \in H'$, we must have that $b^{-1}hb \in H$ which implies that $H \lhd G$. □

Theorem (Second Homomorphism Theorem)

Let H be a subgroup of a group G and N a normal subgroup of G. Then $HN = \{hn \mid h \in H, n \in N\}$ is a subgroup of G, $H \cap N$ is a normal subgroup of H, and $H/(H \cap N) \cong (HN)/N$.

Theorem (Third Homomorphism Theorem)

Let $f : G \to G'$ be an onto homomorphism. Say that $N' \lhd G'$ and N is the set of elements of G mapping into N'. We showed that $N \lhd G$ is forced due to the correspondence theorem. Again we let $K = \text{Ker}(f)$. However, we can go further and say that $G/N \cong G'/N'$ and we can also say that $G/N \cong (G/K)(N/K)$.

Problem (Section 2.7 #3)

Let G be the group of nonzero real numbers under multiplication and let $N = \{1, -1\}$. Prove that $G/N \cong$ positive real numbers under multiplication.

Solution: Let $f : G \to \mathbb{R}^+$ where $f(x) = x^2$. Does $f(xy) = f(x) \cdot f(y)$? Yes this does hold which means that f is a homomorphism. Here notice that $\text{Ker}(f) = N$. Also notice that f is definitely onto. Therefore by the first homomorphism theorem, we have that $G/N \cong \mathbb{R}^+$. $\square$

§15 Cauchy's Theorem

Theorem (Cauchy's Theorem)

If $p \mid o(G)$, then G has an element of order p. (We went over abelian case, but it is true for the non-abelian case also.)

Now we want to try to find non-abelian groups of order $p \cdot q$ where p and q are distinct primes.

Theorem

Say that $|G| = pq$ where $p > q$. Then G has only one subgroup H of order p and $H \lhd G$.

Proof: Say that H_1 and H_2 were two distinct subgroups of order p in G. Then $H_1 \cap H_2 = \{e\}$. Say that $H_1 = (a)$ and $H_2 = (b)$ and consider the set

$$C = \{a^i b^j \mid i, j \in [0, p-1]\}.$$

Then we have that $|C| = p^2$ because $a^{i_1} b^{j_1} \neq a^{i_2} b^{j_2}$ unless we have that $i_1 = i_2$ and $j_1 = j_2$. However this is a contradiction because $|G| = pq < p^2$ since $p > q$. Thus this was impossible and there exists only one subgroup H of order p in G.

Then for all $x \in G$, we have that $x^{-1}Hx$ is a subgroup of order p in G. But since there is only one subgroup of order p in G, this implies that $x^{-1}Hx = H$ for all $x \in G$ which is equivalent to saying $H \lhd G$. $\square$

Theorem

Say that $|G| = pq$ where p and q are distinct primes such that $p > q$. If $q \nmid (p-1)$, then G is cyclic.

Proof: Say that $a \in G$ generates the subgroup H of order p and also take $b \in G$ where b is of order q. Now what is $b^{-1}ab$? Because $H \lhd G$ (previous result), this must be in H, therefore some power of a.

Say that $b^{-1}ab = a^i$ for some $i \in [1, p-1]$. Note that $(b^{-1}a^k b)^n = b^{-1}a^{k\cdot n}b$. Therefore note that we have $b^{-1}ab = a^i$ and

$$b^{-2}ab^2 = b^{-1}a^i b = (b^{-1}ab)^i = a^{i^2}.$$

Then we have that $b^{-3}ab^3 = a^{i^3}$ by using similar logic. So for any j, we have that

$$b^{-j}ab^j = a^{i^j}.$$

In particular, we have that

$$b^{-q}ab^q = a^{i^q}$$

but since b is of order q, we have that

$$a = a^{i^q} \longrightarrow a^{i^q - 1} = e \longrightarrow p \mid (i^q - 1).$$

Therefore we have that

$$i^q \equiv 1 \pmod{p}.$$

We also know that

$$i^{p-1} \equiv 1 \pmod{p}.$$

Putting these two together, we must have that

$$i^{\gcd(q,p-1)} \equiv 1 \pmod{p}.$$

However since we assumed that $q \nmid (p-1)$, we have that $\gcd(q, p-1) = 1$ which implies that $i \equiv \pmod{p}$ which implies that $i = 1$. Therefore going back, we see that $b^{-1}ab = a^i = a$ which implies that $ba = ab$ which means that G is abelian. Therefore we have that G is cyclic since ab has order pq which means the powers of ab sweep out all of G. $\square$

Problem (Section 2.8 #8)

Prove that if G is a group of order 99, then prove G has a nontrivial normal subgroup.

Solution: Take H to be a subgroup of G of order 11. We claim that H must be the only subgroup of G of order 11. Say that $K \neq H$ was a different subgroup of G of order 11. Then $|HK| = 11^2 = 121$, however $|G| = 99$ which is a contradiction. Therefore H is the only subgroup of G of order 11. Therefore we must have that for all $x \in G$ that $x^{-1}Hx = H$ but since there is only one subgroup H, we must have that $H \lhd G$. $\square$

Problem (Section 2.8 #9/10)

Prove that if G is a group of order 42, then prove that G has a normal subgroup of order 21.

Solution: Let H be a subgroup of G of order 7. Then H is the only subgroup of order 7 in G for if K was a different one, then $|HK| = 7^2 = 49 > 42$ which would be a contradiction. Therefore H is the only subgroup of order 7 in G. This implies that $H \lhd G$.

Take J to be a subgroup of G such that $|J| = 3$. Consider HJ. We will have HJ is a subgroup of G since H is normal in G. Then $|HJ| = 21$. So HJ is a subgroup of G of order 21, and since $i_G(HJ) = 2$, we have that $HJ \lhd G$. $\square$

§16 Direct Products

Definition (External Direct Product of Groups)

Let $G_1, G_2, \ldots, G_n$ be groups where they could be potentially completely unrelated. Then we have that

$$G_1 \times G_2 \times G_3 \times \cdots \times G_n$$

is the external direct product. Then we have that

$$(g_1, g_2, \ldots, g_n) * (g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n').$$

Example

Consider the direct product

$$\mathbb{Z}_6 \times S_3.$$

Since $H \subset \mathbb{Z}_6$ is a subgroup, we have that $H \times \{e\}$ is a subgroup of $\mathbb{Z}_6 \times S_3$. If $K \subset S_3$ is a subgroup, we have that $\{0\} \times K$ is also a subgroup of $\mathbb{Z}_6 \times S_3$.

Example

Consider the direct product

$$\mathbb{Z}_p \times \mathbb{Z}_p$$

where p is prime.

Then we have that $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2$. This is abelian because each of the components are abelian, so the product must be abelian. This group is not cyclic since the order of each element will be the $\text{lcm}(o(a), o(b))$ where a is in the first group and b is in the second group. Therefore the order of each element will either be 1 or p. Since no element has order p^2, this group cannot be cyclic.

Definition (Internal Direct Product)

We have that

$$G = N_1 N_2 \ldots N_k$$

where $N_i \triangleleft G$ for all i and each element of G can be written uniquely as $n_1 n_2 \ldots n_k$.

Theorem

Say that $M, N \triangleleft G$ and $M \cap N = \{e\}$. Prove that for all $m \in M$ and all $n \in N$ that $mn = nm$.

Proof: For any $m \in M$ and $n \in N$, consider the element

$$x = mnm^{-1}n^{-1} = (mnm^{-1})n^{-1} \in N$$

since $mnm^{-1} \in N$ since $N \triangleleft G$. Similarly consider

$$x = mnm^{-1}n^{-1} = m(nm^{-1}n^{-1}) \in M$$

since $nm^{-1}n^{-1} \in M$ since $M \triangleleft G$. Therefore since we said that $M \cap N = e$, we must have that $mnm^{-1}n^{-1}$ which implies that $mn = nm$ by cancellation laws. $\square$

Problem (Section 2.9 #3)
Let G be a group and let $A = G \times G$. In A, let $T = \{(g, g) \mid g \in G\}$.
(a) Prove that T is a subgroup of A.
(b) Prove that $T \lhd A$ if and only if G is abelian.

Solution: (a) Take $(g_1, g_1), (g_2, g_2) \in T$. Then we have that

$$(g_1, g_1) \cdot ((g_2, g_2))^{-1} = (g_1, g_1) \cdot (g_2^{-1}, g_2^{-1}) = (g_1 g_2^{-1}, g_1 g_2^{-1}) \in T$$

which implies that T is a subgroup of A.

(b) Take $(g_1, g_1) \in T$ and $(g_2, g_3) \in A$. Then what is $(g_2, g_3)^{-1}(g_1, g_1)(g_2, g_3)$? We have that

$$(g_2, g_3)^{-1}(g_1, g_1)(g_2, g_3) = (g_2^{-1} g_1 g_2, g_3^{-1} g_1 g_3).$$

But are these coordinates equal? Is $g_2^{-1} g_1 g_2 = g_3^{-1} g_1 g_3$?

Suppose we have that $g_1 = g_3$. Then we have that

$$g_2^{-1} g_3 g_2 = g_3^{-1} g_3 g_3 \longrightarrow g_2^{-1} g_3 g_2 = g_3 \longrightarrow g_3 g_2 = g_2 g_3$$

and since g_2 and g_3 are arbitrary elements, we must have that G is abelian. □

§17 The Symmetric Group (Chapter 3)

Definition (Permutation Groups)
We mostly only deal with S_n which is a finite permutation group. For $fg \in S_n$, that means apply g then apply f.

Suppose that we have the permutation

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

Then we have that $f(1) = 1$, $f(2) = 3$, $f(3) = 4$, $f(4) = 5$, and $f(5) = 2$. Now suppose that we have another permutation

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

Then we have that $g(1) = 3$, $g(2) = 2$, $g(3) = 1$, $g(4) = 5$, and $g(5) = 4$. Therefore if we want to calculate

$$\begin{pmatrix} 1 & 3 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 & 1 & 5 & 4 \end{pmatrix},$$

we can use function composition to calculate this.

We can write these permutations as matrices to help us multiply them. On the top, we have 1 2 3 ... n and on the bottom, we have the permutation itself. Therefore we can write the first permutation as

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

and we can the second permutation as

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

To compute fg, send an element through the whole thing (starting on the right). Therefore we have that

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

§18 Cycle Decomposition

The most convenient way to make a permutation on a finite set tends to be with *disjoint cycles*.

Definition

Start with an element a_1. Say that $a_1 \to a_2 \to a_3 \to \cdots \to a_k \to a_1$ for some k. We write this $(a_1 a_2 a_3 \dots a_k)$ and we call this a cycle. Each element maps to the one on its direct right while the rightmost element maps to the first element.

For any permutation, start with an arbitrary element and find its cycle. Then if any elements are leftover, pick one of them and find its cycle. Continuing like this until all elements are exhausted, we can see that the permutation is the product of these disjoint cycles. The cycles of this type are either identical or disjoint.

Suppose that we have two cycles $(a_1 a_2 \dots a_k)$ and $(b_1 b_2 \dots b_j)$. Say that b_1 is not in the first cycle. Then these two cycles are disjoint. Suppose that if $b_3 = a_7$. Then we have that $b_2 = a_6$ because b_2 maps to b_3 and a_6 maps to a_7. Then we also have that $b_1 = a_5$ which is a contradiction since we said b_1 is not in the first cycle. Using a similar type of argument, we can see that these two cycles have to be disjoint.

The product of two disjoint cycles is abelian. Therefore if we write a permutation as a product of disjoint cycles, we do not have to worry about the order of the disjoint cycles in the product as the product of disjoint cycles is abelian.

Definition

If $(a_1 a_2 \dots a_k)$ is a cycle, then this is called a k-cycle as the cycle has k elements.

When writing a permutation as a product of disjoint cycles, we do not include 1-cycles (elements that map to themselves).

Definition

A 2-cycle is called a *transposition*. So cycles are a generalization of transpositions.

If we write the group S_3 such that each element is a cycle, we have that

$$S_3 = \{e, (12), (13), (23), (123), (132)\}.$$

Question — Suppose that $\sigma \in S_{14}$ and we have that

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & & & & & & \\ 2 & 1 & 4 & 5 & 3 & 2 & 8 & 9 & 6 & 11 \\ 12 & 13 & 14 & 10 & & & & & & \end{pmatrix}.$$

What is $o(\sigma)$?

Solution: We will start by writing σ as a product of disjoint cycles. Doing this, we see that

$$\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 6 & 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 10 & 11 & 12 & 13 & 14 \end{pmatrix}.$$

The order of a k-cycle is always k. In order to have $\sigma^j = e$, we need each cycle to the power $j = e$. Thus we must have that $o(\sigma)$ must be divisible by order of each of its disjoint cycles. Thus $o(\sigma) = \text{lcm}(\text{lengths of disjoint cycles})$. $\square$

Theorem

Consider the cycle $(a_1a_2a_3 \dots a_k)$. Can we write $(a_1a_2a_3 \dots a_k)$ as $(a_ka_1)(a_{k-1}a_1) \dots (a_3a_1)(a_2a_1)$? Yes we can. We have that $(a_1a_2a_3 \dots a_k) = (a_ka_1)(a_{k-1}a_1) \dots (a_3a_1)(a_2a_1)$ which means that every cycle can be written as the product of transpositions. So for any permutation do this with each of the disjoint cycles. Therefore we also have that every permutation is the product of transpositions.

Question — In S_n, what is the largest possible order of an element?

Solution: In S_3, it is 3. In S_4, it is 4. Now what is it in S_5? In S_5, it is 6 because we have take the product of a 2 cycle and a 3 cycle. To try to maximize order of element in S_n, write $n = m_1 + m_2 + \cdots + m_k$ and maximize $\text{lcm}(m_1, m_2, \dots, m_k)$. $\square$

Problem (Section 3.2 #7)

Find a deck of 13 cards requiring 20 repeats to return to its original order. Find a deck of 13 cards requiring 42 repeats to return to its original order.

Solution: We are really asking to find permutations in S_{13} of order 20 as well as order 42. Therefore note that

$$\sigma_1 = \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8 & 9\end{pmatrix}$$

has order 20. Also note that

$$\sigma_2 = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4 & 5\end{pmatrix}\begin{pmatrix}6 & 7 & 8 & 9 & 10 & 11 & 12\end{pmatrix}$$

has order 42. We could have had that σ_2 be a product of a cycle of length 6 and a cycle of length 7. $\square$

Problem (Section 3.2 #10)

Prove that there is no $\sigma \in S_n$ such that $\sigma \begin{pmatrix}1 & 2\end{pmatrix} \sigma^{-1} = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$.

Solution: Note that

$$(\sigma \begin{pmatrix}1 & 2\end{pmatrix} \sigma^{-1})^3 = (\begin{pmatrix}1 & 2 & 3\end{pmatrix})^3 = e$$

which implies that

$$\sigma(\begin{pmatrix}1 & 2\end{pmatrix})^3\sigma^{-1} = e \longrightarrow \sigma \begin{pmatrix}1 & 2\end{pmatrix} \sigma^{-1} = e \longrightarrow \sigma \begin{pmatrix}1 & 2\end{pmatrix} = \sigma \longrightarrow \begin{pmatrix}1 & 2\end{pmatrix} = e$$

which is an obvious contradiction. Therefore so such σ can exist in S_n. $\square$

Problem (Section 3.2 #12)

Prove that there is no permutation $\sigma \in S_n$ with $n \geq 7$ such that $\sigma \begin{pmatrix}1 & 2 & 3\end{pmatrix} \sigma^{-1} = \begin{pmatrix}1 & 2 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7\end{pmatrix}$.

Solution: If $\sigma^{-1}(x) \neq 1, 2, 3$, then we have that

$$\sigma \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \sigma^{-1}(x) = x.$$

So in essence we have that $\sigma \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \sigma^{-1}$ an only "move" 3 elements. Therefore we cannot have that $\sigma \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \sigma^{-1} = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 & 7 \end{pmatrix}$ because the permutation on the left can only move 3 elements while the right moves 6 elements which is a contradiction. Therefore such a σ cannot exist. □

Problem (Section 3.2 #15)

Show that if τ is a k-cycle, show that $\sigma\tau\sigma^{-1}$ is also a k-cycle for any permutation σ.

Solution: Say that $\tau = (x_1 x_2 x_3 \dots x_k)$ and say that $\sigma(x_i) = y_i$ for all i, i.e. $\sigma^{-1}(y_i) = x_i$. For any element z which is not one of the y_i, $\sigma\tau\sigma^{-1}$ keeps z fixed. Thus $\sigma\tau\sigma^{-1}$ can only move $y_1, y_2, \dots, y_k$. Therefore we have that $\sigma\tau\sigma^{-1}(y_1) = y_2$, $\sigma\tau\sigma^{-1}(y_2) = y_3$, ... and we are able to show that $\sigma\tau\sigma^{-1} = (y_1 y_2 y_3 \dots y_k)$ which is a k-cycle. □

Problem (Section 3.2 #22)

Find an algorithm for finding $\sigma\tau\sigma^{-1}$ for any permutations $\sigma, \tau \in S_n$.

Solution: Write τ as a product of disjoint cycles. If $(x_1 x_2 \dots x_k)$ is one such cycle, that becomes $(\sigma(x_1)\sigma(x_2)\dots\sigma(x_k))$ in $\sigma\tau\sigma^{-1}$. So if we do that for each disjoint cycle, we can find $\sigma\tau\sigma^{-1}$. □

Definition

In any group G, if $a, b \in G$ are *conjugates* if there exists $x \in G$ with $x^{-1}ax = b$.

Definition

We have that $\sigma, \tau \in S_n$ have the same *cycle structure* if the lengths of their disjoint cycles are identical. In S_n, we have that two permutations are conjugates if and only if they have the same cycle structure.

Problem (Section 3.2 #17)

Show in S_n that $\begin{pmatrix} 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 & \dots & n \end{pmatrix}$ generate S_n.

Solution: Suppose that $\tau = \begin{pmatrix} 1 & 2 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \end{pmatrix}$. Then what is $\sigma\tau\sigma^{-1}$? We have that $\sigma\tau\sigma^{-1} = \begin{pmatrix} 2 & 3 \end{pmatrix}$. But we can see that $\begin{pmatrix} 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 2 & 3 \end{pmatrix}$ generate all permutations on $\{1, 2, 3\}$. Now let $\tau' = \begin{pmatrix} 2 & 3 \end{pmatrix}$. Now what is $\sigma\tau'\sigma^{-1}$? We have that $\sigma\tau'\sigma^{-1} = \begin{pmatrix} 3 & 4 \end{pmatrix}$. Notice that all permutations on $\{1, 2, 3\}$ together with $\begin{pmatrix} 3 & 4 \end{pmatrix}$ will generate all permutations on $\{1, 2, 3, 4\}$. We can keep going like this to see that we will eventually be able to generate S_n. □

§19 Odd and Even Permutations

Definition

Take any arbitrary $\sigma \in S_n$. Suppose that

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ x_1 & x_2 & x_3 & \dots & x_n \end{pmatrix}.$$

For $j, k \in [1, n]$ with $j < k$, if $x_j < x_k$, we say that (j, k) is *forward*, if $x_j > x_k$, we say that (j, k) is *backwards*.

If σ has an even number of backward pairs, we say that σ is an *even permutation*, if σ has an odd number of backward pairs, we say that σ is an *odd permutation*.

If you multiply a permutation with a transposition, it switches the parity of the permutation. When writing a permutation as a product of transpositions, if it has an even number of transpositions, it is an even permutation, if it has an odd number of transpositions, it is an odd permutation.

Theorem

In permutations, we have that even $\times$ even = even, even $\times$ odd = odd, and odd $\times$ odd = even. Because even $\times$ even is even, the collection of even permutations in S_n is a subgroup of S_n, denoted by A_n (alternating group).

Take $\phi : S_n \to \{1, -1\}$ and note that $\{1, -1\}$ is a group under multiplication. Then we have that $\phi(\tau) = 1$ if $\tau \in A_n$ and $\phi(\tau) = -1$ if $\tau \notin A_n$. Then note that ϕ is a homomorphism, which can be easily checked since $\phi(\tau_1\tau_2) = \phi(\tau_1)\phi(\tau_2)$ for all $\tau_1, \tau_2 \in S_n$. We also have that $\text{Ker}(\phi) = A_n$. Therefore by the First Homomorphism Theorem since ϕ is onto, we have that $S_n/A_n \cong \mathbb{Z}_2$ since $\mathbb{Z}_2 \cong \{1, -1\}$. Therefore we have that $\frac{o(S_n)}{o(A_n)} = 2$ which implies that $\frac{n!}{o(A_n)} = 2$ which implies that $o(A_n) = \frac{n!}{2}$.

Definition

It turns out that for all $n \geq 5$, A_n never has any proper normal subgroups. That is, for all $n \geq 5$, A_n is a *simple group*.

For a finite group G, taking proper $N \lhd G$, looking at N and G/N can help us figure out about G. But we cannot do this if G is simple.

Suppose that $f(x) = 0$ where $f(x)$ is a polynomial. If $\deg(f(x)) \leq 4$, then this can be solved using radicals. For $\deg(f(x)) \geq 5$, this can't necessarily be solved. For example, $x^5 - x - 1 = 0$. This is actually because A_n for $n \geq 5$ is simple (not solvable group). For $n \leq 4$, we have that A_n is not simple.

Theorem

Note that a k-cycle is an even permutation if k is odd and a k-cycle is an odd permutation if k is even.

Problem (Section 3.3 #6)

Show that any $\sigma \in A_n$ for $n \geq 3$ is a product of 3-cycles.

Solution: Write σ as a product of transpositions. So let

$$\sigma = \tau_1\tau_2 \dots \tau_{2k}$$

where $\tau_1, \tau_2, \ldots, \tau_{2k}$ are all transpositions. Pair these transpositions off. Suppose that $\tau_1 = \begin{pmatrix} a & b \end{pmatrix}$ and $\tau_2 = \begin{pmatrix} c & d \end{pmatrix}$. Then if $a, b \neq c, d$ then we have that

$$\begin{pmatrix} a & b & c \end{pmatrix} \begin{pmatrix} b & c & d \end{pmatrix} = \tau_1 \tau_2.$$

If τ_1 and τ_2 overlap, say $a = c$, $b \neq d$, then we have

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} a & d \end{pmatrix} = \begin{pmatrix} a & d & b \end{pmatrix}.$$

Therefore doing this for all pairs of transpositions, we can see that every $\sigma \in A_n$ can be written as the product of 3-cycles. □

Problem (Section 3.3 #7)

Show that all $\sigma \in A_n$ is a product of n-cycles.

Solution: To this end, let us prove every 3-cycle is a product of n-cycles. If we can prove this, then using the previous result, we must have that any $\sigma \in A_n$ is a product of n-cycles.

We will prove this for the cycle $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$. Now how do we write $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \tau_1 \tau_2$ where τ_1 and τ_2 are n-cycles. Note that

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 & n & n-1 & \ldots & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 & 2 & 4 & 5 & \ldots & n \end{pmatrix}.$$

Therefore we can write any 3-cycle as the product of n-cycles and since all $\sigma \in A_n$ can be written as the product of 3-cycles, we have that all $\sigma \in A_n$ can be written as the product of n-cycles. □

Remember that parity of cycle is opposite to its length. So for a general permutation, the parity of the permutation will be the parity of the number of cycles of even length.

§20 Definitions and Examples (Chapter 4)

Note that groups do not have a "0" style element. That is you do not have $0 * g = 0$ for all $g \in G$ for a group G. In $\mathbb{R}$, $a \cdot b = 0$ implies that $a = 0$ or $b = 0$. No other real number has that property.

Definition (Rings)

A ring, R, has two operations $+$ and $\cdot$, addition and multiplication. As usual we have that $ab = a \cdot b$.

Definition (Properties of Rings)

We must have that R is an abelian group under $+$. We must also have that R is closed and associative under $\cdot$. We must also have distributive properties in a ring R. This means that

$$a(b+c) = ab + ac \text{ and } (b+c)a = ba + ca.$$

Definition (More Properties of Rings)

In any ring R, 0 is the default expression for the additive identity.

If ring R has a multiplicative identity, by default, we use 1 to symbolize that. If is required that $1 \neq 0$. Such a ring is called a *ring with unit* or *ring with unity*.

Question — In R, is it required that

$$a \cdot b = 0 \longrightarrow a = 0 \text{ or } b = 0.$$

Solution: It is not required but it is possible in some rings and not possible in some rings.

If hypothetically $ab = 0$ with $a \neq 0$ and $b \neq 0$, then a and b are *zero divisors*.

Definition

A ring with no zero divisors is called a *domain*.

Definition

A ring R where $\cdot$ is commutative is called a *commutative ring*.

Definition

A commutative ring which is a domain or a commutative ring with no zero divisors is called an *integral domain*.

Definition

A ring with unit where every nonzero element has a multiplicative inverse is called a *division ring*.

Definition

A commutative division ring is called a *field*.

Example

Consider the set of nonnegative integers less than n under addition and multiplication modulo n which is denoted by $\mathbb{Z}_n$. This is always a ring. We can quickly verify that it is an abelian group under $+$ and it is closed and associative under multiplication and the distributive laws also work which implies that $\mathbb{Z}_n$ must be a ring as it satisfies all the properties. We also have that $\mathbb{Z}_n$ is always a commutative ring with unit. However if n is not prime, it is NOT a domain. If n is prime, then $\mathbb{Z}_n$ is a domain, in fact it is a field.

Example

For R being any ring, the set S of 2×2 matrices over R under usual matrix addition and multiplication is always a ring as well. Since the properties work in R, the properties will also work in S and if we choose to see if the properties hold manually, we will see that the properties do hold. S only has a unit element if R has a unit element. But S is almost never commutative and almost never is a domain (there might be some trivial case in which S is commutative or S is a domain).

Over real numbers, 2×2 matrices still are not commutative and are still not a domain. What if we take only 2×2 matrices with nonzero determinant? These are a group under multiplication but not a ring as it is not closed under addition anymore.

Definition

For any ring R, a subset $T \subset R$ is a *subring* if T is a ring on its own.

Theorem (Subring Test)

To verify $T \subset R$ is a subring, check that T is a subgroup under $+$ and check that it is closed under $\cdot$. This is how to test if a subset $T \subset R$ is a subring of a ring R.

Say for R being any ring, you take 2×2 matrices with nonzero determinant. Is multiplication closed?

Consider in $\mathbb{Z}_6$. What is the product of the matrices

$$\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

However this matrix has determinant 0 which means that multiplication is not closed.

Example (Quaternions)

These are of the form

$$\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

where the α_n's are real numbers. We add these "coordinate-wise" and we have multiplication via the distributive law using the same way as we did with quoternions. The quaternions satisfy all the properties of a ring so the quaternions form a ring. Quaternions are actually a ring with unit. In fact, the quaternions form a division ring. This is because we have that

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot \frac{(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k)}{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2} = 1.$$

The quaternions are a noncommutative division ring.

For F being any field, let $H(F)$ be the ring of quaternions over F. That is,

$$\{f_0 + f_1 i + f_2 j + f_3 k\}$$

where $f_0, f_1, f_2, f_3 \in F$. We had also shown that $H(\mathbb{R})$ is a division ring.

Problem (Section 4.1 #36)

Show that $H(\mathbb{C})$ is not a division ring.

Solution: Note that

$$(1 + \sqrt{-1}j)(1 - \sqrt{-1}j) = 0$$

which implies that these two elements are zero divisors. Therefore $H(\mathbb{C})$ cannot be a division ring as it has zero divisors. $\square$

Problem (Section 4.1 #37)
Find $x \in H(\mathbb{C})$ with $x^2 = 0$ but $x \neq 0$.

Solution: Suppose that α_i's $\in \mathbb{C}$ and let $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$. Then we have that

$$x^2 = (\alpha_0^2 - \alpha_1^2 - \alpha_2^2 - \alpha_3^2) + i(2\alpha_0\alpha_1) + j(2\alpha_0\alpha_2) + k(2\alpha_0\alpha_3) = 0.$$

Therefore we must have that each component equal to 0. Take $\alpha_0 = 0$. Then the i, j, and k components are all equal to 0. Therefore we must also have that

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0.$$

Therefore we can take that $\alpha_1 = 1, \alpha_2 = \sqrt{-1}$, and $\alpha_3 = 0$ which satisfies the equation. Therefore we can have that $x = i + \sqrt{-1}j$ which satisfies that $x^2 = 0$ but $x \neq 0$. □

Problem (Section 4.1 #40)
Prove that a finite domain is a division ring.

Solution: Say that D is a finite domain. Consider, for fixed $a \in D$ and $a \neq 0$, the set

$$\{ax \mid x \in D\}.$$

If $x \neq y$, then $ax \neq ay$ otherwise we have that $a(x - y) = 0$ which is a contradiction because D is a domain. Thus we must have that

$$\{ax \mid x \in D\} = D.$$

Thus there exists $y \in D$ with $ay = a$. Maybe y will be a multiplicative identity? For any $b \in D$, there exists $z \in D$ for which $za = b$. Therefore we have that

$$ay = a \longrightarrow zay = za \longrightarrow by = b$$

which implies that y is a right identity for all $b \in D$. By similar logic, there exists a left identity for all $b \in D$. Let e be the right sided identity and f be the left sided identity. Then we have that

$$e = fe = f$$

which implies that there is a two-sided identity. Now since

$$\{ax \mid x \in D\} = D,$$

there exists an element $x_1 \in D$ such that $ax_1 = e$. We now have to prove that there exists a two sided inverse. It suffices to prove that $ax_1 - e = 0$. Note that

$$a(x_1 a - e) = ax_1 a - ae = a - a = 0$$

but since $a \neq 0$, we must have that $x_1 a - e = 0$ which implies that the right inverse of an element must also be its left inverse. Therefore D is a division ring. □

Problem (Section 4.1 #34)
Let T be the group of matrices A with entries in the field $\mathbb{Z}_2$ such that $\det(A) \neq 0$. Prove that $T \cong S_3$.

Solution: Note that

$$T = \{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\}.$$

Note that T is not abelian. Therefore we must have that T is isomorphic to S_3 since they both have order 6 and are both nonabelian which implies that they are the same group. Therefore they must be isomorphic so $T \cong S_3$. □

§21 Some Simple Results

Definition (Properties of Rings)

Let R be any ring. Then we have that for all $a, b \in R$,

$$0a = a0 = 0.$$

We denote $-a$ as the additive inverse of a. We also have that

$$(-a)b = a(-b).$$

We also have that

$$0 = (a + (-a))b = a(b + (-b)) \longrightarrow (-a)b = a(-b).$$

Specifically a ring with unit R satisfies

$$-1 \cdot a = -a.$$

Theorem (Binomial Theorem in Rings)

We have that

$$(a + b)^2 = a^2 + b^2 + ab + ba.$$

Definition

A ring R is called a *Boolean ring* if we have that $x^2 = x$ for all $x \in R$. It turns out that such a ring is always commutative.

This is because we have that

$$x + y = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx$$

which implies that $xy + yx = 0$ for all $x, y \in R$. Then we have that

$$x(xy + yx) = 0 \longrightarrow x^2y + xyx = 0 \longrightarrow xy + xyx = 0.$$

We also have that

$$(xy + yx)x = 0 \longrightarrow xyx + yx^2 = 0 \longrightarrow xyx + yx = 0.$$

Therefore we have that

$$xy + xyx = xyx + yx \longrightarrow xy = yx$$

which implies that the ring is commutative.

Problem (Section 4.2 #8)
If F is a finite field, show that:
(a) There exists a prime p such that $pa = 0$ for all $a \in F$.
(b) If F has q elements, then $q = p^n$ for some integer n. (**Hint:** Cauchy's Theorem)

Solution: (a) For all $a \in F$, there exists a $k \in \mathbb{N}$ with the property that $ka = 0$ because listing $a, 2a, 3a, \ldots$ will eventually repeat since F is a finite field. If $j_1 a = j_2 a$, then we have that $(j_2 - j_1)a = 0$.

Do this for all $a \in F$ and take the lcm of those integers. Thus there exists $j \in \mathbb{N}$ with $ja = 0$ for all $a \in F$. Take the smallest $b \in \mathbb{N}$ such that $ha = 0$ for all $a \in F$. We claim that b must be prime. Say that b is not prime and $b = mn$ with $m, n > 1$. Then there exists $a_1, a_2 \in F$ such that $ma_1 \neq 0$ and $na_2 \neq 0$. But then we have that

$$(ma_1)(na_2) = (mn)a_1a_2 \neq 0 \longrightarrow b(a_1a_2) \neq 0$$

which is a contradiction. Therefore we must have that b is prime.

(b) Think of F as an addition group. In that group, every nonidentity element has order p. Thus for prime q with $q \neq p$, we cannot have that $q \mid o(p)$ because then F has element with additive order q by Cauchy's theorem. Therefore we have that the cardinality of the field must be a power of p. $\square$

Takeaway. In rings, be very careful about "order" of an element because if there is a unit, that could mean additive or multiplicative order.

§22 Ideals, Homomorphisms, and Quotient Rings

Definition (Ring Homomorphisms)
Let R and R' be rings. Then we have that $f : R \to R'$ is a *ring homomorphism* if for all $a, b \in R$, we have that $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

Note that just as in groups, remember that R and R' may not have the same addition and/or multiplication.

We define ring monomorphism, ring isomorphism, and ring automorphism in the same way that we define them for groups.

Definition
If $f : R \to R'$ is a ring homomorphism and $0'$ is the additive identity in R', then we define

$$K = \{k \in R \mid f(k) = 0'\}$$

is the *kernel* of f.

As we know from groups, K is always an additive subgroup of R. We also have that K is clearly closed under multiplication. Thus K is a subgroup of R.

Let Q be the set of real quaternions and suppose that

$$H = \{\alpha_0 + \alpha_1 i \mid \alpha_0, \alpha_1 \in \mathbb{R}\}.$$

Then H is a subring of Q. Say we had a ring homomorphism f on Q with kernel H. That is, $f(\alpha_0 + \alpha_1 i) = 0'$ and these are the only elements going to $0'$. But then we have that

$$f(k) = f(ij) = f(i)f(j) = 0'f(j) = 0'.$$

So since $f(k) = 0'$, we have that $k \in H$ since H is the kernel but this is a contradiction as $k \notin H$. Therefore the subring H cannot be the kernel of any ring homomorphism.

This also shows that not all subrings can be the kernel of a ring homomorphism.

Theorem

For K being the kernel of a ring homomorphism on R, for all $r \in R$ and $k \in K$, if

$$f(rk) = f(r)f(k) = f(r)0' = 0',$$

then we must have that $rk \in K$. Similarly $kr \in K$. So in essence, for any kernel K in this setting, not only must K be closed under multiplication, we must have that

$$rk, kr \in K \text{ for all } r \in R, k \in K.$$

Definition (Ideal)

For a ring R and a subring $I \subset R$, if I has the property that for all $i \in I$, $r \in R$, you have $ir, ri \in I$, then I is an *ideal* of R (two-sided ideal).

Definition

If $I \subset R$ and only $ri \in I$ is required, then I is a *left ideal*. If only $ir \in I$ is required, then I is a *right ideal*.

Definition

Say R is any ring and K is an ideal in R. Define R/K as the quotient ring of K in R. We have that R/K are the additive cosets of K in R, that is, the collection of cosets of the type

$$\{a + K \mid a \in R\}.$$

So in R/K, if we take two cosets, $a + K, b + K$, our operations are

$$(a + K) + (b + K) = (a + b) + K$$
$$(a + K)(b + K) = ab + K.$$

What if $a + K = a' + K$ and $b + k = b' + K$? Can we be sure that $ab + K = a'b' + K$?

Suppose that $a + K = a' + K$ and $b + k = b' + K$ are true. Then we have that $a - a', b - b' \in K$. Then we also have that

$$(a - a')b + a'(b - b') \in K \longrightarrow ab - a'b' \in K$$

which implies that $ab + K = a'b' + K$.

Therefore this proves that the operation $(a + K)(b + K) = ab + K$ is well defined.

Let $\phi : R \to R/K$ defined by $\phi(a) = a + K$. Then ϕ is a ring homomorphism with kernel K. Therefore this proves that every ideal can be the kernel of some ring homomorphism.

Theorem (First Homomorphism Theorem)
Let the mapping $\phi : R \to R'$ be a homomorphism of R onto R' with kernel K. Then $R' \cong R/K$; in fact, the mapping $\psi : R/K \to R'$ defined by $\psi(a+K) = \phi(a)$ defines an isomorphism of R/K onto R'.

This also creates a correspondence between the ideals in R' and the ideals in R which contain K.

Say $I' \subset R'$ and I' is an ideal and let

$$I = \{i \in R \mid f(i) \in I'\}.$$

Then we must have for $i_1, i_2 \in I$ that $f(i_1 + i_2) = f(i_1) + f(i_2)$. Also note that

$$f(ir) = f(i)f(r) \in I'$$

which implies that $ir \in I$ which implies that I is an ideal.

Theorem (Correspondence Theorem)
Let the mapping $\phi : R \to R'$ be a homomorphism of R onto R' with kernel K. If I' is an ideal of R', let $I = \{a \in R \mid \phi(a) \in I'\}$. Then I is an ideal of R, $I \supset K$, and $I/K \cong I'$. This sets up a $1-1$ correspondence between all the ideals of R' and those ideals of R that contain K.

Theorem (Second Homomorphism Theorem)
Let A be a subring of a ring R and I an ideal of R. Then $A + I = \{a + i \mid a \in A, i \in I\}$ is a subring of R, I is an ideal of $A + I$, and $(A + I)/I \cong A/(A \cap I)$.

Theorem (Third Homomorphism Theorem)
Let the mapping $\phi : R \to R'$ be a homomorphism of R onto R' with kernel K. If I' is an ideal of R' and $I = \{a \in R \mid \phi(a) \in I'\}$, then $R/I \cong R'/I'$. Equivalently, if K is an ideal of R and $I \supset K$ is an ideal of R, then $R/I \cong (R/K)/(I/K)$.

Problem (Section 4.3 #16)
Show that the ring of 2×2 matrices over the reals has nontrival left ideals (and also nontrivial right ideals).

Solution: Suppose that

$$T = \{\begin{pmatrix} 0 & r_1 \\ 0 & r_2 \end{pmatrix} \mid r_1, r_2 \in R\}.$$

Then we have that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & r_1 \\ 0 & r_2 \end{pmatrix} \in T.$$

Therefore for $s \in S$ and $t \in T$, we have that $st \in T$. Therefore we have that this is a nontrivial left ideal because there are additive inverses and T is also closed under matrix addition. Note that this is not a nontrival right ideal. $\square$

Problem (Section 4.3 #25)
Let R be the ring of 2×2 matrices over the real numbers; suppose that I is an ideal of R. Show that $I = (0)$ or $I = R$.

Say that I is an ideal in R such that $I \neq (0)$. If I has a matrix with nonzero determinant, then we are done because the matrix inverse is also in I which means that the identity is in I which implies that the entire ring will be in I. Therefore we will have that $I = R$.

Therefore it suffices to prove that there will be a matrix with nonzero determinant. Take $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in I$ with $b \neq 0$. Then we have that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in I$$

since I is an ideal. Then we must also have that

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & b \end{pmatrix} \in I$$

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} b & b \\ 0 & 0 \end{pmatrix} \in I.$$

The sum of these two matrices must also be in I which means that

$$\begin{pmatrix} b & 2b \\ 0 & b \end{pmatrix} \in I$$

and this matrix has nonzero determinant since $b \neq 0$. Therefore as stated before, we must have that $I = R$. □

Problem (Section 4.3 #26)
Let R be a ring with unit and let S be the ring of 2×2 matrices over R. If I is an ideal of S, show that there is an ideal J in R such that I consists of all the 2×2 matrices over J.

Solution: Suppose that I is an ideal in S. For any nonzero entry that appears in I, say i, create something like

$$\begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}.$$

Then we can see that

$$\begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & r \end{pmatrix} = \begin{pmatrix} 0 & ir \\ 0 & 0 \end{pmatrix}$$

which implies that ir is also an entry in I. This is the idea that we use to prove this problem. □

Problem (Section 4.3 #29)
Let R be a ring with 1. An element $a \in R$ is said to have a *left inverse* if $ba = 1$ for some $b \in R$. Show that if the left inverse b of a is unique, then $ab = 1$ (so b is also a right inverse of a).

Solution: We wish to prove that $ab - 1 = 0$. Note that

$$(ab-1)a = a(ba) - a = a(1) - a = 0.$$

We will add ba to both sides to get that

$$(ab-1)a + ba = ba = 1 \longrightarrow (ab + b - 1)a = 1.$$

Therefore by the uniqueness of b, we must have that

$$ab + b - 1 = b \longrightarrow ab - 1 = 0 \longrightarrow ab = 1$$

which is the desired result. □

§23 Maximal Ideals

Definition (Direct Sum)

Let R_1 and R_2 be rings. Then we say that $R_1 \oplus R_2$ is the *direct sum* of the two rings. We also have that

$$(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2')$$

$$(r_1, r_2)(r_1', r_2') = (r_1 r_1', r_2 r_2').$$

For R being any ring, let $a \in R$ be a fixed element. Consider (a), the subring generated by a. That is

$$(a) = \{ra \mid r \in R\}.$$

We have that (a) is a subring of R since $r_1 a + (-r_2 a) = (r_1 - r_2)a \in (a)$ and $r_1 a \cdot r_2 a = (r_1 a r_2)a \in (a)$ which shows that it is an abelian group under addition and is closed under multiplication. In fact, (a) is a left ideal in R. We only have that (a) is guaranteed to be a two-sided ideal of R if R is commutative.

Theorem

If R is commutative with 1 and if R has no proper ideals, then R is a field.

Proof: Take any $a \neq 0$ in such a ring R. Then we must have that $(a) = R$ since there are no proper ideals. Thus there exists $b \in R$ with $ba = 1$ which means that a will have a left inverse. Therefore since it is commutative, we have that R is a division ring which implies that it will be a field. □

Let $f : R \to R'$ be an onto ring homomorphism. Then ideals in R' correspond to ideals in R containing K, where K is the kernel (Correspondence Theorem). But what if R has no ideals properly containing K (other than R itself? Then R' has no proper ideals.

If R is a ring and M is a proper ideal in R, then we say that M is a *maximal ideal* in R if there is no ideal in R properly containing M aside from R itself.

Theorem

Say that R is a commutative ring with 1 and further suppose M is a maximal ideal in R. Then R/M is a field. The converse of this is also true. Suppose that R is a commutative ring with 1 containing an ideal I. If R/I is a field, then I is a maximal ideal in R.

Definition (Ring of Gaussian Integers)

Suppose that

$$H = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Then H is called the Ring of Gaussian Integers.

Suppose that $M \subset H$ and

$$M = \{a + bi \mid 3 \mid a, 3 \mid b\}.$$

Then M is an ideal of H. In fact, M is a maximal ideal in H.

Suppose that $c + di \in H$ and $c + di \notin M$. Suppose we "add" $c + di$ to M. Since $c + di \notin M$, either $3 \nmid c$ or $3 \nmid d$. Either way, that guarantees that $3 \nmid (c^2 + d^2)$. Since $c + di$ was added to M, we have that $c - di \in M$ as well. However $(c + di)(c - di) = c^2 + d^2$ and $(c + di)(c - di) \in M$ but $3 \nmid (c^2 + d^2)$. Thus the main ideal has 3 and $c^2 + d^2$ so by Euclid's, it will also have 1. Therefore this means that the main ideal is all of H. Therefore we have proven that M is a maximal ideal in H. Thus H/M is a field.

What are the additive cosets of M in H? These cosets are

$$M, M + 1, M + 2, M + i, M + (1 + i), M + (2 + i), M + 2i, M + (1 + 2i), M + (2 + 2i).$$

Thus H/M is a field with $3^2 = 9$ elements.

Question — Can we create a field with 5^2 elements in the same way?

Solution: We can say that

$$M' = \{a + bi \mid 5 \mid a, 5 \mid b\}.$$

We have that M' is an ideal by the same reasoning. But is M a maximal ideal? Consider $2 + i$. Then we have that

$$(2 + i)(2 - i) = 5.$$

Therefore the ideal generated by $2 + i$ will properly contain M' which means this ideal is not a maximal ideal. Therefore we cannot construct a field with 5^2 elements in the same way. □

Note that for integer n, we have that

$$n^2 \equiv 0, 1, 4 \pmod 5.$$

Consider the set

$$S = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

And suppose that $N \subset S$ such that

$$N = \{a + b\sqrt{2} \mid 5 \mid a, 5 \mid b\}.$$

Then N is an ideal in S. Is N a maximal ideal?

Suppose that $c + d\sqrt{2} \in S$ and $c + d\sqrt{2} \notin N$. If we add $c + d\sqrt{2}$ to N, then since $c - d\sqrt{2} \in S$ implies that $(c + d\sqrt{2})(c - d\sqrt{2}) = c - 2d^2 \in N$ also. Now since $5 \nmid c$ and $5 \nmid d$, then we have that $c^2 \equiv 1, 4 \pmod 5$ and $d^2 \equiv 1, 4 \pmod 5$. Checking the possibilities, we see that $5 \nmid (c^2 - 2d^2)$. Hence the new ideal has 5 and $c^2 - 2d^2$ so by Euclid's, the new ideal will have their gcd which means the new ideal has 1. Therefore the new ideal must be S itself which implies that N is a maximal ideal in S.

Therefore we have that S/N is a field with $5^2 = 25$ elements.

Definition (Quadratic Residues)

For n a positive integer, $k \in [0, n-1]$ is a quadratic residue of n if there exists $m \in \mathbb{Z}$ such that $m^2 \equiv k \pmod{n}$.

Theorem

For p being any odd prime, amongst the integers in $[1, p-1]$, exactly half, $\frac{p-1}{2}$, are quadratic residues.

Proof: This is because n and $p-n$ create the same quadratic residue. If k, j are in the same "half" of $[1, p-1]$, they can't create the same quadratic residue since

$$k^2 \equiv j^2 \pmod{p} \longrightarrow p \mid (k-j)(k+j)$$

which is not possible since $k \neq j$ and both are in the same "half". Thus there are exactly $\frac{p-1}{2}$ of the numbers in $[1, p-1]$ are quadratic residues. $\square$

What could we do for 7 since $a + b\sqrt{2}$ wouldn't work as $(3-\sqrt{2})(3+\sqrt{2}) = 7$. The problem is that 2 is a quadratic residue of 7. It worked for 5 because 2 is not a quadratic residue of 5.

Theorem

For p being any odd prime, consider

$$T = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$$

and $I \subset T$ where we have that

$$I = \{a + b\sqrt{m} \mid p \mid a, p \mid b\}.$$

If you pick m to be any non-quadratic residue of p, then I will be a maximal ideal in T. Thus T/I is a field with p^2 elements.

§24 Polynomial Rings

Definition

For any field F, $F[x]$ is the *ring of polynomials* over F under usual addition and multiplication of polynomials.

In $F[x]$, we have two polynomials $p(x)$ and $q(x)$ satisfy $p(x) = q(x)$ if and only if the coefficients of p are identical to the coefficients of q.

Definition

The degree of a polynomial is defined as the highest power of the polynomial that has a nonzero coefficient.

We have that $F[x]$ is an integral domain with unit because degree of product is the sum of the degrees of the polynomials that are being multiplied, i.e.

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)).$$

Theorem

In $F[x]$, we also have a division algorithm. Let $a(x), b(x)$ be nonzero polynomials. We can then write

$$a(x) = b(x)q(x) + r(x)$$

where $\deg(r(x)) < \deg(b(x))$.

Question — What are the ideals in $F[x]$?

Solution: Say that I is an ideal in $F[x]$ and suppose that $g(x) \in I$ where $I \neq (0)$ and $g(x) \neq 0$. Then every multiple of $g(x)$ is in I. Find one of the nonzero elements of lowest degree in I and call it $h(x)$. Then $I = (h(x))$ is forced.

Say that I contained $f(x)$ which is not divisible by $h(x)$. Then write $f(x) = h(x)q(x) + r(x)$ where $\deg(r(x)) < \deg(h(x))$. But note that $r(x) \neq 0$ because $h(x) \nmid f(x)$. However then $r(x) \in I$ but this is a contradiction since we had said $h(x)$ is the element of lowest degree. Therefore we must have that I is generated by $h(x)$, i.e. $I = (h(x))$. $\square$

Definition

A polynomial $a(x)$ is called *monic* if the leading coefficient is 1.

So every ideal in $F[x]$ is generated by a unique monic polynomial. $=$

Definition

An integral domain R is called a *principal ideal domain* if every ideal I in R is of the form $I = \{xa \mid x \in R\}$ for some $a \in I$.

Consider $\mathbb{Z}[x]$. Note that $\mathbb{Z}$ is not a field. We still have that $\mathbb{Z}[x]$ is an integral domain. Take the ideal generated by the two elements 2 and x. This creates all polynomials in $\mathbb{Z}[x]$ with an even constant term. This ideal is not generated by a single element.

Theorem

In $F[x]$, suppose that $p(x), q(x) \in F[x]$ where $p(x) \neq 0$ and $q(x) \neq 0$, we define

$$\gcd(p(x), q(x)) = a(x)$$

where $a(x)$ is a monic polynomial dividing both $p(x)$ and $q(x)$. If $b(x) \mid p(x)$ and $b(x) \mid q(x)$, then $b(x) \mid a(x)$. Just as in integers, we can write $a(x)$ as a linear combination of $p(x)$ and $q(x)$.

We say that $p(x)$ and $q(x)$ are *relatively prime* if $\gcd(p(x), q(x)) = 1$.

Definition

Suppose that $f(x) \in F[x]$. We say that $f(x)$ is *irreducible* if for any $g(x) \in F[x]$ we have either $\gcd(f(x), g(x)) = 1$ or $f(x) \mid g(x)$. This amounts to saying that $f(x)$ cannot be written as a product of two polynomials with lower degree than $f(x)$.

Theorem

In $F[x]$, the ideal $(f(x))$ is maximal, if and only if $f(x)$ is irreducible in $F[x]$.

Proof: Suppose that $f(x)$ is not irreducible and $f(x) = f_1(x)f_2(x)$ where $\deg(f_1), \deg(f_2) < \deg(f)$. Then $f_1(x)$ properly contains $(f(x))$. Since $\deg(f_1) \geq 1$, we have that $(f_1(x))$ is a proper ideal of $F[x]$. We have proven that if it is not irreducible then it cannot be maximal.

Now we will prove the other direction. Say that $f(x)$ is irreducible. Suppose we add $g(x)$ to the ideal $(f(x))$ where $g(x) \in F[x]$ and $g(x) \notin (f(x))$. Then $\gcd(f(x), g(x)) = 1$. But then $f(x), g(x)$ are both in this new ideal so their gcd, 1, must be as well since we can write their gcd as a linear combination of $f(x)$ and $g(x)$. Therefore this means that the new ideal is the entire $F[x]$. Therefore the ideal $(f(x))$ is a maximal ideal. $\square$

Definition

In a ring R, for any $a \neq 0$ in R, we wish to define $d(a)$ as the degree of a satisfying for all $a, b \neq 0$

1. $d(a) \in \mathbb{Z}^{\geq 0}$
2. $d(a) \leq d(ab)$
3. There exists $a, r \in R$ such that $b = qa + r$ where $d(r) < d(a)$ or $r = 0$.

A ring with these properties is a *Euclidean ring.*

Problem (Section 4.5 #14)

(a) Let $F = \mathbb{Z}_{11}$ which is the integers modulo 11. Show that $f(x) = x^2 + 1$ is irreducible in $F[x]$.

Solution: If this was reducible, then it would have a linear factor, meaning it would have a root in $\mathbb{Z}_{11}$. However checking $x \in [0, 10]$, none of these satisfy

$$x^2 + 1 \equiv 0 \pmod{11},$$

or in other words -1 is not a quadratic residue of 11. Therefore $f(x)$ must be irreducible in $\mathbb{Z}_{11}$. $\square$

Thus if $I = (x^2 + 1)$, the ideal generated by $x^2 + 1$, then I is a maximal ideal in $\mathbb{Z}_{11}[x]$. What is $\mathbb{Z}_{11}[x]/I$? It must be a field but how many elements does it have? What are the cosets of I in $\mathbb{Z}_{11}[x]$? The cosets of I in $\mathbb{Z}_{11}[x]$ are

$$\{I + (ax + b) \mid a, b \in [0, 10]\}.$$

This is because suppose that $I + (a_1x + b_1) = I + (a_2x + b_2)$. Then we have that $(a_1 - a_2)x + (b_1 - b_2) \in I$. Therefore we must have that $a_1 = a_2$ and $b_1 = b_2$ since we cannot have a polynomial that is less than degree 2 in I since I is generated by $x^2 + 1$. Therefore this proves that

$$\{I + (ax + b) \mid a, b \in [0, 10]\}$$

are the cosets since no two of these cosets can be equal to each other. Therefore we have 121 distinct cosets.

Now we must show that every coset is of the type

$$\{I + (ax + b) \mid a, b \in [0, 10]\}.$$

For any $I + g(x)$, consider $\frac{g(x)}{x^2+1}$. Then we have that

$$g(x) = q(x)(x^2 + 1) + r(x)$$

where $\deg(r(x)) < 2$ or $r(x) = 0$. Then $I + g(x) = I + r(x)$. Thus $\mathbb{Z}_{11}/I$ will be a field with $11^2 = 121$ elements.

Problem (Section 4.5 #14)
Let $F = \mathbb{Z}_{11}$ which is the integers modulo 11. Show that $f(x) = x^3 + x + 4$ is irreducible in $F[x]$.

We have that $h(x)$ is irreducible because again if it is reducible it would have a linear factor meaning it would have a root in $\mathbb{Z}_{11}$. By checking $[0, 10]$, you can see that it won't. Therefore $J = (x^3 + x + 4) = (h(x))$ is maximal in $\mathbb{Z}_{11}[x]$. $\square$

So what is $\mathbb{Z}_{11}[x]/J$? It would consist of the cosets of the form

$$\{J + (ax^2 + bx + c \mid a, b, c \in [0, 10]\}.$$

We have that $\mathbb{Z}_{11}[x]/J$ is a field since J is maximal and this field has $11^3 = 1331$ elements.

More generally, to create a field with p^n elements, find an nth degree irreducible polynomial in $\mathbb{Z}_p[x]$. Then $\mathbb{Z}_p[x]/I$ where I being the ideal generated by that irreducible polynomial will be a field with p^n elements.

Problem (Section 4.5 #20)
If R is a Euclidean ring, show that every ideal of R is principal.

Solution: Suppose that I is an ideal in R. Take $a \neq 0$ such that $a \in I$ with $d(a)$ as small as possible. Then $I = (a)$ is forced. If $b \in I$ and b is not a "multiple" of a, then write $b = qa + r$ with $r \neq 0$ because $a \nmid b$ but $r \in I$. Then we have found an element which has degree less than a which is a contradiction. Therefore we must have that $I = (a)$. $\square$

Problem (Section 4.5 #25)
If p is a prime, show that

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

is irreducible in $\mathbb{Q}$.

This is a difficult problem and we will attempt this question with the tools in the next section.

§25 Polynomials over the Rationals

Theorem
If R is any ring and I is an ideal of R, then $I[x]$, the polynomial ring in x over I, is an ideal of $R[x]$. Furthermore,

$$R[x]/I[x] \cong (R/I)[x],$$

where $(R/I)[x]$ is the polynomial ring in x over R/I.

Proof: Let $\overline{R} = R/I$; then there is a homomorphism $\phi : R \to \overline{R}$, defined by $\phi(a) = a + I$, whose kernel is I. Define $\Phi : R[x] \to \overline{R}[x]$ by: if

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$

then

$$\Phi(f(x)) = \phi(a_0)x^n + \phi(a_1)x^{n-1} + \cdots + \phi(a_n).$$

We can prove that Φ is a homomorphism of $R[x]$ onto $\overline{R}[x]$. We will omit the proof of this however.

Now what is $\text{Ker}(\Phi)$. If $f(x) = a_0x^n + \cdots + a_n$ is in $\text{Ker}(\Phi)$, then $\Phi(f(x)) = 0$, the 0 element of $\overline{R}[x]$. Since

$$\Phi(f(x)) = \phi(a_0)x^n + \phi(a_1)x^{n-1} + \cdots + \phi(a_n) = 0,$$

we conclude $\phi(a_0) = 0, \phi(a_1) = 0, \ldots, \phi(a_n) = 0$, by the very definition of what we mean by the 0-polynomial in a polynomial ring. Thus each a_i is in the kernel of ϕ, which happens to be I. Because $a_0, a_1, \ldots, a_n$ are in I,

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$

is in $I[x]$. So $\text{Ker}(\Phi) \subset I[x]$. The fact that $I[x] \subset \text{Ker}(\Phi)$ is immediate from the definition of the mapping Φ. Hence we have that $I[x] = \text{Ker}(\Phi)$. By the First Homomorphism Theorem for Rings, the ring $I[x]$ is then an ideal of $R[x]$ and

$$\overline{R}[x] \cong R[x]/\text{Ker}(\Phi) = R[x]/I[x]$$

which is the desired result since we defined $\overline{R}$ as R/I. $\square$

Theorem

In ring $\mathbb{Z}$, consider $I = (p)$ where p is a prime. Then we have $\mathbb{Z}[x]/I[x] \cong \mathbb{Z}_p[x]$. This is what the above theorem turns into when we let $R = \mathbb{Z}$ and $I = (p)$.

Theorem (Gauss's Lemma)

If $f(x) \in \mathbb{Z}[x]$ is primitive (greatest common divisor of its coefficients is 1), then if $f(x)$ is reducible in $\mathbb{Q}[x]$, then it is reducible in $\mathbb{Z}[x]$. In particular, if f is monic, then this is true (special case).

Proof: We will only do the proof for the monic case. Suppose that $f(x) \in \mathbb{Z}px]$ is monic and $f(x) = a(x)b(x)$ where $a(x), b(x) \in \mathbb{Q}[x]$, and $\deg(a(x)) = s, \deg(b(x)) = r$. We can express each of $a(x)$ and $b(x)$ as a product of a rational number and a polynomial with integer coefficients. More precisely,

$$a(x) = \frac{u_1}{m_1}(a_0'x^s + a_1'x^{s-1} + \cdots + a_s') = \frac{u_1}{m_1}a_1(x),$$

where $a_0', a_1', \ldots, a_s'$ are relatively prime integers and

$$b(x) = \frac{u_2}{m_2}(b_0'x^r + b_1'x^{r-1} + \cdots + b_r') = \frac{u_2}{m_2}b_1(x),$$

where $b_0', b_1', \ldots, b_r'$ are relatively prime. Thus

$$f(x) = a(x)b(x) = \frac{u_1u_2}{m_1m_2}a_1(x)b_1(x) = \frac{u}{w}a_1(x)b_1(x),$$

where v and w are relatively prime, by canceling out the common factor of u_1u_2 and m_1m_2. Therefore, $wf(x) = va_1(x)b_1(x)$, and $f(x), a_1(x), b_1(x)$ are all in $\mathbb{Z}[x]$. Of course, we may assume with no loss of generality

that the leading coefficients of $a_1(x)$ and $b_1(x)$ are positive.

If $w = 1$, then, since $f(x)$ is monic, we get that $va_0'b_0'1$ and this leads easily to $v = 1, a_0' = b_0' = 1$ and so $f(x) = a_1(x)b_1(x)$, where both $a_1(x)$ and $b_1(x)$ are monic polynomials with integer coefficients. This is precisely the claim of the theorem, since $\deg(a_1(x)) = \deg(a(x))$ and $\deg(b_1(x)) = \deg(b(x))$.

Suppose then that $w \neq 1$; thus there is a prime p such that $p \mid w$ and since $\gcd(v, w) = 1$, $p \nmid v$. Also, since the coefficients $a_0', a_1', \ldots, a_s'$ of $a_1(x)$ are relatively prime, there is an i such that $p \nmid a_i'$; similarly, there is a j such that $p \nmid b_j'$. Let $I = (p)$ be the ideal generated by p in $\mathbb{Z}$; then $\mathbb{Z}/I \cong \mathbb{Z}_p$ and by the theorem above, we have that

$$\mathbb{Z}[x]/I[x] \cong \mathbb{Z}_p[x]$$

so $\mathbb{Z}[x]/I[x]$ is an integral domain. However, since $p \mid w$, $\overline{w}$, the image of w in $\mathbb{Z}[x]/I[x]$, is 0, and since $p \nmid v$, $\overline{v}$, the image of v in $\mathbb{Z}[x]/I[x]$, is not 0. Thus

$$0\overline{f}(x) = \overline{va_1}(x)\overline{b_1}(x),$$

where $\overline{v} \neq 0$ and $\overline{a_1}(x) \neq 0, \overline{b_1}(x) \neq 0$ because $p \nmid a_i'$ and $p \nmid b_k'$ for the given i, j above. This contradicts the fact that $\mathbb{Z}[x]/I[x]$ is an integral domain. Therefore $w \neq 1$ is not possible and the theorem is proven. □

Theorem (Eisenstein Criterion)

Suppose that

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \in Z[x]$$

and $p \mid a_i$ for all $i \in [0, n-1]$ where p is some prime and $p^2 \nmid a_0$.Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: Suppose that $f(x)$ is a polynomial such that

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \in Z[x]$$

and $p \mid a_i$ for all $i \in [0, n-1]$ where p is some prime and $p^2 \nmid a_0$. Now suppose that $f(x) = u(x)v(x)$ where $\deg(u(x)), \deg(v(x)) < \deg(f(x))$. Now consider the ideal $I = (p)$ in $\mathbb{Z}$ and let $\phi : \mathbb{Z}[x]/I[x] \to \mathbb{Z}_p[x]$ be an isomorphism. What is $\phi(f(x))$? We have that $\phi(f(x)) = x^n$ and say that $\phi(u(x)) = u_1(x)$ and $\phi(v(x)) = v_1(x)$. Then we have that

$$x^n = u_1(x)v_1(x)$$

since ϕ is an isomorphism. Therefore we have that $u_1(x) = x^r$ and $v_1(x) = x^{n-r}$ for some $r \in [1, n-1]$. Therefore this implies that

$$u(x) = x^r + p \cdot g(x) \text{ and } v(x) = x^{n-r} + p \cdot h(x)$$

where $g(x)$ and $h(x)$ are polynomials. Therefore we have that

$$f(x) = u(x)v(x) = (x^r + pg(x))(x^{n-r} + ph(x)) = x^n + px^rh(x) + px^{n-r}g(x) + p^2g(x)h(x).$$

However in this expansion, only $p^2g(x)h(x)$ can have a constant term. This implies that p^2 divides the constant term which is a contradiction. Therefore $f(x)$ is irreducible and the proof is complete. □

Question — Prove that

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

is irreducible in $\mathbb{Q}[x]$.

Solution: Note that

$$f(x+1) = (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 = x^4 + 5x^3 + 10x^2 + 10x + 5.$$

This new polynomial $f(x+1)$ is irreducible by Eisenstein Criterion as the polynomial is monic, 5 divides every coefficient but the first, and $5^2 = 25$ doesn't divide the constant term. Therefore this proves that $f(x)$ is also irreducible in $\mathbb{Q}[x]$. $\square$

Problem (Section 4.6 #5)

If p is a prime, show that

$$g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

is irreducible in $\mathbb{Q}[x]$.

Solution: Note that

$$g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

which implies that

$$g(x+1) = \frac{(x+1)^p - 1}{x}$$

which is monic and the constant term is $\binom{p}{1} = p$. The other coefficients of this polynomial are of the form

$$\binom{p}{k}, 2 \leq k \leq p-1.$$

However since p is a prime, we know that $p \mid \binom{p}{k}$ for $2 \leq k \leq p-1$. Therefore since $g(x+1)$ is monic, p divides all the coefficients but the first coefficient, and p^2 doesn't divide the constant term, we must have that $g(x+1)$ is irreducible in $\mathbb{Q}[x]$. Therefore since $g(x+1)$ is irreducible in $\mathbb{Q}[x]$, we must have that $g(x)$ is also irreducible in $\mathbb{Q}[x]$ which is the desired result. $\square$

Problem (Section 4.6 #8)

Let F be a field and $b \neq 0$ be an element of F. Define the mapping $\phi : F[x] \to F[x]$ by $\phi(f(x)) = f(bx)$ for every $f(x) \in F[x]$. Prove that ϕ is an automorphism of $F[x]$ such that $\phi(a) = a$ for all $a \in F$.

Solution: Note that

$$\phi(f(x) + g(x)) = (f+g)(bx) = f(bx) + g(bx) = \phi(f(x)) + \phi(g(x))$$

so it satisfies the addition criterion. Similarly we have that

$$\phi(f(x)g(x)) = (f \cdot g)(bx) = f(bx) \cdot g(bx) = \phi(f(x)) \cdot \phi(g(x))$$

so it satisfies the multiplication criterion. Therefore we have that ϕ is a homomorphism. Also note that

$$\phi(f(x)) = \phi(g(x)) \longrightarrow f(bx) = g(bx) \text{ for all } x.$$

Using $x = b^{-1}y$ gives us that $f(y) = g(y)$ for all y which proves injectivity. Since we have that

$$\phi(f(b^{-1}x)) = f(x),$$

we have that ϕ is onto as well. Therefore since ϕ is a bijective homomorphism which maps $F[x]$ to itself, we have that ϕ is an automorphism of $F[x]$ where $\phi(a) = a$ because a constant maps to itself. $\square$

Problem (Section 4.6 #14)
Let $\mathbb{C}$ be the field of complex numbers. Given an integer $n > 0$, find an automorphism ϕ of $\mathbb{C}[x]$ of order n.

Solution: For $b \neq 0$ in $\mathbb{C}$,

$$\phi(f(x)) = f(bx)$$

is an automorphism on $\mathbb{C}[x]$. Then we have that

$$\phi^n(f(x)) = f(b^n x)$$

but we wish for the nth power of ϕ to be $f(x)$ (the identity) since the automorphism must have order n. If $b^n x = x$ for all x, then it would work. Take b to be a primitive nth root of unity. Then we have that $\phi^n =$ identity mapping and no other $k < n$ will satisfy $\phi^k =$ identity mapping since b is a primitive nth root of unity. Therefore this automorphism satisfies the conditions of the problem. □

§26 Field of Quotients of an Integral Domain

The idea is if you have an integral domain, extend this to a field by "adding" in multiplicative unit and multiplicative inverses.

Definition
Suppose that D is an integral domain. Take any $a, b \in D$ with $b \neq 0$. We want to define a new element $\frac{a}{b}$. We have that

$$\frac{a}{b} = \frac{c}{d}, b \neq 0, d \neq 0$$

if and only if $ad = bc$.

We will use equivalence classes to denote the field. Therefore if $a, b \in D$ with $b \neq 0, d \neq 0$ then

$$(a, b) \sim (c, d)$$

if and only if $ad = bc$.

The elements of the field will consist of these equivalence classes. The operations on this field are

$$[a, b] + [c, d] = [ad + bc, bd]$$

$$[a, b] \cdot [c, d] = [ac, bd]$$

where $b \neq 0, d \neq 0$ and note that $bd \neq 0$ since there are no zero divisors since D is a domain.

Question — If $[a, b] \sim [a', b']$ and $[c, d] \sim [c', d']$, can we be sure that $[ad + bc, bd] \sim [a'd' + b'c', b'd']$?

Solution: Therefore this is equivalent to showing that

$$(ad + bc)b'd' = (a'd' + b'c')bd.$$

We have that

$$(ad + bc)b'd' = (a'd' + b'c')bd \longrightarrow ab'dd' + bb'cd' = a'bdd' + bb'c'd$$

but the first term on the LHS is equal to the first term on the RHS and the second term on the LHS is equal to the second term on the RHS since $[a, b] \sim [a', b']$ and $[c, d] \sim [c', d']$. Therefore we have that $[ad + bc, bd] \sim [a'd' + b'c', b'd']$ so the addition is well defined. Similarly we can show that if $[a, b] \sim [a', b']$ and $[c, d] \sim [c', d']$, then $[ac, bd] \sim [a'c', b'd']$ so the multiplication is also well defined. □

Definition

Note that we have

$$[a,b]+[0,d]=[ad,bd]=[a,b]$$

which proves that $[0,d]$ is the additive identity for any $d\neq 0$. We also have that

$$[a,b]+[-a,b]=[0,b^2]=\text{ additive identity}$$

which implies that $[-a,b]$ is the additive inverse of $[a,b]$.

Therefore this is an abelian group under addition. For multiplication, it is fairly obvious that it is closed under addition and it is not too difficult to show that it is associative as well.

Definition

Note that

$$[a,b][c,c]=[ac,bc]=[a,b]$$

so $[c,c]$ is the multiplicative identity for all $c\neq 0$. Also note that

$$[a,b][b,a]=[ab,ab]=\text{ multiplicative identity}$$

which implies that $[b,a]$ is the multiplicative inverse of $[a,b]$.

Also note that

$$[a,b]([c,d]+[e,f])=[a,b][cf+de,df]=[a(cf+de),bdf]$$
$$[a,b][c,d]+[a,b][e,f]=[ac,bd]+[ae,bf]=[acbf+bdae,b^2df]=[acf+dae,bdf]$$

which implies that

$$[a,b]([c,d]+[e,f])=[a,b][c,d]+[a,b][e,f]$$

so the distributive laws hold. Therefore we must have that this is a field and this is called the field of quotients.

§27 Fields (Chapter 5)

Recall a field F has two operations, $+$ and $\cdot$. We have that F is an abelian group under $+$. We also have that the nonzero elements of F are an abelian group under $\cdot$. And lastly, we have that the distributive laws are satisfied in F.

Example

Some examples of fields are $\mathbb{Q}$ (the field of rationals), $\mathbb{R}$ (the field of reals), $\mathbb{C}$ (the field of complex numbers) all under normal addition and multiplication.

The simplest example of a finite field is $\mathbb{Z}_p$ where p is any prime.

Theorem (Creating Fields)

1. Let R be a commutative ring with unit. Then if M is a maximal ideal in R, we have that R/M is a field.

A major use of this is in $\mathbb{Z}_p[x]$ we take an irreducible polynomial $f(x)$ of degree n. Then if $I=(f(x))$, then

we have that

$$\mathbb{Z}_p[x]/I$$

is a field with p^n elements.

2. If D is an integral domain, then we can use the field of quotients.

Suppose that $K \subset \mathbb{R}$. Consider the set

$$K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

It is not difficult to verify that K is a field and we have that $\mathbb{Q} \subset K \subset \mathbb{R}$. In essence, we can think of just "adding" $\sqrt{2}$ to $\mathbb{Q}$.

Note that by "adding" i to $\mathbb{R}$, we create $\mathbb{C}$. We add in i to $\mathbb{R}$ so the equation $x^2 + 1$ has roots in this new field. Adding in $\sqrt{2}$ to $\mathbb{Q}$ so the equation $x^2 - 2 = 0$ has roots is quite similar. This is simpler than moving from $\mathbb{Q}$ to $\mathbb{R}$; we can just move from $\mathbb{Q}$ to K.

Say that we add both $\sqrt{2}$ and $\sqrt{3}$ to $\mathbb{Q}$. Does this represent the set

$$L = \{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}\}?$$

Unfortunately this is not true. For example, L won't contain the element $\sqrt{6}$.

Question — Can we add one element to $\mathbb{Q}$ that will create the same field as adding both $\sqrt{2}$ and $\sqrt{3}$?

Solution: Yes we can. What we can do is add $\sqrt{3} + \sqrt{2}$ to $\mathbb{Q}$. This element is definitely in the field created by adding both $\sqrt{2}$ and $\sqrt{3}$ to $\mathbb{Q}$.

Also note that

$$(3 + \sqrt{2})^{-1} = \frac{1}{\sqrt{3} + \sqrt{2}} = \sqrt{3} - \sqrt{2}.$$

Therefore if we add $\sqrt{3} + \sqrt{2}$ to $\mathbb{Q}$, we are also adding $\sqrt{3} - \sqrt{2}$ to $\mathbb{Q}$. Therefore the sum and differences of $\sqrt{3} - \sqrt{2}$ and $\sqrt{3} + \sqrt{2}$ will also be in $\mathbb{Q}$ which implies that $\sqrt{2}$ and $\sqrt{3}$ will also be there. □

Question — What if we wish to add one element to $\mathbb{Q}$ that will create the same field as adding both $\sqrt{2}$ and $\sqrt[3]{3}$? What about with $\sqrt{2}$ and π?

Solution: This is a rather difficult question and this is the question that we will pondering throughout this chapter. □

An important part of any field is its *characteristic*. That is, the smallest positive integer n such that $na = 0$ for all $a \in F$. If no such n exists, we say that F has characteristic zero.

Finite fields always have nonzero characteristic. In fact any field with nonzero characteristic has characteristic p where p is some prime. In fact, this works for integral domains also.

We have that $\mathbb{Z}_p[x]$ is an integral domain with characteristic p. Its field of quotients will also have characteristic p since we have that

$$p[a, b] = [pa, b] = [0, b] = \text{ zero element.}$$

Problem (Section 5.1 #7)
If F is a field with characteristic p where p is a prime, show that $(a+b)^p = a^p + b^p$ for all $a, b \in F$.

Solution: By the binomial theorem, we have that

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Note that for $k \neq 0$ and prime p, we have that $p \mid \binom{p}{k}$. Therefore we have that

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = \binom{p}{0} a^0 b^{p-0} + \binom{p}{p} a^p b^{p-p} = a^p + b^p$$

which is the desired result. □

§28 Vector Spaces

Definition
A vector space V over a field F is an abelian group under addition such that for every $\alpha \in F$ and every $v \in V$, there is an element $\alpha v \in V$ such that:

1. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$ for $\alpha \in F$, $v_1, v_2 \in V$.
2. $(\alpha + \beta)v = \alpha v + \beta v$ for $\alpha, \beta \in F$, $v \in V$.
3. $\alpha(\beta v) = (\alpha\beta)v$ for $\alpha, \beta \in F$, $v \in V$.
4. $1v = v$ for all $v \in V$, where 1 is the unit element of F.

Example
Let $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Can we think of K as a vector space over $\mathbb{Q}$? Yes this is a vector space over $\mathbb{Q}$ as it satisfies all the properties of a vector space.

Example
Most common type of vector space is some space multiplied by itself. For example $\mathbb{R}^3$ as a vector space over $\mathbb{R}$. What we mean by $\mathbb{R}^3$ is

$$\mathbb{R}^3 = (r_1, r_2, r_3) \text{ where } r_1, r_2, r_3 \in \mathbb{R}.$$

Example
Another example is $F[x]$ is a vector space over F.

Definition

For a vector space V and $W \subset V$, W is a *subspace* if W is a vector space on its own. That is, W is an abelian group under addition and is closed under scalar multiplication.

Question — In a vector space is 0 times anything equal to 0? Do you mean 0 in a field or 0 in a vector space?

Solution: Say that 0 is the 0 vector. Then we have for $\alpha \in F$ that

$$\alpha \cdot 0 = \alpha(0+0) = \alpha \cdot 0 + \alpha \cdot 0 \longrightarrow \alpha \cdot 0 = 0.$$

Now say that 0 is 0 in the field. Then for $v \in V$, we have that

$$0 \cdot v = (0+0)v = 0v + 0v \longrightarrow 0v = 0.$$

Therefore we have that 0 times anything equals 0. □

Question — If $\alpha v = 0$, does that force $\alpha = 0$ or $v = 0$?

Solution: Yes this is forced. Suppose that $\alpha \neq 0$. Then α^{-1} does exist. Therefore we have that

$$\alpha^{-1}(\alpha v) = \alpha^{-1} \cdot 0 \longrightarrow (\alpha^{-1}\alpha)v = 0 \longrightarrow v = 0. \square$$

Say we have a collection of r linear equations over V with all the equations equal to 0 with coefficients from F and variables from V. Let these equations be

$$\alpha_{11}v_1 + \alpha_{12}v_2 + \cdots + \alpha_{1r}v_n = 0$$

$$\alpha_{21}v_1 + \alpha_{22}v_2 + \cdots + \alpha_{2r}v_n = 0$$

$$\cdots$$

$$\alpha_{r1}v_1 + \alpha_{r2}v_2 + \cdots + \alpha_{rr}v_n = 0$$

where the α_{ij}'s $\in F$ and v_i's $\in V$ and in each of the equations at least one of the $\alpha_{ij} \neq 0$.

Suppose we take the case of two equations and two unknowns

$$\alpha_{11}v_1 + \alpha_{12}v_2 = 0$$

$$\alpha_{21}v_1 + \alpha_{21}v_2 = 0.$$

Is there a solution to this system where $v_1 \neq 0$ and $v_2 \neq 0$?

Theorem

If $n = r$, then it depends on consistency (may or may not have a nontrivial solution). However if $n > r$, then a nontrivial solution is guaranteed.

Proof: Consider the case when $n = 2$ and $r = 1$ and

$$\alpha_{11}v_1 + \alpha_{12}v_2 = 0$$

where $\alpha_{11} \neq 0$ and $\alpha_{12} \neq 0$.

Choose $v_1 \neq 0$. Then $v_2 = \alpha_{12}^{-1} \cdot \alpha_{11}v_1$ is a nontrivial solution.

Now take $n = 3$ and $r = 2$ and

$$\alpha_{11}v_1 + \alpha_{12}v_2 + \alpha_{13}v_3 = 0$$
$$\alpha_{21}v_1 + \alpha_{22}v_2 + \alpha 23v_3 = 0.$$

Say that $\alpha_{11} \neq 0$ and $\alpha_{21} \neq 0$. Then multiply the first equation by α_{21} and the second equation by α_{11} and subtract the two equations. Then we get that

$$(\alpha_{12}\alpha_{21} - \alpha_{11}\alpha_{22})v_2 + (\alpha_{13}\alpha_{21} - \alpha_{23}\alpha_{11})v_3 = 0.$$

Now we know that this will have a nontrivial solution as we had shown there is a nontrivial solution when $n = 2$ and $r = 1$. Therefore we see that there is a nontrivial solution for the case $n = 3$ and $r = 2$.

Therefore we can use induction to see that if $n > r$, then there will always be a nontrivial solution. □

Definition (Linear Combination of Vectors)

Say you have $v_1, v_2, \ldots, v_n \in V$. Then anything of the form

$$\alpha_1v_1 + \alpha_2v_2 + \cdots + \alpha_nv_n$$

is a *linear combination* of these vectors.

In any vector space V, we wonder what is the minimum number of vectors needed so that these linear combinations create the whole space (i.e. they span the space).

In $\mathbb{R}^3$ using the vectors $(1, 0, 0)$ and $(0, 1, 0)$, these vectors do not span the whole space as taking any linear combination of these vectors results in the last coordinate always being 0.

Question — In $\mathbb{R}^4$, how many vectors are needed to span the space?

Solution: Using the 4 vectors $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$, and $(0, 0, 0, 1)$, we claim that we can span the whole space. This is true because for $(r_1, r_2, r_3, r_4) \in \mathbb{R}^4$, we have that

$$(r_1, r_2, r_3, r_4) = r_1(1, 0, 0, 0) + r_2(0, 1, 0, 0) + r_3(0, 0, 1, 0) + r_4(0, 0, 0, 1).$$

Therefore these 4 vectors span the entire space. Now the question becomes, how do we know whether we can span the entire space with 3 vectors? □

Example

Recall that if $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, then K is a field such that $\mathbb{Q} \subset K \subset \mathbb{R}$. Now think of K as a vector space over $\mathbb{Q}$. Then the set $\{1, \sqrt{2}\}$ are the two vectors which span K.

Now think of $\mathbb{R}$ as a vector space over $\mathbb{Q}$. How many vectors are needed to span the space?

Definition

We say that a vector space V over F is *finite dimensional* if finitely many vectors in V generate all of V via linear combinations.

Definition

For V a finite dimensional vector space over F, the *degree* of V over F is the cardinality of the minimal generating set.

Definition

A collection of vectors $\{v_1, v_2, \ldots, v_n\}$ is *linearly independent* if

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

implies that $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Definition

In a minimal generating set, the vectors must be linearly independent. Such a set is called a *basis* for the vector space. It turns out that any two bases have the same number of vectors.

Say that $\{w_1, w_2, \ldots, w_7\}$ and $\{v_1, v_2, \ldots, v_5\}$ are both bases for v. Then we must have that

$$w_1 = \alpha_{11} v_1 + \cdots + \alpha_{15} v_5$$

$$w_2 = \alpha_{21} v_1 + \ldots \alpha_{25} v_5$$

$$\cdots$$

$$w_7 = \alpha_{71} v_1 + \cdots + \alpha_{75} v_5.$$

Now consider the equation

$$\beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_7 w_7 = 0.$$

Now think of doing this with the v_i's. Then we have 7 variables and 5 equations so we will have a nontrivial solution.

Problem (Section 5.2 #6)

If V is a finite-dimensional vector space over F and if W is a subspace of V, prove that:
(a) W is finite dimensional over F and $\dim_F(W) \leq \dim_F(V)$.
(b) If $\dim_F(W) = \dim_F(V)$, then $V = W$.

Solution: (a) Suppose that $w_1, w_2, \ldots, w_n$ generate W. This is linearly independent. Thus in V, it is also linearly independent. Thus $\{w_1, w_2, \ldots, w_n\}$ is linearly independent in V which implies that $\dim_F(V) \geq n$.

(b) Suppose that $\{w_1, w_2, \ldots, w_n\}$ is a basis for W. Then since $\dim_F(V) = n$, you cannot have greater than n linearly independent vectors in V. Hence this must be a basis for V also. If not, then add any v' not spanned by these and you have greater than n linearly independent vectors in V. Therefore if $\dim_F(W) = \dim_F(V)$, we must have that $V = W$. $\square$

§29 Field Extensions

Definition

Say F, K are fields with $F \subset K$ (also have the same operations). We call F a *subfield* of K. Also we can refer to K as an *extension field* of F.

Definition

We can also think of K as a vector space over F. When $\dim_F(K)$ is finite, we say K is a *finite extension* of F, otherwise we say K is an infinite extension. When finite, we write $\dim_F(K)$ as $[K : F]$.

Theorem

Let $L \supset K \supset F$ be three fields such that both $[L : K]$ and $[K : F]$ are finite. Then L is a finite extension of F and $[L : F] = [L : K][K : F]$.

Theorem

Suppose that $[K : F] = n$. Then every element of K is a root of a nonzero polynomial in $F[x]$ with degree less than or equal to n.

Proof: Suppose that this polynomial is $\alpha_0 + \alpha_1 u + \cdots + \alpha_n u^n = 0$. Since $[K : F] = \dim_F(K) = n$ and consider the $n + 1$ vectors

$$1, u, u^2, \ldots, u^n$$

in K. Then they must be linearly dependent over F. Thus we can find $\alpha_0, \alpha_1, \ldots, \alpha_n$ in F, not all 0, such that $\alpha_0+\alpha_1 u+\cdots+\alpha_n u^n = 0$. Thus u is a rot of a nonzero polynomial with degree less than or equal to n in F. □

For $F \subset K$ with F, K being fields, an element $\alpha \in K$ is *algebraic* over F if α is the root of some nonzero polynomial in F. A field extension $F \to K$ is *algebraic* if every element of K is algebraic over F. □

Theorem

Every finite extension is algebraic but the converse is not necessarily true.

Proof: If $[K : F] = n$, then for all $\alpha \in K$, we have that α is a root of a nonzero polynomial with degree less than or equal to n over F. Then we have that α is algebraic over F. Since α was arbitrary, K is an algebraic extension.

Now we will prove that the converse is not true. Consider $\mathbb{Q}$ extended by all $2^{\frac{1}{n}}$ for all $n \in \mathbb{N}$ and call this K. Say that $[K : \mathbb{Q}]$ is finite and say that it is 100 perhaps. Then consider $2^{\frac{1}{101}}$. That is a root of $x^{101} - 2 = 0$ but since $[K : \mathbb{Q}] = 100$, we would need $2^{\frac{1}{101}}$ to be the root of a polynomial with degree less than or equal to 100. However this won't work as we know that $x^{101} - 2$ is irreducible in $\mathbb{Q}$ by Eisenstein Criterion. Therefore this is a contradiction and proves that the converse is not true. □

If you extend a field (say $\mathbb{Q}$) by a single element, that does not necessarily mean its a finite extension.

When we extend $\mathbb{Q}$ by $\sqrt{2}$ and $\sqrt{3}$, that is the same as extending by $\sqrt{3} + \sqrt{2}$. We had shown this previously. This is just one example why the number of elements you extend by doesn't mean much.

Definition

For F a field, if we extend F by a single element b, that is denoted by $F(b)$ and is called a *simple extension*.

Example

For example, a simple extension would be

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

A simple extension ($F(b)$) can actually be an infinite extension if the element if the element b is not algebraic over F.

Definition

If b is not algebraic over F, it is called *transcendental*.

Example

As it turns out, most real numbers are transcendental over the rationals. For example, π and e are transcendental. Some other examples of transcendental numbers are 0.01001000100001... and $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$.

Theorem

Say F is extended by b where b is algebraic over F. The *degree* of this extension, that is $[F(b) : F]$, is equal to the degree n of the smallest nonzero polynomial in F (minimal polynomial) having b as a root.

Proof: If n is the lowest degree nonzero polynomial in F, then $[F(b) : F] = n$. Now why is this true?

First off, note that

$$\{1, b, b^2, \ldots, b^{n-1}\}$$

has to be linearly independent. Say that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ has b as a root with $a_n \neq 0$. Then we must have that

$$\{1, b, b^2, \ldots, b^{n-1}\}$$

is linearly dependent. Say that we took

$$\{1, b, b^2, \ldots, b^{n-1}, b^{n+1}\}.$$

Then we have that

$$a_n b^{n+1} + a_{n-1}b^n + \cdots + a_1 b^2 + a_0 b = 0$$

and we also have that

$$a_n b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

which means that $\{1, b, b^2, \ldots, b^{n-1}, b^{n+1}\}$ is linearly dependent. Therefore if we add another element to the set $\{1, b, b^2, \ldots, b^{n-1}\}$, it becomes linearly dependent. $\square$

Definition

If $f(x)$ is the lowest degree nonzero polynomial in $F[x]$ having b as a root, then $f(x)$ is irreducible in $F[x]$.

Problem (Section 5.3 #5)

Prove that if p is a prime number and if $a = \text{cis}(\frac{2\pi}{p})$, then $[\mathbb{Q}(a) : \mathbb{Q}] = p - 1$.

Solution: Note that a is a root of the polynomial $x^p - 1$. Also note that

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

Therefore we have that a is a root of

$$g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

which implies that $[\mathbb{Q}(a) : Q] \leq p - 1$ is assured. However we know that $g(x)$ is irreducible over $\mathbb{Q}$ which implies that $[\mathbb{Q}(a) : \mathbb{Q}] = p - 1$. $\square$

§30 Finite Extensions

Theorem

Say that K is an extension field of F. Let $E(K) \subset K$ denote the subset of K consisting of the elements which are algebraic over F. It turns out that $E(K)$ is always a subfield of K.

Proof: Say that $a, b \in E(K)$. Then a, b are algebraic over F. Thus we must have that $[F(a) : F]$ and $[F(b) : F]$ are both finite. What about if $[F(a, b) : F]$? Note that we have

$$[F(a, b) : F] \leq [F(a) : F][F(b) : F].$$

Extend F by a and suppose this has degree m. But in $F(a)$, still b has minimal polynomial of degree $\leq m$. Therefore if we extend $F(a)$ by b, still b has minimal polynomial of degree n. Therefore we have that

$$[F(a, b) : F] \leq mn.$$

Hence if $a, b \in E(K)$, it is assured that $a + b, ab \in E(K)$ since both $a + b, ab \in F(a, b)$. Thus this proves that $E(K)$ is a subfield (additive inverses can be shown easily). $\square$

Problem (Section 5.4 #4)

If $K \supset F$ is such that $[K : F] = p$ where p is a prime, show that $K = F(a)$ for every a in K that is not F.

Solution: For any such a, what is $[F(a) : F]$? It cannot be 1 since $a \notin F$. We also have that

$$[K : F][K : F(a)][F(a) : F] = p$$

since we are given that $[K : F] = p$ for some prime p. We must have that $[F(a) : F] = p$ since $[F(a) : F] \neq 1$ and $[F(a) : F]$ must divide p. Therefore since $[F(a) : F] = p$ and $[K : F] = p$, we must have that $F(a) = K$. $\square$

§31 Constructability

Say that you have a straight line segment of length 1. Using a straightedge and a compass, what other lengths of line segments can be created?

Definition (Constructible Numbers)

A real number r is *constructible* if $|r|$ can be created as a length of a line segment from segment of length 1 using a straightedge and compass.

The set of constructible numbers is a subfield of $\mathbb{R}$.

Question — Note that any integer is constructible which implies that any rational number is also constructible. Note that $\sqrt{2}$ and $\sqrt{3}$ are also constructible using triangles. But what about the numbers $\sqrt[3]{2}$ and π? Are they constructible?

Theorem

If b is constructible, then $[\mathbb{Q}(b) : \mathbb{Q}]$ must be a power of 2.

Thus we can see that $\sqrt[3]{2}$ is not constructible since we have that the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ which implies that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Similarly, $\mathbb{Q}(\pi)$ is an infinite extension of $\mathbb{Q}$ so π is not constructible. In fact, any transcendental number is not transcendental.

Theorem

The subset of constructible numbers is a subfield of the algebraic numbers, that is $E(\mathbb{R})$.

We also have another result. We are not able to trisect a $60°$ angle because $\cos(20°)$ is not constructible.

§32 Roots of Polynomials

Suppose that F is a field (characteristic zero probably). Say that $f(x) \in F[x]$ has a root b which is not in F. A simple example is $x^2 - 2 \in \mathbb{Q}[x]$.

So when thinking of $f(x)$ in F, it might not be easier to think of $f(x)$ in the field $F(b)$ because then $x - b$ might be a factor of $f(x)$.

Theorem

In a field F of characteristic 0, if $f(x)$ is of degree n, $f(n)$ has at most n roots in F or any extension field of F.

Proof: Note that if $f(x)$ is of degree 1, say $f(x) = ax + b$ with $a \neq 0$, then $x = -a^{-1}b$ is the only root. Now suppose that $f(x)$ is of degree n and say that b is a root of $f(x)$. In the field $F(b)$, write $f(x) = (x - b)g(x)$ where $g(x)$ has degree $n - 1$. So by induction, an nth degree equation has at most n roots. □

With $f(x) \in F[x]$, if possible, we would like to factor $f(x)$ into linear factors.

Say $g(x) \in \mathbb{Q}[x]$. Then g might not be factorable into linear factors in $\mathbb{Q}$. However, if we consider $g(x) \in \mathbb{C}[x]$, then g can be factorable into linear factors.

Example

Take $x^2 + 1 \in \mathbb{Q}[x]$ and we wish to factor this into linear factors. We can go to $\mathbb{C}[x]$ but is that the easiest way? Consider $\mathbb{Q}(i)$. This would be a lot easier than moving to $\mathbb{C}[x]$.

Definition

Say that $f(x) \in F[x]$ has n roots, $r_1, r_2, \ldots, r_n$, each of which may or may not be in F. What extension field contains all the roots? The easiest extension field is $K = F(r_1, r_2, \ldots, r_n)$ and we obtain this by extending F by each root of f. K is the smallest field containing all roots of $f(x)$, that is the smallest field in which $f(x)$ can be factored into linear factors. K is called the *splitting field* of $f(x)$ in F.

Now if K is the splitting field of $f(x)$ in F, then what is $[K : F]$? This is a fairly difficult question to answer. One result that we have though is that if $f(x)$ has degree n, then $[K : F] \leq n!$. Why is this? Say that we look at $[F(r_1) : F]$. Since r_1 is the root of an nth degree polynomial in $F[x]$, we must have that $[F(r_1) : F] \leq n$. Then in $F(r_1)$, write $f(x) = (x - r_1)g(x)$. Now r_2 is a root of $g(x)$ which has degree $n - 1$ in $F(r_1)$. Then we must have that $[F(r_1, r_2) : F(r_1)] \leq n - 1$. So inductively extending by one root at a time, we have that

$$[F(r_1, r_2, \ldots, r_n) : F] \leq n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1 = n!.$$

Say that $f(x) \in F[x]$ is irreducible of degree > 1. Now suppose that $M = (f(x))$ and note that M is a maximal ideal in $F[x]$ since $f(x)$ is irreducible in $F[x]$. Then we must have that $F[x]/M$ is a field. Now consider the mapping $\psi : F[x] \to F[x]/M$ defined by $\psi(g(x)) = g(x) + M$. Then ψ is $1 - 1$ on F (that is, the constant polynomials). Thus $\psi(F)$ is a copy of F in $F[x]/M$. In this way, $F[x]/M$ is an extension field of F. Note that $\psi(x) = x + M$ and $\psi(x^2) = \psi(x)\psi(x) = (x + M)^2$. Similarly, we have that $\psi(x^n) = (x + M)^n$. From that, we have that $\psi(h(x)) = h(x + M)$ for some polynomial $h(x)$. That being so, we have that

$$\psi(f(x)) = f(x) + M = M = 0$$

where 0 is the additive identity. We also have that

$$\psi(f(x)) = f(x + M)$$

and putting these together, we have that $f(x + M) = 0$. Hence $x + M$ is a "root" of $f(x)$ in this extension field. Thus we have found an extension field which has a new root for $f(x)$. So $F[x]/M$ has a new root for $f(x)$ and has degree $\leq n$ over F, using the natural basis $\{1, x, x^2, \ldots, x^{n-1}\}$.

Question — Prove that, for any prime p, we have that

$$(p-1)! \equiv -1 \pmod{p}.$$

Solution: Say that G is a finite field with $q = p^n$ elements. In this field, we have that $x^{q-1} - 1 = 0$ for all $x \neq 0$ in G. Thus $x^q - x$ has q distinct linear factors. Therefore when $q = p$ ($\mathbb{Z}_p$ field), we have that

$$x^{p-1} - 1 = (x-1)(x-2)\ldots(x-(p-1))$$

in $\mathbb{Z}_p$. Therefore if we compare the constant terms, we have that in $\mathbb{Z}_p$,

$$-1 = (-1)(-2)\ldots(-(p-1)),$$

so if p is odd, then we have that in $\mathbb{Z}_p$,

$$(p-1)! = -1$$

which implies that $(p-1)! \equiv -1 \pmod{p}$. $\square$

Problem (Section 5.6 #4)
If $q(x) = x^n + a_1x^{n-1} + \cdots + a_n$, $a_n \neq 0$, is a polynomial with integer coefficients and if the rational number r is a root of $q(x)$, prove that r is an integer and $r \mid a_n$.

Solution: Say that $r = \frac{l}{m}$ is a rational root with $\gcd(l, m) = 1$ and $l, m \in \mathbb{Z}$. Then we must have that

$$\frac{l^n}{m^n} + a_1\frac{l^{n-1}}{m^{n-1}} + \cdots + a_{n-1}\frac{l}{m} + a_n = 0.$$

Now suppose that we multiply by m^n. Then we have that

$$-l^n = a_1ml^{n-1} + \cdots + a_{n-1}m^{n-1}l + a_nm^n.$$

The right hand side is divisible by m since each term is divisible by m on the right hand side. Thus we need $m \mid l^n$. However since $\gcd(l, m) = 1$, that is only possible if $m = \pm 1$. Thus $r = \frac{l}{m} = \pm l$ which is an integer.

Now we will prove that $r \mid a_n$. Suppose that $r = l \in \mathbb{Z}$ is a root of $q(x)$. Then we have that

$$l^n + a_1l^{n-1} + \cdots + a_{n-1}l + a_n = 0.$$

Then rearranging, we have that

$$l^n + a_1l^{n-1} + \cdots + a_{n-1}l = -a_n$$

and since each term on the left hand side is divisible by l, the left hand side must be divisible by l. Thus $l \mid a_n$ as well, which is the desired result. $\square$