MAT 3004 - Abstract Algebra I

Daniel Wong

Contents

Chapter 1

Preliminaries

In this Chapter, we will recall some knowledge which will be assumed throughout the course.

1.1 Divisibility of Integers

We begin our studies on the integers $\mathbb{Z}$. Let $t, s \in \mathbb{Z}$ with $t \neq 0$. We write $t \mid s$ if and only if

$$\exists\, u \in \mathbb{Z} \text{ , such that } s = tu.$$

If u does not exist, write $t \nmid s$.

Remark 1.1. Every integer divides 0 whereas 0 is a divisor of only 0.

Theorem 1.2 (Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q, r such that $a = bq + r$, where $0 \leq r < b$.*

Proof. (Existence) Let $a, b \in \mathbb{Z}$ with $b > 0$ Consider the set:

$$S = \{a - bk \mid k \in \mathbb{Z},\ a - bk \geq 0\}.$$

We first show that S is nonempty:
If $a \geq 0$, then $a = a - b \cdot 0 \in S$.
If $a < 0$, since $b > 0$, we may choose $k = 2a$, then we can get: $a - b(2a) = a(1 - 2b) \in S$.

By the well-ordering property of $\mathbb{Z}_{\geq 0}$, the set S has the has a minimal element r.
By the definition of S, there exists $q \in \mathbb{Z}$ such that:

$$r = a - bq > 0.$$

Thus, $a = bq + r$.

Then we need to show that $r < b$. Suppose, to the contrary, that $r \geq b$. Then:

$$a - b(q+1) = r - b \geq 0,$$

So $a - b(q+1) \in S$. But this element satisfies:

$$a - b(q+1) < a - bq = r,$$

contradicting the minimality of r. Therefore $0 \leq r < b$, completing the proof of existence.

The proof of uniqueness of q and r is left as an exercise. □

Definition 1.3. The **greatest common divisor (gcd)** of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by $\gcd(a, b)$.

Definition 1.4. Two nonzero integers a and b are **coprime** or **relatively prime** if $\gcd(a, b) = 1$.

Remark 1.5. One can also define the gcd of $a_1, a_2, \ldots, a_k$ as the largest of common divisors of all a_i's. Then one has

$$\gcd(a_1, \ldots, a_k) = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_k) = \gcd(\gcd(\gcd(a_1, a_2), a_3), \ldots, a_k).$$

Similarly, if $\gcd(a_1, \ldots, a_k) = 1$, we say $a_1, \ldots, a_k$ are **relatively prime**. Note that $a_1, \ldots, a_k$ are relatively prime does not necessarily mean $\gcd(a_i, a_j) = 1$ for any $i \neq j$. For instance:

$$\gcd(6, 10, 15) = 1$$

but $\gcd(6, 10) = 2$, $\gcd(6, 15) = 3$, $\gcd(10, 15) = 5$.

Definition 1.6. An integer p is **irreducible** if $p \neq \pm 1$ and the only divisors of p are ± 1 and $\pm p$ (except for zero). A nonzero integer, except for ± 1, is **reducible**(or **composite**) if it is not irreducible.

Definition 1.7. A nonzero integer p is **prime** if and only if it is irreducible.

1.2 Euclidean algorithm and Bézout's Theorem

To find the greatest common divisor of two integers, one can apply Euclidean algorithm:

Example 1.8. To find $\gcd(374, 221)$, one can keep dividing the larger integer by the smaller integer:

$$\begin{aligned} 374 &= 1 \cdot 221 + 153 \\ 221 &= 1 \cdot 153 + 68 \\ 153 &= 2 \cdot 68 + 17 \\ 68 &= 4 \cdot 17 + 0 \end{aligned}$$

when the remainder is zero, the last remainder to it (colored in red) is the greatest common divisor. Therefore,

$$\gcd(374, 221) = 17$$

Theorem 1.9 (Bézout's Theorem)**.** *Suppose* $\gcd(p, q) = m$*. Then there exist integers* $a, b \in \mathbb{Z}$ *such that*

$$m = ap + bq.$$

Example 1.10. By Bezout's Theorem, there exists a, b integers such that:

$$374a + 221b = 17$$

We now determine such integers explicitly:

To find these integers, one do backward induction from the bottom equality to the top:
From the bottom equality:

$$17 = 153 - 2 \cdot 68$$

Substitute the second equality $(68 = 221 - 1 \cdot 153)$ to the above equation:

$$17 = 153 - 2(221 - 1 \cdot 153) = 3 \cdot 153 - 2 \cdot 221$$

Now substitute the first equality $(153 = 374 - 1 \cdot 221)$ to the above equation:

$$\begin{aligned} 17 &= 3(374 - 221) - 2 \cdot 221 \\ &= 3 \cdot 374 - 3 \cdot 221 - 2 \cdot 221 \\ &= 3 \cdot 374 - 5 \cdot 221 \end{aligned}$$

Thus:

$$a = 3, \quad b = -5$$

In the special case of when a and b are relatively prime, there exist integers s and t such that

$$as + bt = 1.$$

This plays an important role in algebra. More generally, for $a_1, \ldots, a_k \in \mathbb{Z}$, one has

$$a_1 s_1 + \cdots + a_k s_k = \gcd(a_1, \ldots, a_k)$$

for some integers $s_1, \ldots, s_k$. This can be checked by using the fact that $\gcd(a_1, a_2, a_3 \ldots, a_k) = \gcd(\cdots \gcd(\gcd(a_1, a_2), a_3), \ldots, a_k)$ and apply the above algorithms repeatedly.

Finally, we state a standard yet important theorem for natural numbers, and is slightly extended to all integers:

Theorem 1.11 (Fundamental Theorem of Airthmetic)**.** *Every nonzero integer $n \in \mathbb{Z}$ can be factorized into a product of primes up to ± 1, i.e. $n = p_1 p_2 \cdots p_r$ if $n > 0$ or $n = -p_1 p_2 \cdots p_r$ if $n < 0$. Moreover,this product is unique up to ± 1 and the ordering of factors. That is, if*

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

where the p's and q's are primes, then $r = s$ and, after renumbering the q's, we have $p_i = \pm q_i$ for all i.

1.3 Modular Arithmetic $\mathbb{Z}_n$

Sometimes, we would like to study integers that has a certain 'cycle'. For instance, days in a week has a cycle of 7, months in a year has a cycle of 12, hours in a day has a cycle of 24 and so on. We define the *congruence numbers*:

$$\mathbb{Z}_n := \{0 \pmod{n},\ 1 \pmod{n},\ \ldots, (n-1) \pmod{n}\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

For example, when $n = 7$, it corresponds to days in a week, and when $n = 12$ it corresponds to months in a year.

The addition and multiplication rule in $\mathbb{Z}_n$ is given by:

$$[a] + [b] = [\text{remainder of } a + b \text{ in } n]$$
$$[a] \cdot [b] = [\text{remainder of } ab \text{ in } n]$$

(we may sometimes omit the subscript $[\ ]_n$ if it is clear from the context). For instance, when $n = 7$:

$$[4]_7 \cdot [5]_7 = [4 \cdot 5]_7 = [20]_7 = [6]_7$$

There are many applications on modular arithmetic - for instance, RSA cryptography, fast Fourier transform, etc. It can also be used to verify the validity of statements about divisibility regarding all positive integers by checking only finitely many cases.

Example 1.12. To see:

$$[n^3 + (n+1)^3 + (n+2)^3]_9 \equiv [0]_9$$

for all integers $n \in \mathbb{Z}$, one only needs to check this holds for $n = 0, 1, \ldots, 8$.

1.4 Equivalence Relations

One has encountered the notion of 'equivalence' in different contexts within or outside of mathematics. This allows us to relate different objects that are not necessarily identical to each other.

For instance, one studies 'similar triangles' in middle school mathematics, where two non-identical triangles $\Delta_1 \sim \Delta_2$ are similar if one can resize one triangle to get another. Another example is the congruence numbers we studied in the previous relation, where $1 \neq 8 \neq 15 \neq 22 \neq 29$ but $[1] = [8] = [15] = [22] = [29]$ in $\mathbb{Z}_7$.

Here is a precise definition of what it means for two elements to be equivalent:

Definition 1.13 (Equivalence Relation)**.** An equivalence relation on a set X is a binary relation R on X that has the following three properties:

1. $(x, x) \in R$ for all $x \in X$ (reflexivity).
2. $(x, y) \in R$ implies $(y, x) \in R$ (symmetry).
3. $(x, y) \in R$ and $(y, z) \in R$ imply $(x, z) \in R$ (transitivity).

We will write $x \sim y$ instead of $(x, y) \in R$.
If $\sim$ is an equivalence relation on a set X and $x \in X$, then the **equivalence class containing/with representative** x is the subset:

$$[x] = \{y \in X \mid x \sim y\}.$$

The collection of equivalence classes of X is denoted as:

$$X/\sim := \{[x] \mid x \in X\}$$

Example 1.14.

1. Let S be the set of all triangles in a plane. If $a, b \in S$, define $a \sim b$ if a and b are similar-that is, if a and b have corresponding angles that are the same. Then $\sim$ is an equivalence relation on S.

2. Let $S = \mathbb{Z}$ be the set of integers. We define $a \sim b$ if $a \equiv b \bmod 7$, or equivalently $[a]_7 = [b]_7$. Then one can show that $\sim$ is an equivalence relation, and the equivalence class containing 1 is

$$[1] = \{\cdots, -13, -6, 1, 8, 15, \cdots\} = [8] = [15]$$

This justifies our notation of using $[\ ]_n$ for the elements in $\mathbb{Z}_7$.

One important aspect of equivalence relation on S is that it gives a **partition** of S. Namely, a partition of S is a disjoint union of nonempty subsets $P_i \subseteq S$ such that

$$\bigsqcup_{i \in I} P_i = S$$

Theorem 1.15. *Let $\sim$ be an equivalence relation on a set S. Then the collection of equivalence classes constitute a partition of S.*

Conversely, for any partition P_i of S, there is an equivalence relation on S whose equivalence classes are precisely the elements of P_i.

Proof. Let $\sim$ be an equivalence relation on a set S. For any $a \in S$, $a \in [a]$ since $a \sim a$. Therefore, $[a]$ is nonempty, and $\bigcup_{a\in S}[a] = S$.

There are repetitions in the union above. One therefore has to show that for $a, b \in S$, one either has $[a] = [b]$ or $[a] \cap [b] = \emptyset$ is disjoint.

To do so, suppose $c \in [a] \cap [b]$, so that $c \sim a$ and $c \sim b$. By symmetry and transitivity, one therefore has $a \sim b$. Then for any $x \in [a]$, one has $x \sim a$ (and $a \sim b$). So $x \sim b$ and hence $x \in [b]$. In other words,

$$[a] \subseteq [b] .$$

The above argument can be reversed, so that one has $[b] \subseteq [a]$ as well. Thus, $[a] = [b]$.

To prove the converse, let $\{P_i \mid i \in I\}$ be a partition of S. Define $a \sim b$ if $a, b \in P_i$ for some $i \in I$. One then can easily check that $\sim$ is an equivalence relation on S. □

1.5 Functions

Definition 1.16. A **function** $\phi : A \to B$ from a set A to a set B is a rule that assigns to each element $a \in A$ exactly one element $\phi(a) \in B$. The set A is called the **domain** of ϕ, and B is called the **codomain** of ϕ.

When we say ϕ is **well-defined**, we need to show the following:

- For all $a \in A$, $\phi(a) \in B$; and
- If $a = a' \in A$, then $\phi(a) = \phi(a') \in B$.

The above definition of well-definedness may look trivial at the first sight, but this may become an issue when one has two or more 'representatives' of the same element in A. For instance, a map $\phi : \mathbb{Z}_7 \to \mathbb{Z}$ given by $\phi([a]_7) = a$ is *not* well-defined, since $[1]_7 = [8]_7$ but $\phi([1]_7) = 1 \neq 8 = \phi([8]_7)$.

Definition 1.17. A function $\phi : A \to B$ is called

- injective (or one-to-one) if for every $a, a' \in A$, $\phi(a) = \phi(a')$ implies $a = a'$.
- surjective (or onto) if for any $b \in B$, there exists $a \in A$ such that $\phi(a) = b$.
- bijective if it is both injective and surjective.

In the case when $\phi : A \to B$ is bijective, one says that ϕ is **invertible**, and has an inverse $\psi : B \to A$ (often denoted as ϕ^{-1}) such that

$$\phi^{-1} \circ \phi = \mathrm{id}_A, \qquad \phi \circ \phi^{-1} = \mathrm{id}_B.$$

where $\mathrm{id}_S : S \to S$ is the identity map $\mathrm{id}_S(s) := s$ for all $s \in S$.

1.6 Polynomials

In this section, we will introduce some basic aspects of polynomials over a field $\mathbb{F}$. For beginners, it is safe to assume $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

Definition 1.18. 1. A polynomial over $\mathbb{F}$ has the form

$$p(z) = a_m z^m + \cdots + a_1 z + a_0, \quad (a_m \neq 0).$$

Here $a_m z^m$ is called the **leading term** of $p(z)$; m is called the degree; a_m is called the **leading coefficient**; $a_m, \ldots, a_0$ are called the coefficients of this polynomial.

2. A polynomial over $\mathbb{F}$ is **monic** if its leading coefficient is $1_{\mathbb{F}}$.

3. A polynomial $p(z) \in \mathbb{F}[z]$ is **irreducible** if for any $a(z), b(z) \in \mathbb{F}[z]$,

$$p(z) = a(z)b(z) \implies \text{either } a(z) \text{ or } b(z) \text{ is a constant polynomial.}$$

Otherwise $p(z)$ is **reducible**.

Example 1.19. The polynomial $p(x) = x^2 + 1$ is irreducible over $\mathbb{R}[x]$; but $p(x) = (x - i)(x + i)$ is **reducible** in $\mathbb{C}[x]$.

Theorem 1.20. *Division Algorithm For all $p, q \in \mathbb{F}[z]$ such that $p \neq 0$, there exists unique $s, r \in \mathbb{F}[x]$ satisfying $\deg(r) < \deg(q)$, such that*

$$p(z) = s(z) \cdot q(z) + r(z).$$

Here $r(z)$ is called the ***remainder****.*

Theorem 1.21 (Root Theorem)**.** *For $p(x) \in \mathbb{F}[x]$, and $\lambda \in \mathbb{F}$, $x - \lambda$ divides $p(x)$ if and only if $p(\lambda) = 0$.*

Proof. 1. If $(x - \lambda)$ divides p, then $p(x) = (x - \lambda)q(x)$ for some $q(x) \in \mathbb{F}[x]$. Thus clearly $p(\lambda) = 0$.

2. For the other direction, suppose that $p(\lambda) = 0$. By division theorem, there exists $q(x), r(x) \in \mathbb{F}[x]$ such that

$$p(x) = (x - \lambda)q(x) + r(x) \quad \text{with } \deg(r(x)) < \deg(x - \lambda) = 1. \tag{1.1}$$

Therefore, $r(x) = r$ must be a constant polynomial. Substituting λ into both sides in the above equation, we have

$$0 = p(\lambda) = 0 \cdot q(x) + r \implies r = 0.$$

Therefore, $p = (x - \lambda) \cdot q(x)$, i.e., $(x - \lambda)$ divides $p(x)$. □

Corollary 1.22. *A polynomial with degree n has at most n roots counting multiplicity.*

Definition 1.23 (Algebraically Closed)**.** A field $\mathbb{F}$ is called **algebraically closed** if every non-constant polynomial $p(x) \in \mathbb{F}[x]$ has a root $\lambda \in \mathbb{F}$, or equivalently, all polynomials in $p(x) \in \mathbb{F}[x]$ can be factorized into linear terms:

$$p(x) = c(x - \lambda_1) \cdots (x - \lambda_n)$$

for $c, \lambda_1, \dots, \lambda_n \in \mathbb{F}$.

We have seen before that $\mathbb{R}$ is not algebraically closed. Nevertheless, we have:

Theorem 1.24 (Fundamental Theorem of Algebra)**.** *$\mathbb{C}$ is algebraically closed.*

We will skip the proof of the theorem. This can be proved using complex **analysis** (MAT 3253); or **topology** of S^1 (MAT 4002); or **algebra**ic number theory (MAT 5210).

In general, $\mathbb{F}$ may not necessarily be factorized into linear terms. But the factorization is still unique. This can be seen as an analogue of the fundamental theory of arithmetic in $\mathbb{Z}$:

Theorem 1.25 (Unique Factorization)**.** *Every $f(x) = a_n x^n + \cdots + a_0$ in $\mathbb{F}[x]$ can be factorized as*

$$f(x) = a_n [p_1(x)]^{e_1} \cdots [p_k(x)]^{e_k}$$

*where p_i's are **monic, irreducible, distinct**. Furthermore, this expression is unique up to the permutation of factors.*

This will be proved in the chapter of Ring Theory. Assuming its validity for the moment, we can now define:

Definition 1.26 (Factor)**.** If $p(x) = q(x)s(x)$ with $p, q, s \in \mathbb{F}[x]$, then we say

- $p(x)$ is **divisible** by $s(x)$;
- $s(x)$ is a **factor** of $p(x)$;
- $s(x)|p(x)$;
- $s(x)$ **divides** $p(x)$;
- $p(x)$ is **multiple** of $s(x)$.

Definition 1.27 (Common Factor)**.** 1. The polynomial $g(x)$ is said to be a **common factor** of $f_1, \dots, f_k \in \mathbb{F}[x]$ if

$$g | f_i, \quad i = 1, \dots, k$$

2. The polynomial $g(x)$ is said to be a **greatest common divisor** of $f_1, \dots, f_k$ if

   - g is **monic**.
   - g is common factor of $f_1, \dots, f_k$

- g is of largest possible (maximal) degree.

$\gcd(f_1, f_2)$ is easy to compute for factorized polynomials. For example, let $f_1(x) = (x^2 + x + 1)^3(x-3)^2x^4$ and $f_2(x) = (x^2+1)(x-3)^4x^2$ in $\mathbb{R}[x]$, then

$$\gcd(f_1, f_2) = (x-3)^2x^2.$$

As for general polynomials, the gcd can be computed using Euclidean algorithm as in the case of integers: For example, given $x^3 + 6x + 7$ and $x^2 + 3x + 2$, we imply

$$\begin{aligned} x^3 + 6x + 7 &= (x-3)(x^2+3x+2) + (13x+13) \\ x^2 + 3x + 2 &= \frac{x+2}{13}(13x+13) + 0 \end{aligned}$$

Therefore, $\gcd(x^2+3x+2, 13x+13)$ is equal to a scalar multiple of $13x+13$ such that it is monic, namely

$$\gcd(x^3+6x+7, x^2+3x+2) = x+1.$$

Similarly, one has Bezout's theorem for polynomials:

Theorem 1.28 (Bezout). *Let $g = \gcd(f_1, f_2)$, then there exists $r_1, r_2 \in \mathbb{F}[x]$ such that*

$$g(x) = r_1(x)f_1(x) + r_2(x)f_2(x)$$

More generally, $g = \gcd(f_1, \dots, f_k)$ implies there exists $r_1, \dots, r_k$ such that

$$g = r_1f_1 + \cdots + r_kf_k$$

1.7 Introduction to Abstract Algebra

We now give a brief introduction of abstract algebra - in a nutshell, abstract algebra is about generalization of number systems we studied in kindergarten, such as:

$$\begin{aligned} &\mathbb{Z} = \{\dots, -1, 0, 1, \dots\} \\ &\mathbb{Q} = \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus \{0\} \right\} \\ &\mathbb{R} = \text{real numbers (limits of Cauchy sequences in } \mathbb{Q}) \\ &\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\} \end{aligned}$$

All these number systems have addition and multiplication, e.g. in $\mathbb{Q}$:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

And they all possess nice properties, e.g.,

$$(a+b)+c = a+(b+c) \tag{A1}$$

$$(ab)c = a(bc) \tag{A2}$$

$$ab = ba \tag{C1}$$

$$a+b = b+a \tag{C2}$$

$$a(b+c) = ab+ac \tag{D1}$$

$$(a+b)c = ac+bc \tag{D2}$$

One goal in abstract algebra is to study different number systems, and to find out their common features and obtain theorems that hold for all such generalized number systems.

Example 1.29.

$$M_{2\times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{R} \right\}$$

We can still do + and × on $M_{2\times 2}(\mathbb{R})$, but we no longer have (C1) - in other words,

$$AB \neq BA \quad \text{in general for matrices.}$$

Chapter 2

Groups

2.1 Basic Definitions

Definition 2.1. Let S be a set. A *binary operation* on S is a map:

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

Let $T \subseteq S$ be a subset. We say that the binary operation is *closed* in T if:

$$\forall a, b \in T, \quad a * b \in T$$

Example 2.2. Let $S = \mathbb{Z}$. Then the following are binary operations:

- $S = \mathbb{Z}, \quad * = +$ (addition)
- $S = \mathbb{Z}, \quad * = \times$ (multiplication)

Let

$$T = \{\text{all even integers}\} \subset \mathbb{Z}.$$

For $a, b \in T$, $a + b \in T$ (the sum of two even numbers is even). Hence $(T, +)$ is closed in $(S, +)$. Also, if $a, b \in T$, $a \cdot b \in T$ (the product of two even numbers is even). Therefore, $(T, \times)$ is also closed in $(S, \times)$.

However, let

$$T' = \{\text{all odd integers}\}$$

Then $(T', +)$ is **not** closed in $(S, +)$. But for any $(2p + 1), (2q + 1) \in T'$:

$$(2p + 1) \cdot (2q + 1) = 4pq + 2p + 2q + 1 = 2(2pq + p + q) + 1 \in T'$$

Therefore, $(T', \times)$ is closed in $(S, \times)$.

Example 2.3. 1. Let $S = \mathbb{R}^n$, and $* =$ be the vector addition operation. If $W \leq \mathbb{R}^n$ is a vector subspace, then $(W, +)$ is closed in $(\mathbb{R}^n, +)$.

2. Let $S = M_{n\times n}(\mathbb{R})$, and $* =$ multiplication of the ne matrix. Suppose $T = GL_n(\mathbb{R})$ is the subset of all invertible real matrices. To check if T is closed in $(S, \times)$: If $A, B \in T$ (invertible matrices), then $A \cdot B$ is invertible since
$$(AB)^{-1} = B^{-1}A^{-1}$$
or alternatively:
$$\det(AB) = \det(A)\det(B) \neq 0$$
Hence, T is closed in $(S, \times)$.

Definition 2.4 (Group)**.** A **group** G is a set along with a binary operation $* : G \times G \to G$ satisfying:

1. $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G \quad$ (associativity)
2. $\exists\ e \in G$ such that $e * a = a * e = a,\ \forall a \in G \quad$ (identity)
3. $\forall a \in G,\ \exists b \in G$ s.t. $a * b = b * a = e$ (b is often written as a^{-1}, called the inverse of a)

Example 2.5. (a) $(\mathbb{Z}, +)$ is a group. To see this, note that
$$\begin{cases} (a+b)+c = a+(b+c) \\ 0+a = a+0 = a \quad \forall a \in \mathbb{Z} \quad (\text{i.e., } e = 0) \\ a+(-a) = (-a)+a = 0 \quad (\text{i.e., } a^{-1} = -a) \end{cases}$$

(b) Similarly $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ as well as $(\mathbb{Z}_n, +)$ are groups.

(c) $(\mathbb{Z}, -)$ is **not** a group, since $(a-b)-c \neq a-(b-c)$ and $0-a \neq a-0 = a$ in general, i.e. it is not associative.

(d) $(\mathbb{Z}, \times)$ is also **not** a group. Although $(a\times b)\times c = a\times(b\times c)$ is associative, and $a\times 1 = 1\times a = a$ (so that the identity can be taken as $e = 1$), but there is *no* $a \in \mathbb{Z}$ such that $2 \times a = 1 = e$.)

(e) $(\mathbb{Q}, \times)$ is **not** a group. Although now one can take $a = \frac{1}{2}$ such that $2 \times \frac{1}{2} = 1$, yet the element $0 \in \mathbb{Q}$ does not have a multiplicative inverse.

(f) To resolve the issue, let $\mathbb{Q}^* = \{q \in \mathbb{Q} \mid q \neq 0\}$. Then $(\mathbb{Q}^*, \times)$ is a group.

(g) Similarly, $(\mathbb{R}^*, \times)$ and $(\mathbb{C}^*, \times)$ are groups.

(h) The set of 2×2 real matrices, denoted $M_2(\mathbb{R})$, under matrix multiplication $(M_2(\mathbb{R}), \times)$ is **not** a group, because not all matrices have a multiplicative inverse (namely, singular matrices do not have a multiplicative inverse).

(i) Let $GL(2, \mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid \det(A) \neq 0\}$ be the set of 2×2 invertible matrices with real entries. Then $(GL(2, \mathbb{R}), \times)$ is a group, known as the general linear group of degree 2 over $\mathbb{R}$.

Question 2.6. *Given $n \in \mathbb{N}$, for which $a \in \mathbb{Z}$ does $[a]_n$ (the congruence class of a modulo n) have a multiplicative inverse in $\mathbb{Z}_n$?*

Answer: An element $[a]_n \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$. For instance, when $n = 6$, then:

- For $a = 3$, $\gcd(3, 6) = 3 \neq 1$. Therefore, $[3]_6$ does not have a multiplicative inverse in $\mathbb{Z}_6$.
- For $a = 5$, $\gcd(5, 6) = 1$. Therefore, $[5]_6$ has a multiplicative inverse in $\mathbb{Z}_6$. Indeed, $[5]_6 \cdot [5]_6 = [25]_6 \equiv [1]_6 \pmod 6$, so $[5]_6^{-1} = [5]_6$.

Remark 2.7. When there is no ambiguity, we often write ab instead of $a * b$. Also, for all $m \in \mathbb{Z}$, we denote

$$a^m := \begin{cases} \overbrace{a * a * \cdots * a}^{m\ times} & \text{if } m > 0 \\ e & \text{if } m = 0 \\ \overbrace{a^{-1} * a^{-1} * \cdots * a^{-1}}^{-m\ times} & \text{if } m < 0 \end{cases}$$

In the case when the operation $*$ is the 'usual' addition $+$, we call $(G, +)$ **additive group**, and write

$$0 := e, \quad -a := a^{-1}, \quad m \cdot a := a^m.$$

The order of multiplication matters, namely for $b \in G$, multiplying $a \in G$ on the left or on the right may result in different elements. In the case when they are the same, we have:

Definition 2.8 (Abelian Group)**.** A group $(G, *)$ is called *abelian* if its operation is commutative; that is, for all $a, b \in G$, we have $a * b = b * a$.

Example 2.9.

- Examples of abelian groups include: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, and $(\mathbb{Z}_n, +)$.
- The group $(GL(2, \mathbb{R}), \times)$ is NOT abelian, as matrix multiplication is generally not commutative.

Proposition 2.10. *Let $(G, *)$ be a group.*

1. *(Uniqueness of Identity) The identity element e in G is unique.*
2. *(Uniqueness of Inverses) For each $a \in G$, its inverse a^{-1} is unique.*
3. *(Cancellation Laws) For $a, b, c \in G$:*
   - *If $a * b = a * c$, then $b = c$.*
   - *If $b * a = c * a$, then $b = c$.*

2.2 Cayley Table

Definition 2.11 (Order of a Group)**.** The *order* of a group G, denoted $|G|$, is the number of elements in the group. If $|G| < \infty$, the group is called a *finite group.*

Definition 2.12 (Cayley Table)**.** For a finite group $(G, *)$, a *Cayley table* (or group table) is a square table where the rows and columns are labeled by the elements of the group. The entry in the row corresponding to a and the column corresponding to b is $a * b$.

Example 2.13. The Cayley table for $\mathbb{Z}_9^*$ is:

$\times$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[1]_9$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[2]_9$	$[2]_9$	$[4]_9$	$[8]_9$	$[1]_9$	$[5]_9$	$[7]_9$
$[4]_9$	$[4]_9$	$[8]_9$	$[7]_9$	$[2]_9$	$[1]_9$	$[5]_9$
$[5]_9$	$[5]_9$	$[1]_9$	$[2]_9$	$[7]_9$	$[8]_9$	$[4]_9$
$[7]_9$	$[7]_9$	$[5]_9$	$[1]_9$	$[8]_9$	$[4]_9$	$[2]_9$
$[8]_9$	$[8]_9$	$[7]_9$	$[5]_9$	$[4]_9$	$[2]_9$	$[1]_9$

Proposition 2.14. *In a Cayley table for a finite group, each element of the group appears exactly once in each row and exactly once in each column. In other words, for all $a \in G$, the sets*

$$\{a * g \mid g \in G\}$$

and

$$\{g * a \mid g \in G\}$$

contains all elements of G exactly once, with no repetitions.

2.3 Subgroups

Definition 2.15 (Subgroup)**.** Let $(G, *)$ be a group and H be a non-empty subset of G. We say that H is a *subgroup* of G, denoted $H \leq G$, if $(H, *)$ is itself a group under the same operation $*$ restricted to H.

Proposition 2.16 (Subgroup Test)**.** *Let $(G, *)$ be a group and H be a non-empty subset of G. Then H is a subgroup of G if and only if:*

1. *For all $a, b \in H$, $a * b \in H$, i.e. $*$ is closed in H.*
2. *For all $a \in H$, $a^{-1} \in H$.*

Equivalently, one can check the following:

$$\text{For all } a, b \in H,\ a * b^{-1} \in H.$$

Example 2.17. 1. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

2. If $W \leq \mathbb{R}^n$ is a vector subspace, then $(W, +) \leq (\mathbb{R}^n, +)$ is a subgroup.

3. Let $(G, *) = (\mathbb{Z}, +)$, and $H =$ all even integers $= 2\mathbb{Z} \subseteq G$. Take $2p, 2q \in H$ $(p, q \in \mathbb{Z})$. Then $2p + 2q = 2(p + q) \in H$ and $-2p = 2(-p) \in H$. Hence, $H \leq G$ is a subgroup of G. More generally, for all $k \in \mathbb{Z}$, $(k\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

   Meanwhile, if $K =$ all odd integers $\subseteq G$, then K is **NOT** a subgroup of G, since $1, 3 \in K$ but $1 + 3 \notin K$.

4. Let $(G, *) = (GL(n, \mathbb{R}), \cdot)$, and

$$SL(n, \mathbb{R}) := \{A \in G \mid \det(A) = 1\}$$

   Then $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$:

   - For all $A, B \in SL(n, \mathbb{R})$, $\det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$. Therefore, $AB \in SL(n, \mathbb{R})$ for all $A, B \in SL(n, \mathbb{R})$
   - For all $A \in SL(n, \mathbb{R})$, $\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1$. Therefore, $A^{-1} \in SL(n, \mathbb{R})$ as well.

5. Let $(G, *) = (\mathbb{Z}_8, +)$. Then $H = \{0, 4\}$ is a subgroup of G, while $K = \{0, 3\}$ is **NOT** a subgroup.

Definition 2.18. Let $(G, *)$ be a group. Then:

1. $(G, *) \leq (G, *)$ is a subgroup of G. We say all $H \leq G$ satisfying $H \neq G$ a **proper subgroup** of G.
2. $\{e\} \leq G$ is a subgroup. We say all $H \leq G$ with $H \neq \{e\}$ a **nontrivial subgroup** of G.

2.4 Cyclic Groups

Definition 2.19 (Cyclic Subgroup)**.** Let $(G, *)$ be a group. A **cyclic subgroup** generated by $g \in G$ is the subgroup

$$\langle g \rangle := \{g^m \mid m \in \mathbb{Z}\}.$$

(Exercise: Check $\langle g \rangle \leq G$ is a subgroup of G, i.e.: for any $g^a, g^b \in \langle g \rangle$ $\begin{cases} g^a * g^b \in \langle g \rangle \\ (g^a)^{-1} \in \langle g \rangle \end{cases}$.)

Example 2.20. Here are some examples of cyclic subgroups:

1. Let $(G, *) = (\mathbb{Z}, +)$, then

$$\langle 2 \rangle = \{2, 2+2, 2+2+2, \ldots, 0, (-2), (-2)+(-2), (-2)+(-2)+(-2), \ldots\} = 2\mathbb{Z}.$$

2. Let $(G, *) = (GL(2, \mathbb{R}), \cdot)$, then

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \middle| m \in \mathbb{Z} \right\} = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \middle| m \in \mathbb{Z} \right\}.$$

(Check: $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & a+b\\ 0 & 1\end{pmatrix}$)

3. Let $(G, *) = (\mathbb{Z}_8, +)$, then

$$\langle 2\rangle = \{0, 2, 4, 6, \dots\} = \{0, 2, 4, 6\}$$

$$\langle 3\rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24, \dots\} = \{0, 3, 6, 1, 4, 7, 2, 5, 0, \dots\} = G$$

Definition 2.21 (Cyclic Group)**.** Let $(G, *)$ be a group. We say G is **cyclic** if there is $g \in G$ such that $\langle g\rangle = G$.

Example 2.22.

- $(G, *) = (\mathbb{Z}, +)$ is cyclic, since $G = \langle 1\rangle$.
- $(G, *) = (\mathbb{Z}_8, +)$ is cyclic, since $G = \langle 3\rangle = \langle 1\rangle$.
- $(G, *) = (GL(2, \mathbb{R}), \cdot)$ is **NOT** cyclic, since for all $H = \langle g\rangle$, H is countable but G is uncountable. Hence, H can never be equal to G.
- $(G, *) = (\mathbb{Z}_8^*, \cdot) = \{1, 3, 5, 7\}$. Then the cyclic subgroups of G are:
  $\langle 1\rangle = \{1\}$,
  $\langle 3\rangle = \{3^0 = 1, 3^1 = 3, 3^2 = 1, 3^3 = 3, \dots\} = \{1, 3\}$;
  $\langle 5\rangle = \{1, 5\}$;
  $\langle 7\rangle = \{1, 7\}$.

  Note that none of them is equal to G. So G is **not** cyclic.

Question: $(G, *)$ group, $H = \langle g\rangle$. What's the order of H? For instance, if $G = (\mathbb{Z}_8, +)$, then $|\langle [2]\rangle| = 4,\ |\langle [3]\rangle| = 8,\ |\langle [4]\rangle| = 2$.

Definition 2.23 (Order)**.** Let $g \in G$. The *order* of g is equal to the smallest positive integer k such that $g^k = e$. If no such k exists, then we say the order of g is ∞.

Proposition 2.24. *If* $\operatorname{ord}(g) = k$*, then* $|\langle g\rangle| = k$*.*

Example 2.25.

- $(G, *) = (\mathbb{Z}_8, +)$. $\operatorname{ord}([2]) = 4$ since

$$[2] = [2], [2] + [2] = [4], [2] + [2] + [2] = [6], [2] + [2] + [2] + [2] = [8] = [0].$$

Also, $\operatorname{ord}([3]) = 8$, since

$$1 \cdot [3] = [3],\ 2 \cdot [3] = [6],\ 3 \cdot [3] = [9] = [1],\ 4 \cdot [3] = [12] = [4],$$

$$5 \cdot [3] = [15] = [7],\ 6 \cdot [3] = [18] = [2],\ 7 \cdot [3] = [21] = [5],\ 8 \cdot [3] = [24] = [0].$$

- Let $(G, *) = (GL(2, \mathbb{R}), \cdot)$. Then $\operatorname{ord}\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \infty$, since

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \forall m \in \mathbb{N}.$$

Remark 2.26. If $|G| < \infty$ is finite, then $\langle g \rangle \leq G$ is a finite subgroup with $|\langle g \rangle| \leq |G|$. Indeed, all $H \leq G$ has $|H| \mid |G|$ (see Section 2.7 - Lagrange's Theorem below).
e.g.: If $|G| = 12$, then there is **NO** $H \leq G$ with $|H| = 8$, can only be $1, 2, 3, 4, 6, 12$.
Therefore, $\operatorname{ord}(g) \mid |G|$ (take $H = \langle g \rangle$).

2.5 More examples of Groups

Permutation group / Symmetric group S_n

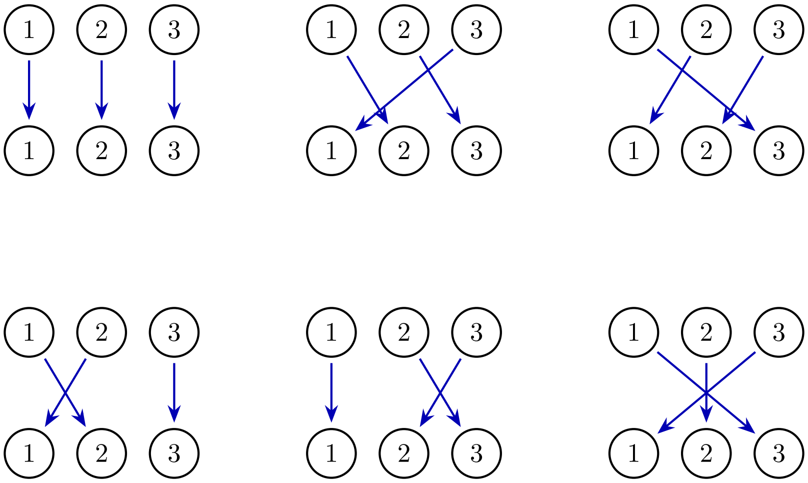
Definition 2.27. A *permutation* of $X_n = \{1, 2, \ldots, n\}$ is a bijection $\sigma : X_n \to X_n$.

For example, when $n = 3$, $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$ is a permutation.

Definition 2.28. The **symmetric / permutation group** of n elements is the collection of all permutations $\sigma : X_n \to X_n$.

$$S_n := \{\sigma : X_n \to X_n \mid \sigma \text{ is bijective}\}$$

For instance, when $n = 3$, one has:



Hence $|S_3| = 6$. More generally,

$$|S_n| = n \cdot (n-1) \cdots 1 = n!.$$

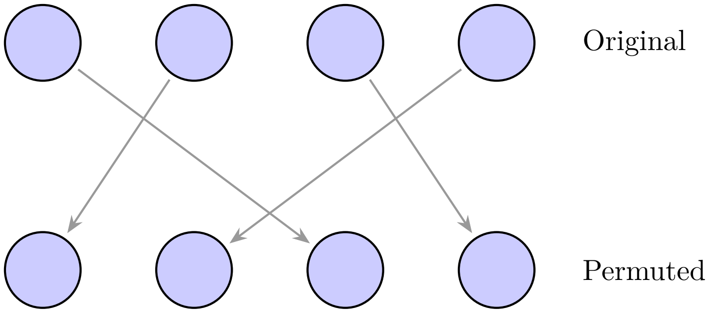
Proposition 2.29. *$(S_n, \circ)$ is a group, where $\circ$ is the composition of functions.*

Proof. We need to show that the three axioms of groups hold for $(S_n, \circ)$:

1. $(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3)$ is true, since composition of functions $\circ$ is associative.
2. Take $e = \mathrm{id} : X_n \to X_n$, $e(i) := i$ for all $1 \leq i \leq n$. Then $\sigma \circ e = e \circ \sigma = \sigma$.
3. Since σ is bijective, then $\sigma^{-1} : X_n \to X_n$ exists with $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e$.

□

Remark 2.30. Groups are often used to study "symmetry" of objects. For example, S_n can be used to study symmetry of n identical objects. Here is an example of $n = 4$:



Although we have carried out a permutation $1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 4$, $4 \mapsto 2$, one cannot tell the difference of the objects before and after permutation.

As another example, to describe (some) symmetries of $\mathbb{R}^n$, we have:

$$GL(n, \mathbb{R}) = \{A : \mathbb{R}^n \to \mathbb{R}^n \mid A \text{ is a bijective linear transformation}\}$$

which can be seen as a certain kind of ‘permutation’ on the points in $\mathbb{R}^n$.

Calculations on S_n

We use cycle notations to denote elements of S_n.

Definition 2.31. A permutation $\sigma \in S_n$ is called a **k-cycle** (or a cycle of length k) if there exists a set of k distinct elements $\{a_1, a_2, \ldots, a_k\} \subseteq \{1, 2, \ldots, n\}$ such that:

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \quad \ldots, \quad \sigma(a_{k-1}) = a_k, \quad \sigma(a_k) = a_1$$

and $\sigma(i) = i$ for all $i \notin \{a_1, a_2, \ldots, a_k\}$.

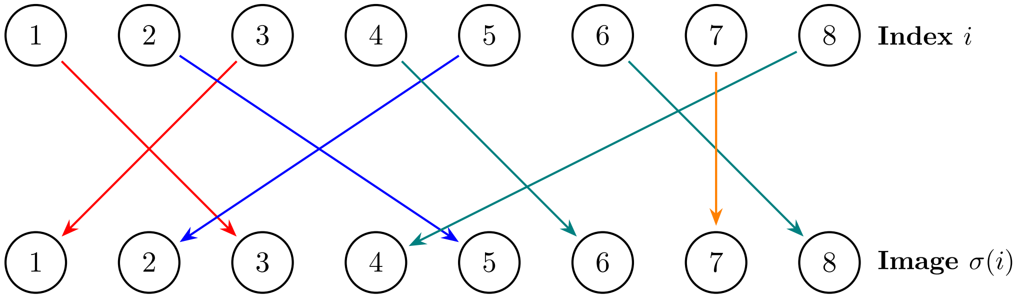
As an example, the element $\sigma \in S_4$ in Remark 2.30 is a 4-cycle $\sigma = (1\ 3\ 4\ 2)$.

Note that every $\sigma \in S_n$ can be expressed as a product of **disjoint** cycles (possibly of different lengths):

$$\sigma = (a_1 \dots a_k)(b_1 \dots b_l) \cdots (c_1 \dots c_m) := (a_1 \dots a_k) \circ (b_1 \dots b_l) \circ \cdots \circ (c_1 \dots c_m).$$

where the sets $\{a_1, \dots, a_k\}$, $\{b_1, \dots, b_l\}$, $\cdots$, $\{c_1, \dots, c_m\}$ are disjoint subsets of X_n. For instance, in S_8, the permutation

$$1 \to 3, \quad 2 \to 5, \quad 3 \to 1, \quad 4 \to 6, \quad 5 \to 2, \quad 6 \to 8, \quad 7 \to 7, \quad 8 \to 4$$



can be split into:

- $1 \to 3$ and $3 \to 1$. This gives the cycle $(1\,3)$.
- $2 \to 5$ and $5 \to 2$. This gives the cycle $(2\,5)$.
- $4 \to 6$, $6 \to 8$, and $8 \to 4$. This gives the cycle $(4\,6\,8)$.
- $7 \to 7$. This is a fixed point, giving the 1-cycle (7).

Therefore,

$$\sigma = (1\,3)(2\,5)(4\,6\,8)(7) := (1\,3) \circ (2\,5) \circ (4\,6\,8) \circ (7)$$

Here are some examples in calculating products in S_n:

Example 2.32. Let $\sigma = (1\,2\,3)$, $\tau = (1\,3\,4\,2)(7\,6)$ in S_7. Then:

- $\sigma\tau = (1\,2\,3)(1\,3\,4\,2)(7\,6) = (1)(2)(3\,4)(7\,6) = (3\,4)(6\,7)$.
- $\tau\sigma = (1\,3\,4\,2)(7\,6)(1\,2\,3) = (1)(2\,4)(3)(6\,7) = (2\,4)(6\,7)$.

Therefore,

$$\sigma \circ \tau \neq \tau \circ \sigma \text{ **in general, i.e.** } S_n \text{ **is not abelian for** } n \geq 3.$$

Remark 2.33.

- From now on, we'll express $\sigma \in S_n$ using (disjoint) product of k-cycles.
- If α and β are k-cycles with disjoint entries, then $\alpha\beta = \beta\alpha$.
  (e.g.: $\alpha = (1\,3\,2)$, $\beta = (4\,7) \Rightarrow \alpha\beta = (1\,3\,2)(4\,7) = (4\,7)(1\,3\,2) = \beta\alpha$).
  Otherwise, $\alpha\beta \neq \beta\alpha$ in general.

- The inverse of a k-cycle is given by:

$$(i_1\, i_2 \ldots i_k)^{-1} = (i_1\, i_k\, i_{k-1} \ldots i_2)$$

- More generally, for any $\sigma \in S_n$, $\sigma = (i_1 \ldots i_k)(j_1 \ldots j_\ell) \ldots (m_1 \ldots m_p)$ where the cycles are disjoint, then:

$$\sigma^{-1} = (i_1\, i_k \ldots i_2)(j_1\, j_\ell \ldots j_2) \ldots (m_1\, m_p \ldots m_2)$$

Alternating Group A_n

Definition 2.34 (Transposition)**.** A 2-cycle $\tau = (i\, j) \in S_n$ is called a **transposition**.

Proposition 2.35. *Every $\sigma \in S_n$ can be expressed as a product of (NOT necessarily disjoint) transpositions.*

Proof. $\sigma = (i_1 \ldots i_k)(j_1 \ldots j_\ell) \ldots (m_1 \ldots m_p)$ with each $i, j, \ldots, m$ cycles are disjoint. Then for $(i_1 \ldots i_k)$:

$$(i_1 \ldots i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \ldots (i_1\, i_3)(i_1\, i_2)$$

Do the same for $(j_1 \ldots j_\ell), \ldots, (m_1 \ldots m_p)$. Then we're done. □

Remark 2.36. The expression of $\sigma \in S_n$ into product of transpositions is **NOT** unique. For example,

$$\sigma = (2\,3) = (2\,3)(2\,3)(2\,3) = (1\,2)(2\,3)(1\,3).$$

But the number of transpositions in each expression of σ is always **even** or **odd**, as we will see below.

Lemma 2.37. *If $e = \tau_1 \cdots \tau_k$, where each τ_i is a transposition. Then $k \equiv 0 \pmod 2$ is even.*

Proof. Apply induction on k, that is,

$$\text{If } e = \tau_1 \cdots \tau_k, \text{ then } k \text{ is even.} \qquad (*)$$

The case of $k = 0$ is trivial. Also, it is obvious that the $k \neq 1$, since e cannot be equal to any single transposition τ. So (*) holds for $k = 1$.

Now suppose by induction hypothesis that (*) holds for all expressions of $e = \tau_1' \cdots \tau_{k'}'$ for $k' \leq m$. Consider

$$e = \tau_1 \cdots \tau_m \tau_{m+1},$$

an expression of e with $(m + 1)$ transpositions. Let $\tau_{m+1} = (a\, b)$, Then:

Case 1: $\tau_m = (a\, b)$. In this case, $e = \tau_1 \cdots \tau_{m-1}(a\, b)(a\, b) = \tau_1 \cdots \tau_{m-1}$. By induction, $m-1 \equiv 0 \pmod 2$. Hence, $m + 1 \equiv 0 \pmod 2$ is even.

Case 2: $\tau_m \neq (a\,b)$. Then $\tau_m = \begin{cases} (a\,c) & c \neq b \\ (b\,d) & d \neq a \\ (i\,j)(a\,b) & \{i,j\} \cap \{a,b\} = \emptyset \end{cases}$. Then one has

$$\tau_m \tau_{m+1} = \begin{cases} (a\,c)(a\,b) = (a\,b)(b\,c) \\ (b\,d)(a\,b) = (a\,d)(d\,b) \\ (i\,j)(a\,b) = (a\,b)(i\,j) \end{cases}$$

(where the right hand side in the new expression ($(b\ c)$, $(d\ b)$, $(i\ j)$) have no "a"s). Therefore,

$$e = \tau_1 \cdots \tau_{m-1} \tau_m \tau_{m+1} = \tau_1 \cdots \tau_{m-1} (a\,\star)(*\,*).$$

where $* \neq a$.

Continue the same argument on $\tau_1 \ldots \tau_{m-1}(a\,*)$. If $\tau_{m-1} = (a\,*)$, then $\tau_{m-1}(a\,*)$ goes away. Then one can apply induction as in Case 1 and get the same conclusion. Otherwise, $\tau_{m-1} \neq (a\,*)$, then we use Case 2 to move one more step to the left and get:

$$e = \tau_1 \cdots \tau_{m-2} (a\,\square)(*\,*)(*\,*)$$

with $* \neq a$.

We keep moving a to the left, and claim that Case 1 must occur somewhere, so that we can apply the induction argument to conclude $m+1$ is even. Otherwise, we can keep applying Case 2 to 'push' a to the leftmost position, and get

$$e = (a\,\triangle)(*\,*) \cdots (*\,*)$$

with $* \neq a$. But this **cannot** happen, since the expression on right-hand-side permutes $a \to \triangle$ (note that $(a\ \triangle)$ is the only transposition on the right that moves a), which contradicts that fact that it is the identity element. □

Proposition 2.38. *Let $\sigma = \tau_1 \cdots \tau_k = \tau_1' \cdots \tau_\ell'$ be two expressions of σ as product of transpositions. Then $k \equiv \ell \pmod 2$.*

Proof.
$$e = \sigma^{-1}\sigma = (\tau_1 \cdots \tau_k)^{-1}(\tau_1' \cdots \tau_\ell') = \tau_k^{-1} \cdots \tau_1^{-1} \tau_1' \cdots \tau_\ell' = \tau_k \cdots \tau_1 \tau_1' \cdots \tau_\ell'.$$

Then by Lemma 2.37, $k + \ell \equiv 0 \pmod 2$. □

Definition 2.39. $\sigma \in S_n$ is called an **even / odd permutation** if σ is a product of an even / odd number of transpositions.

Definition 2.40 (Alternating Group)**.** The **alternating group** A_n is the subgroup of S_n given by:

$$A_n := \{\sigma \in S_n \mid \sigma \text{ is even}\}$$

(Check: $A_n \leq S_n$. Also, is the set $\{\sigma \in S_n \mid \sigma \text{ is odd}\}$ a subgroup?)

Proposition 2.41. $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$

Proof. Let $\tau \in S_n$ be a transposition and define $f : A_n \to \{\sigma \in S_n \mid \sigma \text{ odd}\}$ by:

$$f(\sigma) := \sigma\tau.$$

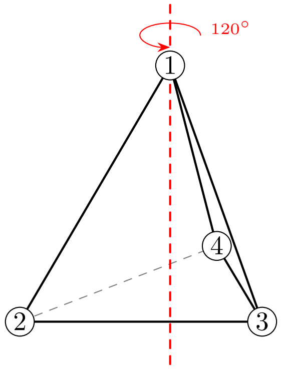
Note that f is bijective with $f^{-1} = f$. Hence, $|A_n| = |\{\sigma \in S_n \mid \sigma \text{ odd}\}|$.

Since $A_n \cap \{\sigma \in S_n \mid \sigma \text{ odd}\} = \emptyset$, and $A_n \sqcup \{\sigma \in S_n \mid \sigma \text{ odd}\} = S_n$, therefore

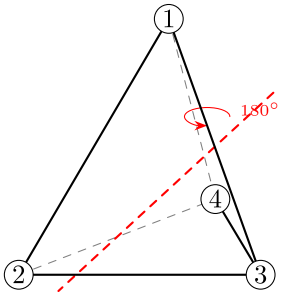
$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

□

Example 2.42. 1. A_4 is the group of "symmetries of a tetrahedron".



Rotation $(2\,3\,4)$



Rotation $(1\,3)(2\,4)$

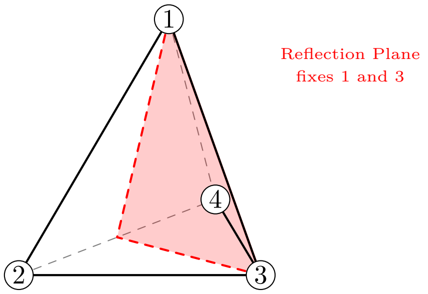
- A rotation of the tetrahedron corresponds to a permutation of its 4 vertices. For example, a 120° rotation about a vertex fixies one vertex and cyclically permutes the other three:

$$(2\,3\,4) = (2\,4)(2\,3) \in A_4$$

- A 180° rotation about the midpoints of opposite edges corresponds to:

$$(1\,3)(2\,4) \in A_4$$

2. If we allow reflections (not just rotations), we get the full symmetric group, e.g. $(2\,4) \in S_4 \backslash A_4$ comes from the reflection:



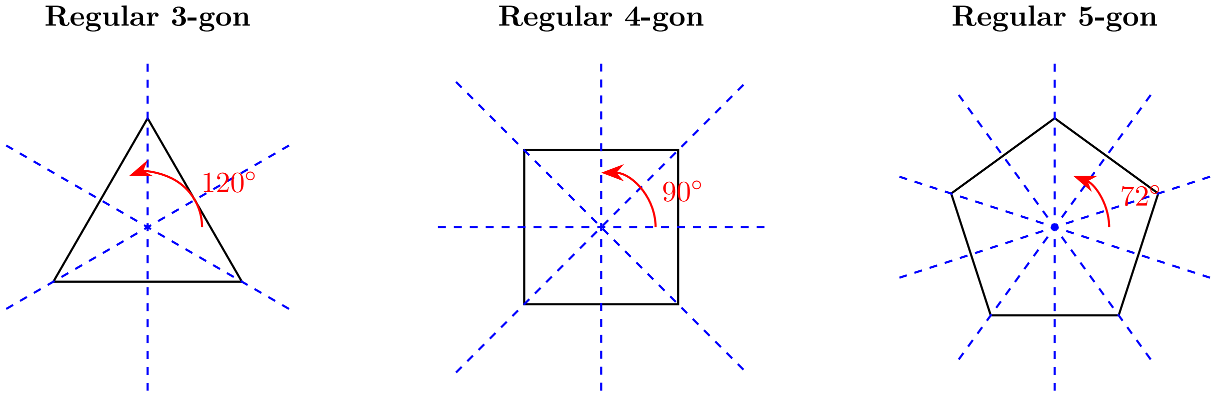
Reflection $(2\,4)$

3. **Galois Theory**: A_5 is a simple group (we will define simple group later). This is a purely group theoretic observation, but it is used by Galois to showing that a general quintic (degree-5) equation **cannot** be solved using radicals, i.e. $+, \times, \frac{*}{*}, \sqrt[k]{*}$.

Dihedral Groups D_n

We begin by giving an informal definition of the dihedral group D_n:

The dihedral group D_n describes the rotational and reflectional symmetries of a regular n-gon. Here are the pictures for $n = 3, 4, 5$:



For example, when $n = 3$, D_3 describes the symmetries of an equilateral triangle:

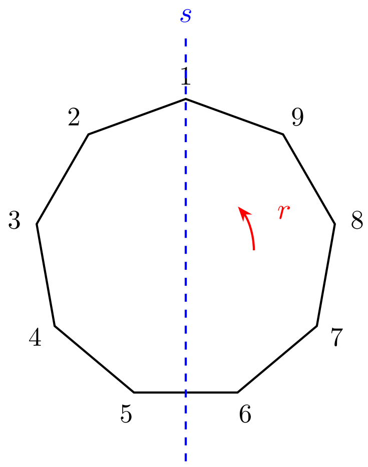
- Rotations: e, σ_{120°, σ_{240°.
- Reflections: 3 axes of symmetry, each fixing one vertex and swapping the other two.

Hence, D_3 has 6 elements. As for $n = 4$, D_4 describes the symmetries of a square, namely:

- There are 4 rotations e, σ_{90°, σ_{180°, σ_{270°
- There are also 4 reflections - 2 reflections on along the diagonals, and 2 reflections along the midpoints of the parallel sides.

Hence, $|D_4| = 8$, and more generally, $|D_n| = 2n$ for all $n \geq 3$.

We now give an algebraic representation of n-gon symmetries. Label the vertices of the n-gon by $1, 2, \ldots, n$. Let r be a rotation by $\left(\frac{360}{n}\right)^\circ$ anticlockwise, , and s be a reflection along the axis passing through vertex 1. For $n = 9$, it looks like:



Then $r^n = e$ and $s^2 = e$. Moreover, if we trace how the vertices are moved along under r and s, we have

$$r \longleftrightarrow (1\ 2\ 3 \ldots n), \qquad s \longleftrightarrow (2\ \ (n-1))(3\ \ (n-2))\cdots$$

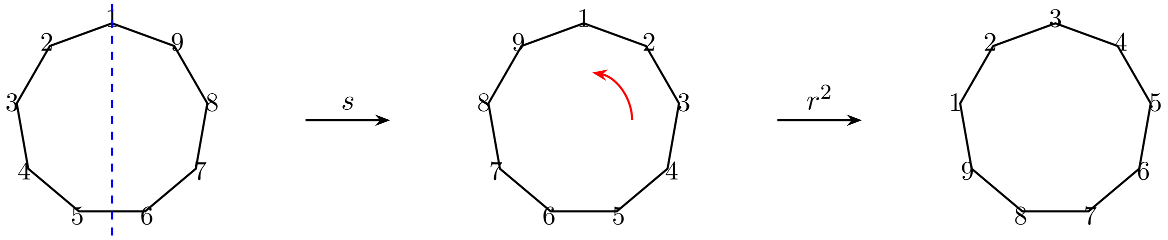
Obviously, all n rotations can be expressed as

$$r^i, \quad 0 \leq i < n.$$

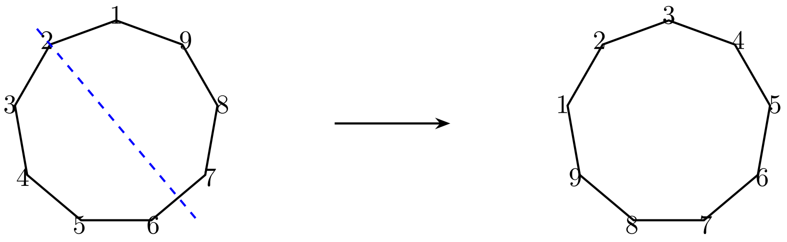
Indeed, the n reflections in D_n can be expressed as

$$r^i s \quad 0 \leq i < n.$$

As an example, for $n = 9$, the picture of $r^2 s$ looks like:



This has the same effect as doing the reflection:



In terms of movement of vertices,

$$r^2 s \longleftrightarrow (1\ 3)(4\ 9)(5\ 8)(6\ 7).$$

More generally, $r^k s$ represents a reflection along an axis obtained by rotating the "axis passing through vertex 1" by $180 \times \left(\frac{k}{n}\right)^\circ$ anticlockwise.

Definition 2.43. The dihedral group D_n is given by the set:

$$D_n = \{e, r, r^2, \dots, r^{n-1}, s, rs, r^2 s, \dots, r^{n-1}s\}$$

such that $r^n = e, s^2 = e$ and $sr^l = r^{n-l}s$ for all $0 \leq l \leq n$. In terms of *generators and relations* (not to be defined precisely in this course), D_n can be written as

$$D_n = \langle s, r \mid r^n = e, s^2 = e, sr^l = r^{n-l}s \text{ for all } l\rangle.$$

For example, in D_5, one can write

$$s^3 r^{14} s^5 r^{-3} s^{16} = sr^{10} r^4 sr^5 r^{-3} e = sr^4 sr^2 = s(sr^1)r^2 = s^2 r^3 = r^3.$$

Product Groups (External Direct Product)

Definition 2.44 (Product Group)**.** Let $G_1, \dots, G_n$ be groups. The **product group** $G := \prod_{i=1}^n G_i = G_1 \times \cdots \times G_n$ is given by

$$G := \{(g_1, \dots, g_n) \mid g_i \in G_i\}$$

whose multiplication is given by:

$$(g_1, \dots, g_n) * (h_1, \dots, h_n) := (g_1 h_1, g_2 h_2, \dots, g_n h_n)$$

In particular, $|G| = |G_1| \times \cdots \times |G_n|$ and $e_G := (e_1, \dots, e_n) \in G$, where $e_i = e_{G_i}$ is the identity element of G_i.

Example 2.45. The product group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is given by

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{([a], [b]) \mid a = 0, 1;\ b = 0, 1, 2\}$$

with $(1, 2) * (0, 1) = (1 + 0, 2 + 1) = (1, 3) \equiv (1, 0)$. (Exercise: $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1, 1) \rangle$ is cyclic.)

One can construct many other groups using products, for instance:

$$S_3 \times D_4; \quad \mathbb{Z} \times \mathbb{R}; \quad GL(2, \mathbb{R}) \times S_5 \times \mathbb{Z}_7; \quad \dots$$

2.6 Homomorphism and Isomorphism

Motivation: Recall that in understanding D_4, one can look at how the vertices of the squares are permuted. This gives the following 'dictionary' between elements of D_4 and S_4:

D_4		S_4	D_4		S_4
e	$\leftrightarrow$	e	s	$\leftrightarrow$	$(2\,4)$
r	$\leftrightarrow$	$(1\,2\,3\,4)$	rs	$\leftrightarrow$	$(1\,2)(3\,4)$
r^2	$\leftrightarrow$	$(1\,3)(2\,4)$	r^2s	$\leftrightarrow$	$(1\,3)$
r^3	$\leftrightarrow$	$(1\,4\,3\,2)$	r^3s	$\leftrightarrow$	$(1\,4)(2\,3)$

To understand D_4, it is equally good to understand the 8 elements in S_4 in the above dictionary.

Definition 2.46 (Homomorphism & Isomorphism)**.** Let $(G, *), (H, \circledast)$ be groups. A *homomorphism* from G to H is a map $\phi : G \to H$ such that

$$\phi(g_1 * g_2) = \phi(g_1) \circledast \phi(g_2).$$

If ϕ is bijective, then ϕ is an *isomorphism.*

Example 2.47. Here is a long list of (non-)examples of group homomorphisms:

- $\phi : D_4 \to S_4$ given by $\phi(r) = (1\,2\,3\,4)$, $\phi(s) = (2\,4)$ and so on, as in the above dictionary. Then ϕ is an *injective* homomorphism. For instance,

  $$\phi(r^2s) = (1\ 3) = (1\ 3)(2\ 4)(2\ 4) = \phi(r^2)\phi(s)$$

- $\phi : \mathbb{Z}_3 \to S_4$ given by

  $$\phi([0]) = e, \quad \phi([1]) := (1\ 2\ 4), \quad \phi([2]) := (1\ 4\ 2),$$

  then ϕ is a homomorphism. For instance,

  $$\phi([1] + [1]) = \phi([2]) = (1\ 4\ 2) = (1\ 2\ 4) * (1\ 2\ 4) = \phi([1]) * \phi([1])$$

- Let $(G, *) = (\mathbb{R}^n, +)$ and $(H, \circledast) = (\mathbb{R}^m, +)$. Then any linear transformation

  $$T : \mathbb{R}^n \to \mathbb{R}^m$$

  is a group homomorphism, since

  $$T(x_1 + x_2) = T(x_1) + T(x_2)$$

- $\phi : (\mathbb{Z}^*_{15}, \times) \to (\mathbb{Z}_{15}, +)$ given by

  $$\phi([k]) := [k]$$

is **NOT** a homomorphism, since

$$\phi([2]\cdot[4]) = \phi([8]) = [8] \neq [6] = [2] + [4] = \phi(2) + \phi(4)$$

- $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ given by $\exp(a) := e^a$ is a homomorphism (here $\mathbb{R}_{>0}$ is the set of all positive real numbers), since:

  $$\exp(a+b) = e^{a+b} = e^a \cdot e^b = \phi(a)\cdot\phi(b)$$

  Indeed, it is an isomorphism since $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ is bijective.

- S_3 and $\mathbb{Z}_6$ both have 6 elements, but there are no bijective homomorphism $\phi : S_3 \to \mathbb{Z}_6$ (see below). Similarly, there are not bijective homomorphism from D_4 to $\mathbb{Z}_8$.

- $i : (\mathbb{Z}, +) \hookrightarrow (\mathbb{R}, +)$ defined by $i(a) := a$ for all $a \in \mathbb{Z}$ is a homomorphism. More generally, if $H \leq G$, then $i : (H, *) \hookrightarrow (G, *)$ is a homomorphism.

- $\pi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ with

  $$\pi(a) := [a]_n$$

  is a homomorphism, since

  $$\pi(a+b) = [a+b]_n = [a]_n + [b]_n = \pi(a) + \pi(b).$$

- $\det : GL(n, \mathbb{R}) \to (\mathbb{R}^*, \cdot)$ is a homomorpism, since

  $$\det(A\cdot B) = \det(A)\cdot\det(B).$$

- Let $\phi : S_n \to (\{\pm 1\}, \cdot)$ by

  $$\phi(\sigma) := \begin{cases} +1, & \text{if } \sigma \text{ is even} \\ -1, & \text{if } \sigma \text{ is odd} \end{cases}$$

  Then ϕ is a surjective homomorphism, i.e.

  $$\phi(\sigma\tau) = \phi(\sigma)\cdot\phi(\tau) \quad \forall \sigma, \tau \in S_n,$$

  since:

			$\phi(\sigma\tau)$		$\phi(\sigma)\phi(\tau)$
σ even,	τ even	$\Rightarrow \sigma\tau$ even	1	$=$	$1\cdot 1$
σ even,	τ odd	$\Rightarrow \sigma\tau$ odd	-1	$=$	$1\cdot(-1)$
σ odd,	τ even	$\Rightarrow \sigma\tau$ odd	-1	$=$	$(-1)\cdot 1$
σ odd,	τ odd	$\Rightarrow \sigma\tau$ even	1	$=$	$(-1)\cdot(-1)$

Proposition 2.48. *Let $(G, *), (H, \circledast)$ and $(K, \star)$ be groups. Then:*

(a) *If $\phi : G \to H, \psi : H \to K$ are homomorphism, then $\psi \circ \phi : G \to K$ is homomorphism*

(b) *If $\phi : G \to H$ is homomorphism, then $\phi(e_G) = e_H$, $\phi(a^{-1}) = (\phi(a))^{-1}$.*

(c) *If $\phi : G \cong H$ is isomorphism, then $\phi^{-1} : H \to G$ satisfies*

$$\phi^{-1}(h_1 \circledast h_2) = \phi^{-1}(h_1) * \phi^{-1}(h_2).$$

In other words, the inverse of isomorphism is an isomorphism.

Proof. (a) Since ϕ and ψ are homomorphisms, $\phi(g_1 * g_2) = \phi(g_1) \circledast \phi(g_2)$ and $\phi(h_1 \circledast h_2) = \phi(h_1) \star \phi(h_2)$. Hence we have:

$$\begin{aligned}(\psi \circ \phi)(g_1 * g_2) = \psi(\phi(g_1 * g_2)) &= \psi(\phi(g_1) \circledast \phi(g_2)) \\ &= \psi(\phi(g_1)) \star \psi(\phi(g_2)) \\ &= (\psi \circ \phi)(g_1) \star (\psi \circ \phi)(g_2).\end{aligned}$$

(b) Since $\phi(g) = \phi(e_G * g) = \phi(e_G) \circledast \phi(g)$, one has

$$\begin{aligned}\phi(g)(\phi(g))^{-1} &= \phi(e_G) \circledast (\phi(g) \circledast (\phi(g))^{-1}) \\ e_H &= \phi(e_G).\end{aligned}$$

Similarly, since $\phi(e_G) = \phi(a * a^{-1}) = \phi(a) \circledast \phi(a^{-1})$, therefore

$$e_H = \phi(a) \circledast \phi(a^{-1}) \Rightarrow \phi(a^{-1}) = (\phi(a))^{-1}$$

(c) Note that

$$\phi(\phi^{-1}(h_1 \circledast h_2)) = h_1 \circledast h_2 = (\phi \circ \phi^{-1}(h_1)) \circledast (\phi \circ \phi^{-1}(h_2)) = \phi(\phi^{-1}(h_1) * \phi^{-1}(h_2))$$

Since ϕ is bijective, one can apply ϕ^{-1} on both sides of the equation and get

$$\phi^{-1}(h_1 \circledast h_2) = \phi^{-1}(h_1) * \phi^{-1}(h_2).$$

□

Definition 2.49 (Kernel and Image)**.** Let $\phi : G \to H$ be a group homomorphism.

- The **kernel** of ϕ is:
$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}.$$

- The **image** of ϕ is:
$$\text{im } \phi := \phi(G) = \{\phi(g) \mid g \in G\}.$$

Example 2.50. • Let A be an $m \times n$ real matrix, which defines a linear transformation A :

$(\mathbb{R}^n, +) \to (\mathbb{R}^m, +)$. Then

$$\ker(A) = \{\mathbf{v} \in \mathbb{R}^n \mid A(\mathbf{v}) = \mathbf{0}_{\mathbb{R}^m}\} = \text{Null space of } A.$$

$$\operatorname{im}(A) = \{A(\mathbf{v}) \in \mathbb{R}^m \mid \mathbf{v} \in \mathbb{R}^n\} = \text{Column space of } A.$$

- Let $\pi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$. Then

$$\ker(\pi) = \{\text{multiples of } n\} = \langle n \rangle, \quad \operatorname{im}(\pi) = (\mathbb{Z}_n, +).$$

- Let $\det : GL(n, \mathbb{R}) \to (\mathbb{R}^*, \cdot)$. Then

$$\ker(\det) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\} =: SL(n, \mathbb{R}), \quad \operatorname{im}(\det) = \mathbb{R}^*.$$

Proposition 2.51. *(a) $\ker\phi \leq G$, im $\phi \leq H$ are subgroups of G and H respectively.*

(b) ϕ is an isomorphism if and only if $\ker\phi = \{e_G\}$ and im $\phi = H$.

(c) If G is cyclic / abelian, then $\phi(G)$ is cyclic / abelian.

Proof. (a) $\forall g_1, g_2 \in \ker\phi$:

(i) $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e_H \cdot e_H = e_H \Rightarrow g_1 g_2 \in \ker\phi$

(ii) $\phi(g_1^{-1}) = (\phi(g_1))^{-1} \Rightarrow g_1^{-1} \in \ker\phi$

(b) Skipped. ($\ker\phi = \{e_G\} \iff \phi$ is injective; im $\phi = H \iff \phi$ is surjective)

(c) If G is abelian, i.e.: $ab = ba$ $\forall a, b \in G$. Then $\forall \phi(a), \phi(b) \in \phi(G)$:

$$\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$$

If $G = \langle g \rangle$ is cyclic, then for all $\phi(a) \in \phi(G)$, $a = g^k$ for some $k \in \mathbb{Z}$, and:

$$\phi(a) = \phi(g^k) = (\phi(g))^k \in \langle \phi(g) \rangle$$

(when $k < 0$ is negative, Proposition 2.48(b) is needed to prove the second equality). Therefore, $\phi(G) \subseteq \langle \phi(g) \rangle$. Meanwhile, $\langle \phi(g) \rangle \subseteq \phi(G)$ since $\phi(g) \in \phi(G)$. Therefore, $\phi(G) = \langle \phi(g) \rangle$ is cyclic. □

Example 2.52.

- $S_3, \mathbb{Z}_6$ both have 6 elements. But $S_3 \ncong \mathbb{Z}_6$ – Suppose by contrary that

$$\phi : \mathbb{Z}_6 \xrightarrow{\cong} S_3.$$

Then $\phi(\mathbb{Z}_6) = S_3$ and hence $\phi(\mathbb{Z}_6)$ is abelian by the above proposition. However, we already know that S_3 is not abelian, so this is impossible.

- Similarly, $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. (Hint: Suppose on contrary, $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ and study $\phi(x)$)

From now on, we will classify groups up to isomorphism, i.e. we will not distinguish $A_3 \cong \mathbb{Z}_3$ but $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are different!

Theorem 2.53 (Classification of cyclic groups)**.** *Let $G = \langle g \rangle$ be a cyclic group. Then:*

(a) If $|G| = \infty$, then $G \cong (\mathbb{Z}, +)$.

(b) If $|G| = n < \infty$, then $G \cong (\mathbb{Z}_n, +)$.

Proof. (a) Consider the map $\phi : \mathbb{Z} \to G = \langle g$ by $\phi(a) := g^a$. Then

$$\phi(a+b) = g^{a+b} = g^a g^b = \phi(a)\phi(b).$$

Therefore, ϕ is a surjective homomorphism. Suppose on contrary that ϕ is **NOT** injective, i.e. there exists $m > n$ such that $\phi(m) = \phi(n)$. Then:

$$\phi(m) = \phi(n) \ \Rightarrow\ g^m = g^n \Rightarrow\ g^{m-n} = e \Rightarrow\ \operatorname{ord}(g) \le m - n$$

(Exercise: $g^k = e \ \Leftrightarrow\ \operatorname{ord}(g) \mid k$). Therefore, $\operatorname{ord}(g) < \infty$ and hence $|G| = |\langle g \rangle| = |\operatorname{ord}(g)| < \infty$ (c.f. Proposition 2.24), contradicting $|G| = \infty$. Therefore, ϕ must be injective, and is an isomorphism between $\mathbb{Z} \cong G$.

(b) Let $|G| = |\langle g \rangle| = n < \infty$. Then $\operatorname{ord}(g) = n$ by Proposition 2.24 again, with

$$G = \{e = g^0, g^1, \dots, g^{n-1}\}.$$

Consider $\psi : G \to \mathbb{Z}_n$ with $\psi(g^i) := i$ for $0 \le i \le n-1$. Then ψ is a surjective homomorphism, since

$$\psi(g^a g^b) = \psi(g^{a+b}) = a + b = \psi(g^a) + \psi(g^b).$$

Since $|G| = |\mathbb{Z}_n| = n$, then any surjective map is also injective. Therefore, $\psi : G \overset{\cong}{\to} \mathbb{Z}_n$ is bijective. □

2.7 Lagrange's Theorem

To begin this section, recall that an equivalence relation $\sim$ on a set S partitions the set into disjoint equivalence classes. That is, $S = \bigsqcup_{\alpha \in I} C_\alpha$, where C_α are the equivalence classes.

Example 2.54.

- Let $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. Define $a \sim b$ iff $a \equiv b \pmod 3$. This is an equivalence relation where the classes are

$$C_0 = 0 + 3\mathbb{Z},\ C_1 = 1 + 3\mathbb{Z}, \text{ and } C_2 = 2 + 3\mathbb{Z}.$$

- Let $G = GL(n, \mathbb{R})$ and $H = SL(n, \mathbb{R})$. Define $A \sim B$ iff $\det(A) = \det(B)$. The equivalence classes are $C_\alpha = \{B \in GL(n, \mathbb{R}) \mid \det(B) = \alpha\}$ for $\alpha \in \mathbb{R}^*$.

Definition 2.55. Let G be a group and $H \leq G$ be a subgroup. We define a relation on G by

$$a \sim b \text{ if and only if } a^{-1}b \in H.$$

Proposition 2.56. *The relation $a \sim b \iff a^{-1}b \in H$ is an equivalence relation.*

Proof. (i) **Reflexive:** $a \sim a$ since $a^{-1}a = e \in H$.

(ii) **Symmetric:** If $a \sim b$, then $a^{-1}b \in H$. Since H is a group, $(a^{-1}b)^{-1} = b^{-1}a \in H$, so $b \sim a$.

(iii) **Transitive:** If $a \sim b$ and $b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$. Thus $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$, so $a \sim c$.

□

Definition 2.57 (Cosets)**.** Let G be a group and $H \leq G$.

- The **left coset** of H with representative $a \in G$ is the set:

$$aH := \{ah \mid h \in H\}$$

- The **right coset** of H with representative $a \in G$ is the set:

$$Ha := \{ha \mid h \in H\}$$

Example 2.58.

- Let $G = \mathbb{Z}, H = 3\mathbb{Z}$. The left cosets (using additive notation) are $0 + 3\mathbb{Z}$, $1 + 3\mathbb{Z}$, and $2 + 3\mathbb{Z}$.
- Let $G = S_3, H = \langle (1\,2) \rangle = \{e, (1\,2)\}$. The left cosets are:

$$\begin{aligned} eH &= \{e, (1\,2)\} \\ (1\,2\,3)H &= \{(1\,2\,3), (1\,3)\} \\ (1\,3\,2)H &= \{(1\,3\,2), (2\,3)\} \end{aligned}$$

- Let $G = D_4, H = \langle s \rangle = \{e, s\}$. The distinct left cosets are eH, rH, r^2H, and r^3H. Each coset contains 2 elements.

Remark 2.59. The left coset aH is precisely the equivalence classes of the equivalence relation

$$a \sim_L b \iff a^{-1}b \in H.$$

Indeed, one can easily check that

$$aH = \{ah \mid h \in H\} = \{b \in G \mid b = ah \text{ for } h \in H\} = \{b \in G \mid a^{-1}b = h \in H\} = \{b \in G \mid a \sim_L b\}.$$

Similarly, the right coset Ha is the equivalence class of the relation $\sim_R$ defined by

$$a \sim_R b \iff ab^{-1} \in H.$$

Theorem 2.60 (Lagrange's Theorem)**.** *Let G be a finite group and $H \leq G$. Then the order of H divides the order of G. Specifically:*

$$|G| = [G : H] \cdot |H|$$

where $[G : H]$ is the ***index*** *of H in G (the number of distinct left cosets).*

Proof. The left cosets of H partition G. Let $m = [G : H]$. We can write G as a disjoint union:

$$G = a_1 H \sqcup a_2 H \sqcup \cdots \sqcup a_m H$$

where $a_i H \cap a_j H = \emptyset$ for $i \neq j$. We claim that every coset has the same size, namely

$$|a_i H| = |eH| = |H|.$$

To see so, define a map $f : H \to a_i H$ by $f(h) = a_i h$. This map is surjective by the definition of a coset. It is also injective because $a_i h_1 = a_i h_2 \implies h_1 = h_2$ by left cancellation. Thus, $|a_i H| = |H|$ for all i. It follows that:

$$|G| = \sum_{i=1}^{m} |a_i H| = \sum_{i=1}^{m} |H| = m|H|.$$

In other words, $|G| = [G : H]|H|$ as required. □

Corollary 2.61. *Let G be a finite group. For any $g \in G$, $\operatorname{ord}(g)$ divides $|G|$.*

Proof. Let $H = \langle g \rangle$. By definition, $|H| = \operatorname{ord}(g)$. By Lagrange's Theorem, $|H|$ divides $|G|$. □

Example 2.62 (Fermat's Little Theorem)**.** Let p be a prime. For any $a \in \mathbb{Z}$ such that $p \nmid a$, then

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

Proof. Consider the group $G = \mathbb{Z}_p^*$, which has order $p - 1$. For any $[a] \in G$, the order d of $[a]$ divides $p - 1$. Thus $p - 1 = dk$ for some integer k. Then:

$$[a]^{p-1} = ([a]^d)^k = [1]^k = [1]$$

and hence $a^{p-1} \equiv 1 \pmod{p}$. □

Remark 2.63. More generally, for the group $G = \mathbb{Z}_n^*$, the order is given by Euler's totient function $\phi(n)$. Thus, for any a coprime to n, $a^{\phi(n)} \equiv 1 \pmod{n}$.

2.8 Group Action

In this section, we will apply Lagrange's Theorem to go deeper into studying the symmetry of any set X by defining an 'action' of a group G on X. Here is the definition:

Definition 2.64. Let G be a group and X be a set. A **(left) group action** of G on X is a function

$$\phi : G \times X \to X,$$

often denoted by $\phi(g, x) = g \cdot x$, such that the following are satisfied for all $x \in X$ and $g_1, g_2 \in G$:

1. (Identity) $e \cdot x = x$, where e is the identity element of G.
2. (Compatibility) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

A more intuitive way to understand the group action of G on X is to define

$$\sigma_g : X \to X$$

by $\sigma_g(x) := g \cdot x$. In other words, each $g \in G$ defines how X is move around.

Proposition 2.65. *Let $\phi : G \times X \to X$ be a group action. Then the map*

$$\sigma : G \to \mathrm{Aut}(X), \qquad g \mapsto \sigma_g$$

is a well-defined homomorphism.

Remark 2.66. For any set X, $\mathrm{Aut}(X)$ is defined as:

$$\mathrm{Aut}(X) := \{f : X \to X \mid f \text{ is bijective}\}.$$

If there are extra structure on X, we often impose more conditions on the bijective map in the definition of $\mathrm{Aut}(X)$. For instance, if $X = G$ is a group, $\mathrm{Aut}(G)$ is usually understood as:

$$\mathrm{Aut}(G)\ (= \mathrm{Aut}_G(G)) := \{\phi : G \to G \mid \phi \text{ is a bijective homomorphism}\}.$$

Proof. To see σ is well-defined, one needs to show $\sigma_g \in \mathrm{Aut}(X)$ is bijective. Indeed, by the identity and compatibility axioms, σ_g has an inverse $\sigma_{g^{-1}}$, making σ_g a bijection. Thus $\sigma_g \in \mathrm{Aut}(X)$. As for σ being a homomorphism, one applies compatibility axiom and get

$$\sigma_{g_1 g_2}(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \sigma_{g_1}(\sigma_{g_2}(x))$$

for all $x \in X$. Therefore,

$$\sigma(g_1 g_2) := \sigma_{g_1 g_2} = \sigma_{g_1} \sigma_{g_2} =: \sigma(g_1)\sigma(g_2),$$

i.e. σ is a homomorphism. □

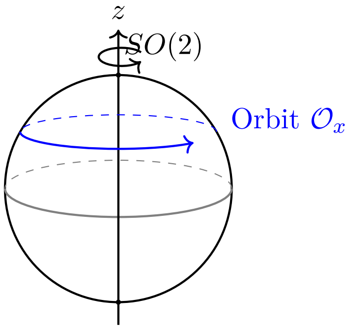
From now on, we will use

$$\sigma_g(x) \longleftrightarrow g \cdot x$$

interchangeably to denote the action of $g \in G$ on $x \in X$.

Example 2.67.

- By definition of symmetric group, one automatically has a bijective map
$$\sigma : S_n \to \mathrm{Aut}(X_n),$$
which is an S_n-action on $X_n := \{1, 2, \ldots, n\}$.
- Similarly, one also has a D_n-action
$$\gamma : D_n \to \mathrm{Aut}(X_n).$$
- Let $G = SO(2) := \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \,\middle|\, \theta \in \mathbb{R} \right\}$ be the group of rotations on $\mathbb{R}^2$. Define a group action
$$\sigma : SO(2) \to \mathrm{Aut}(S^2)$$
(where $S^2 = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\} \subseteq \mathbb{R}^3$ is the unit sphere) by:
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \mapsto \quad R_\theta : S^2 \to S^2, \quad \text{where } R_\theta(\mathbf{x}) := \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \mathbf{x}$$
for $\mathbf{x} \in S^2$. So the $SO(2)$-action is precisely the rotation on the sphere along the polar axis:



Definition 2.68 (Orbit and Stabilizer)**.** Let G act on a set X.

- The **orbit** of x, denoted by $G \cdot x$ or $\mathcal{O}_x$, is the subset of X containing all elements that x can be moved to by G:
$$\mathcal{O}_x = \{g \cdot x \mid g \in G\} \subseteq X$$
- The **stabilizer** of x, denoted by G_x or $\mathrm{Stab}(x)$, is the set of elements in G that fix x:
$$G_x = \{g \in G \mid g \cdot x = x\} \subseteq G$$

Example 2.69. Note that for $x, y \in X$,
$$x \sim y \quad \Leftrightarrow \quad x, y \text{ are in the same orbit}$$

is an equivalence relation (Exercise). Therefore, the orbits form a partition of the set X. For instance, an orbit of $SO(2)$-action on S^2 in the above example is a *latitude line* on the sphere (marked in blue). Obviously, lines of different latitudes give a partition of S^2.

As for the stabilizer, one can check that G_x is always a subgroup of G (Exercise). Therefore, if G is finite, one always has

$$|G_x| \mid |G|$$

by Lagrange's theorem. Indeed, one has a more refined result in terms of the size of the orbit:

Theorem 2.70 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group acting on a set X. For any $x \in X$:*

$$|G| = |G_x| \cdot |\mathcal{O}_x|$$

Equivalently, the size of the orbit is the index of the stabilizer: $|\mathcal{O}_x| = [G : G_x]$.

Proof. To prove $|\mathcal{O}_x| = [G : G_x]$, we will construct a bijection f between the set of all left cosets of G_x in G and the elements of the orbit $\mathcal{O}_x$. To do so, let $G/G_x = \{gG_x \mid g \in G\}$ be the set of left cosets, and define:

$$f : G/G_x \to \mathcal{O}_x \qquad f(gG_x) := g \cdot x$$

1. Well-defined: We must ensure that if two cosets are equal, their images are equal. Suppose $g_1G_x = g_2G_x$. Then $g_2^{-1}g_1 \in G_x$. By the definition of the stabilizer:

$$\begin{aligned} (g_2^{-1}g_1) \cdot x &= x \\ g_2 \cdot (g_2^{-1}g_1 \cdot x) &= g_2 \cdot x \\ (g_2g_2^{-1}g_1) \cdot x &= g_2 \cdot x \\ g_1 \cdot x &= g_2 \cdot x \end{aligned}$$

Thus $f(g_1G_x) = f(g_2G_x)$, so f is well-defined.
2. Injective: Suppose $f(g_1G_x) = f(g_2G_x)$. Then:

$$\begin{aligned} g_1 \cdot x &= g_2 \cdot x \\ g_2^{-1} \cdot (g_1 \cdot x) &= g_2^{-1} \cdot (g_2 \cdot x) \\ (g_2^{-1}g_1) \cdot x &= e \cdot x = x \end{aligned}$$

This implies $g_2^{-1}g_1 \in G_x \;\Leftrightarrow\; g_1G_x = g_2G_x$. Thus f is injective.
3. Surjective: By the definition of the orbit $\mathcal{O}_x$, any element $y \in \mathcal{O}_x$ is of the form $g \cdot x$ for some $g \in G$. Then $y = f(gG_x)$, so f is surjective.

Since f is a bijection, the number of elements in the orbit is equal to the number of left cosets:

$$|\mathcal{O}_x| = |G/G_x| = [G : G_x]$$

By Lagrange's Theorem, we know that $[G : G_x] = \frac{|G|}{|G_x|}$. Therefore:

$$|\mathcal{O}_x| = \frac{|G|}{|G_x|} \implies |G| = |\mathcal{O}_x| \cdot |G_x|.$$

□

Example 2.71. Let G be the group of rotational symmetries of the tetrahedron. Then G defines an action on the 4 faces of the tetrahedron. Suppose x be a specific face of the tetrahedron, then:

- There are 4 faces, and any face can be rotated to any other face, so $|\mathcal{O}_x| = 4$.
- The rotations fixing face x are the 3 rotations (0, 120, 240 degrees) around the axis through the center of that face. So $|G_x| = 3$.

By the Orbit-Stabilizer Theorem, one has $|G| = 4 \times 3 = 12$. But of course we already knew that the rotational symmetries of a tetrahedron is isomorphic to A_4, the alternating group. So we have re-confirmed that $|A_4| = 12$.

Example 2.72. Let G be any finite group, and $X = G$. Then G act on itself by conjugation:

$$g \cdot x = gxg^{-1}.$$

In such a case:

- The orbit $\mathcal{O}_x$ is the **conjugacy class** of x.
- The stabilizer G_x is the **centralizer** $Z_G(x) := \{g \in G \mid gx = xg\}$.

By the orbit-stabilizer theorem, the size of a conjugacy class must divide the order of the group. Also, it can be computed by computing the centralizer group $Z_G(x)$ (see Homework).

We end this section with Burnside's Lemma, which provides a way to count the number of distinct orbits in X for any finite group action.

Theorem 2.73 (**Burnside's Lemma**). *Let G be a finite group acting on a finite set X. Then the number of orbits, denoted $|X/G| := |\{\mathcal{O}_x \mid x \in X\}|$, is the average number of points fixed by the elements of G:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

where $X^g = \{x \in X \mid g \cdot x = x\}$ be the set of points fixed by g.

Proof. Consider the set of all fixed pairs $S = \{(g, x) \in G \times X \mid g \cdot x = x\}$. We will count the number of elements in S in two different ways.

Method 1: Summing over G For a fixed $g \in G$, the number of elements x such that $(g, x) \in S$ is exactly $|X^g|$. Therefore:

$$|S| = \sum_{g \in G} |X^g|$$

Method 2: Summing over X For a fixed $x \in X$, the number of elements g such that $(g, x) \in S$ is exactly the size of the stabilizer G_x. Therefore:

$$|S| = \sum_{x \in X} |G_x|$$

Therefore, one has:

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|$$

Let $\Omega_1, \Omega_2, \ldots, \Omega_k$ be the distinct orbits of X (note that $k = |X/G|$). Then for any $x \in X$, $x \in \Omega_{i_x}$ for a unique $1 \leq i_x \leq k$. Therefore:

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}_x|} = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}_x|} = |G| \sum_{i=1}^{k} \sum_{x \in \Omega_i} \frac{1}{|\Omega_i|} \qquad (*)$$

where the second $=$ comes from the Orbit-Stabilizer Theorem.

For any specific orbit Ω_i, the inner sum $\sum_{x \in \Omega_i} \frac{1}{|\Omega_i|}$ is just adding the value $\frac{1}{|\Omega_i|}$ to itself $|\Omega_i|$ times:

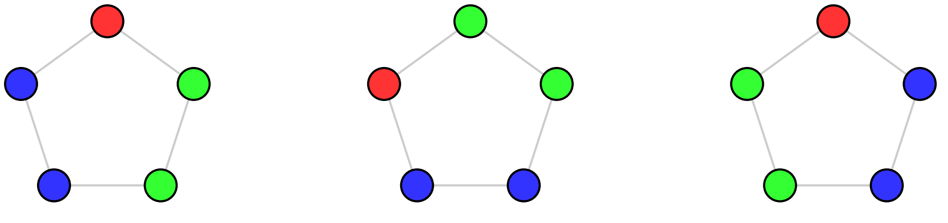
$$\sum_{x \in \Omega_i} \frac{1}{|\Omega_i|} = |\Omega_i| \cdot \frac{1}{|\Omega_i|} = 1$$

Therefore, Equation $(*)$ reduces to

$$\sum_{g \in G} |X^g| = |G| \sum_{i=1}^{k} 1 = |G| \cdot k = |G| \cdot |X/G|$$

and consequently $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$. □

Example 2.74. To see how many distinct ways can the vertices of a regular pentagon be colored using 3 colors up rotations and reflections. For example, the following colorings are treated the same:



Original (x) **Rotated** $(r \cdot x)$ **Reflected** $(s \cdot x)$

since the second can be obtained from the first by rotation, and the third can be obtained from the first by reflection.

Consider the action of $G = D_5$ on the set X of 5 vertices each with three different possible colors. Therefore, there are

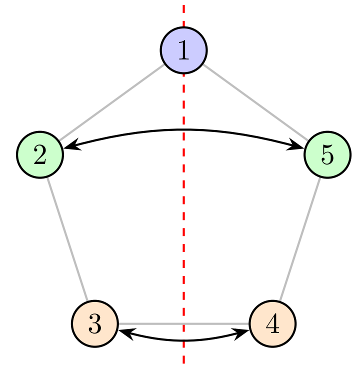
$$|X| = 3 \times 3 \times 3 \times 3 \times 3 = 3^5 = 243$$

elements in X. The three diagrams above are *in the same orbit* under our action. So we need to calculate $|X/G|$ – the *distinct* orbits of X under the action of G.

To do so, we need to calculate X^g for each $g \in D_5$. A coloring $x \in X$ is fixed by $g \in D_5$ if all vertices in the same cycle of the permutation g have the same color. If g has ℓ cycles, there are 3^ℓ fixed colorings. Therefore, one has

Element Type	**No. of Elements**	**Cycle Structure**	**No. of Cycles**	$\lvert X^g\rvert$
Identity	1	$(1)(2)(3)(4)(5)$	5	$3^5 = 243$
Rotations	4	$(1\,2\,3\,4\,5)$	1	$3^1 = 3$
Reflections	5	$(1)(2\,5)(3\,4)$	3	$3^3 = 27$

Here is an example of the number of possible colorings for a reflection $s \in D_5$ along the axis passing through vertex 1. Among all the possible 3^5 colorings of the five vertices, the colorings such that s fixes the coloring is of the form:



Cycles of the Reflection:

- **Cycle 1:** $\{1\}$
- **Cycle 2:** $\{2, 5\}$
- **Cycle 3:** $\{3, 4\}$

Total independent choices of X^s:
$3 \times 3 \times 3 = 3^3$

By Burnside Lemma, the number of distinct colorings $|X/G|$ is given by:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{10} (1 \cdot 243 + 4 \cdot 3 + 5 \cdot 27) = \frac{390}{10} = 39$$

There are **39** distinct ways to color the vertices of a regular pentagon with 3 colors under dihedral symmetry.

2.9 Normal Subgroups

Recall that for a subgroup $H \leq G$, the group G can be partitioned into left cosets $G = \bigsqcup_i \; g_i H$ or right cosets $G = \bigsqcup_j \; H b_j$. A natural question is whether these partitions are identical—that is, whether $gH = Hg$ for all $g \in G$.

In general, the answer is no. Consider $G = S_3$ and $H = \langle (1\,2) \rangle$:

$$(1\,3)H = \{(1\,3), (1\,3)(1\,2)\} = \{(1\,3), (1\,2\,3)\}$$
$$H(1\,3) = \{(1\,3), (1\,2)(1\,3)\} = \{(1\,3), (1\,3\,2)\}$$

Since $(1\,3)H \neq H(1\,3)$, we look for subgroups that satisfy this property.

Definition 2.75 (Normal Subgroup)**.** A subgroup $H \leq G$ is called a **normal subgroup** if $gH = Hg$ for all $g \in G$. We denote this by $H \triangleleft G$.

Example 2.76.

- $A_n \triangleleft S_n$ for all n.
- If G is abelian, then any subgroup $H \leq G$ is normal. For any $g \in G$ and $h \in H$, $gh = hg$, so $gH = Hg$.
- $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$. Let $A \in GL(n, \mathbb{R})$ and $h \in SL(n, \mathbb{R})$. Then:

  $$\det(AhA^{-1}) = \det(A)\det(h)\det(A)^{-1} = \det(A) \cdot 1 \cdot \frac{1}{\det(A)} = 1$$

  Thus $AhA^{-1} \in SL(n, \mathbb{R})$, which implies $AHA^{-1} = H$, or $AH = HA$.
- If $H \leq G$ and $[G : H] = 2$, then $H \triangleleft G$. In this case, G is the disjoint union $H \sqcup gH$ and also $H \sqcup Hg$ for any $g \notin H$. It follows that $gH = G \setminus H = Hg$.
- The trivial subgroup $\{e\}$ and the group G itself are always normal in G.

Theorem 2.77. *Let $H \leq G$ be a subgroup. The following are equivalent:*

(i) $H \triangleleft G$.

(ii) $ghg^{-1} \in H$ *for all* $h \in H$ *and* $g \in G$.

(iii) $gHg^{-1} = H$ *for all* $g \in G$.

Proof.

- **(i) ⇒ (ii):** By assumption, $gH = Hg$. Thus for any $h \in H$, $gh \in Hg$, so $gh = h'g$ for some $h' \in H$. Multiplying by g^{-1} on the right gives $ghg^{-1} = h' \in H$.
- **(ii) ⇒ (iii):** Condition (ii) implies $gHg^{-1} \subseteq H$ for all $g \in G$. Applying this to g^{-1}, we have $g^{-1}H(g^{-1})^{-1} \subseteq H \Rightarrow g^{-1}Hg \subseteq H$. Multiplying by g on the left and g^{-1} on the right gives $H \subseteq gHg^{-1}$. Thus $gHg^{-1} = H$.
- **(iii) ⇒ (i):** If $gHg^{-1} = H$, then multiplying by g on the right gives $(gHg^{-1})g = Hg$, so $gH = Hg$.

□

Corollary 2.78. *Let $\phi : G \to H$ be a group homomorphism. Then* $\ker \phi \triangleleft G$.

Proof. Let $k \in \ker \phi$ and $g \in G$. We check the conjugation condition:

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_H(\phi(g))^{-1} = \phi(g)(\phi(g))^{-1} = e_H$$

Since $\phi(gkg^{-1}) = e_H$, we have $gkg^{-1} \in \ker\phi$. By the previous theorem, $\ker\phi \triangleleft G$. □

Example 2.79.

- Consider $\det : GL(n,\mathbb{R}) \to \mathbb{R}^*$. Since $\ker(\det) = SL(n,\mathbb{R})$, it follows that $SL(n,\mathbb{R}) \triangleleft GL(n,\mathbb{R})$.
- Consider $\psi : S_n \to (\{\pm 1\}, \cdot)$ given by the parity of the permutation. Since $\ker\psi = A_n$, it follows that $A_n \triangleleft S_n$.

2.10 Quotient Groups

Let $H \triangleleft G$ be a normal subgroup. We want to define a group structure on the set of left cosets $G/H := \{gH \mid g \in G\}$. To do this, we must ensure that the natural multiplication of cosets is independent of the choice of representative.

Definition 2.80 (Quotient Group)**.** Let G be a group and $H \triangleleft G$. The **quotient group** G/H is the set of left cosets $\{gH \mid g \in G\}$ equipped with the binary operation:

$$(aH) * (bH) := (ab)H$$

Remark 2.81. Since many different elements can represent the same coset (i.e., $a_1H = a_2H$ even if $a_1 \neq a_2$), we must verify that the operation is well-defined.

Proposition 2.82. *If $H \triangleleft G$, the operation $(aH) * (bH) = (ab)H$ is well-defined and makes G/H into a group.*

Proof. First, we show the operation is **well-defined**. Suppose $aH = a'H$ and $bH = b'H$. This implies $h_a := a^{-1}a' \in H$ and $h_b := b^{-1}b' \in H$. We compute:

$$a'b' = (ah_a)(bh_b) = ab(b^{-1}h_ab)h_b$$

Since $H \triangleleft G$, the element $h_3 := b^{-1}h_ab$ is in H. Thus $a'b' = ab(h_3h_b)$. Since $h_3h_b \in H$, we have $a'b' \in (ab)H$, so $(a'b')H = (ab)H$.

Next, we check the **group axioms**:

1. **Associativity:** $((aH)(bH))(cH) = (ab)H(cH) = (abc)H = aH(bc)H = (aH)((bH)(cH))$.
2. **Identity:** The coset $eH = H$ serves as the identity since $(aH)(eH) = (ae)H = aH$.
3. **Inverses:** The inverse of aH is $a^{-1}H$, since $(aH)(a^{-1}H) = (aa^{-1})H = eH$.

□

Example 2.83.

- Let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Since G is abelian, H is normal. The quotient group is:

$$G/H = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

The operation is $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$. This group is isomorphic to $(\mathbb{Z}_n, +)$. We often write $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

- Since $A_n \triangleleft S_n$ and $|S_n/A_n| = |S_n|/|A_n| = 2$, the quotient group S_n/A_n is a group of order 2. Any group of order 2 is isomorphic to $\mathbb{Z}_2$, so $S_n/A_n \cong \mathbb{Z}_2$.
- Since $SL(n,\mathbb{R}) \triangleleft GL(n,\mathbb{R})$, we can form the quotient group. Each coset is of the form:

$$A \cdot SL(n,\mathbb{R}) = \{B \in GL(n,\mathbb{R}) \mid \det(B) = \det(A)\}$$

  The multiplication of cosets corresponds to the multiplication of their determinants: $\det(AB) = \det(A)\det(B)$. Thus, $GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong (\mathbb{R}^*, \times)$.
- Let $K = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \triangleleft S_4$. The quotient group S_4/K has order $24/4 = 6$. It can be shown that $S_4/K \cong S_3$.

The construction of quotient groups is a powerful tool in group theory:

- **Construction:** It allows us to construct new groups from existing ones (e.g., constructing $\mathbb{Z}_n$ from $\mathbb{Z}$).
- **Cauchy's Theorem:** If G is a finite group and p is a prime dividing $|G|$, then G contains an element of order p. Quotient groups are used in the inductive proof of this theorem.
- **Classification:** They are essential for the classification of finite groups and understanding group extensions.

Theorem 2.84 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a group homomorphism. Then:*

$$G/\ker\phi \cong \text{im }\phi$$

Example 2.85.

- Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $\phi(a) = [a]_n$. Then $\ker\phi = n\mathbb{Z}$ and $\text{im }\phi = \mathbb{Z}_n$. By the First Isomorphism Theorem, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.
- Let $\det : GL(n,\mathbb{R}) \to \mathbb{R}^*$ be the determinant map. Then $\ker(\det) = SL(n,\mathbb{R})$ and $\text{im}(\det) = \mathbb{R}^*$. Thus, $GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R}^*$.
- Define $\phi : \mathbb{R} \to GL(2,\mathbb{R})$ by $\phi(x) = \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}$. This is a homomorphism where $\ker\phi = 2\pi\mathbb{Z}$ and the image is the special orthogonal group $SO(2)$. Hence, $\mathbb{R}/2\pi\mathbb{Z} \cong SO(2)$.

Proof. Define a map

$$\Psi : G/\ker\phi \to \text{im }\phi$$

by $\Psi(g\ker\phi) := \phi(g)$. We verify the following properties:

1. **Ψ is well-defined and injective:** Let $a, b \in G$. Then:

$$\begin{aligned} a \ker\phi = b \ker\phi &\iff a^{-1}b \in \ker\phi \\ &\iff \phi(a^{-1}b) = e_H \\ &\iff \phi(a)^{-1}\phi(b) = e_H \\ &\iff \phi(a) = \phi(b) \\ &\iff \Psi(a\ker\phi) = \Psi(b\ker\phi). \end{aligned}$$

   Reading this from left to right shows Ψ is well-defined; reading from right to left shows Ψ is injective.

2. **Ψ is a homomorphism:** For any $a, b \in G$:

$$\begin{aligned} \Psi((a\ker\phi)(b\ker\phi)) &= \Psi(ab\ker\phi) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= \Psi(a\ker\phi)\Psi(b\ker\phi). \end{aligned}$$

3. **Ψ is surjective:** By definition, im $\phi = \{\phi(g) \mid g \in G\}$. Since $\Psi(g\ker\phi) = \phi(g)$, every element in the image of ϕ has a preimage under Ψ.

Since Ψ is a bijective homomorphism, $G/\ker\phi \cong$ im ϕ. □

We end this section with the notion of simple groups. It will play a big role in the Galois theory course (MAT 5210).

Definition 2.86 (Simple Group)**.** A group G is called **simple** if G has no normal subgroups other than the trivial subgroup $\{e\}$ and the group G itself.

Remark 2.87. The concept of simple groups is analogous to prime numbers in arithmetic. If a group G is **not** simple, there exists a proper normal subgroup $N \lhd G$. This allows us to "decompose" G into two smaller groups: the normal subgroup N and the quotient group G/N, which can then be studied individually.

However, it is important to note that if G is not simple with $N \lhd G$, it is **not** necessarily isomorphic to the direct product $N \times (G/N)$ (Exercise: Find one such example of N and G).

Example 2.88.
- The symmetric group S_n is **not** simple for $n \geq 3$ because the alternating group A_n is a proper normal subgroup ($A_n \lhd S_n$). We can analyze S_n via A_n and the quotient $S_n/A_n \cong \mathbb{Z}_2$, but $S_n \ncong A_n \times \mathbb{Z}_2$ for $n \geq 3$.
- The alternating group A_4 is **not** simple because the Klein four-group

$$K = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

is a normal subgroup of A_4.

- The alternating group A_n is simple for all $n \geq 5$ (Homework). This result is a cornerstone of Galois Theory, as it implies that there is no general formula using radicals to solve polynomial equations of degree 5 or higher.

2.11 Fundamental Theorem of Finite Abelian Groups

We will conclude our study of groups by giving a classification of all finite abelian groups up to isomorphism. Here are some initial observations:

(1) $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ is abelian.

(2) G and H are abelian if and only if $G \times H$ is abelian.

(3) If $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Theorem 2.89. *All finite abelian groups are of the form $G \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$ where $p_1 \leq \cdots \leq p_k$ are primes and $a_i \in \mathbb{N} \setminus \{0\}$.*

The proof consists of two main steps:

- **Step 1:** If $|G| = q_1^{a_1} \dots q_r^{a_r}$ for distinct primes q_i, then $G \cong G_1 \times \cdots \times G_r$ where $|G_i| = q_i^{a_i}$.
- **Step 2:** If $|G| = q^b$, then $G \cong \mathbb{Z}_{q^{b_1}} \times \cdots \times \mathbb{Z}_{q^{b_r}}$ with $\sum b_j = b$.

Proof of Step 1 : We only deal with the case when $r = 2$, and the general case follows by repeatedly using this case.

Suppose $|G| = p^a q^b$ for distinct primes p, q. Let $m = p^a$ and $n = q^b$. We want to show $G \cong G_1 \times G_2$ with $|G_1| = m$ and $|G_2| = n$. Let

$$G^m := \{g^m \mid g \in G\}, \quad G^n := \{g^n \mid g \in G\}.$$

- **Claim 1 -** $G^m \cap G^n = \{e\}$:

  Suppose $x \in G^m \cap G^n$. Then $x = g^m = h^n$. By Lagrange's Theorem,

  $$x^n = g^{mn} = e \qquad x^m = h^{nm} = e.$$

  Since $\gcd(m, n) = 1$, there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha m + \beta n = 1$ by Bezout's Theorem. Then

  $$x^1 = x^{\alpha m + \beta n} = (x^m)^\alpha (x^n)^\beta = e \cdot e = e.$$

- **Claim 2 -** $\phi : G^m \times G^n \to G$ given by $\phi(g^m, h^n) := g^m (h^n)^{-1}$ is an isomorphism:

  Note that ϕ is a homomorphism because G is abelian. For injectivity, if $g^m (h^n)^{-1} = e$, then $g^m = h^n \in G^m \cap G^n = \{e\}$, so $\ker \phi = \{(e, e)\}$. For surjectivity, for any $y \in G$, $y = y^{\alpha m + \beta n} = (y^\alpha)^m (y^\beta)^n = \phi((y^\alpha)^m, (y^{-\beta})^n)$.

- **Claim 3 -** $|G^m| = n$ and $|G^n| = m$:

  Suppose $q \mid |G^n|$. By Cauchy's Theorem (proved in Homework), there exists $x = g^n \in G^n$ of order q. By Bezout's Theorem, $\alpha q + \beta m = 1$ for some $\alpha, \beta \in \mathbb{Z}$. Then

  $$x = x^{\alpha q+\beta m} = (x^q)^\alpha (x^m)^\beta = e \cdot (g^{nm})^\beta = e,$$

  contradicting $\mathrm{ord}(x) = q$. Thus

  $$\gcd(|G^n|, q) = 1 \Rightarrow |G^n| = p^r.$$

  Similarly $|G^m| = q^s$. Since $G^m \times G^n \cong G$, we have $p^r q^s = p^a q^b$, so $r = a, s = b$.

Proof of Step 2 : Suppose $|G| = p^a$. By Lagrange's Theorem, for all $x \in G$:

$$\mathrm{ord}(x) = p^i \quad \text{for some } 0 \le i \le a.$$

Let $\mu \in G$ be an element with maximum order $\mathrm{ord}(\mu) = p^m$ in G.

Proposition 2.90. *Let G be an abelian group with $|G| = p^a$. Suppose $\mu \in G$ has maximum order ord(μ) $= p^m$ in G, then*

$$G \cong \langle \mu \rangle \times K \cong \mathbb{Z}_{p^m} \times K.$$

Assuming the validity of the proposition, then one can reduce the study of G into that of K, since K is also abelian with $|K| = |G|/|\langle \mu \rangle| = p^{a-m}$. Then **Step 2** follows by induction on power of p.

Proof of Proposition. We proceed by induction on $|G| = p^a$. For the base case $a = 1$, $|G| = p$ implies $G \cong \mathbb{Z}_p$, and the result holds with $K = \{e\}$. Assume the proposition holds for all abelian groups of order p^r with $r < a$.

Now let $|G| = p^a$ and let $\mathrm{ord}(\mu) = p^m$ be maximal. If $m = a$, then $\langle \mu \rangle = G$ and the result is trivial. Otherwise, if $m < a$, let $\nu \in G$ be a non-identity element not in $\langle \mu \rangle$ with the smallest possible order p^k.

- **Claim 4 -** $\mathrm{ord}(\nu) = p$:

  Since $\mathrm{ord}(\nu^p) < p^k$, by the minimality of p^k, we must have $\nu^p \in \langle \mu \rangle$, so $\nu^p = \mu^i$ for some $i \in \mathbb{Z}$. Then:

  $$(\mu^i)^{p^{m-1}} = (\nu^p)^{p^{m-1}} = \nu^{p^m} = e$$

  since every element in G has order $\le p^m$. This implies $\mathrm{ord}(\mu^i) \mid p^{m-1}$, so $|\langle \mu^i \rangle| < p^m$, which means $\gcd(i, p^m) > 1$. Thus, $i = pj$ for some $j \in \mathbb{Z}$, and we have:

  $$\nu^p = \mu^{pj}.$$

Let $c := \nu\mu^{-j}$. Then $c \notin \langle\mu\rangle$ and:

$$c^p = (\nu\mu^{-j})^p = \nu^p\mu^{-pj} = e.$$

Since ν was chosen with the smallest order among elements not in $\langle\mu\rangle$, it follows that $\mathrm{ord}(\nu) = p$.

- **Claim 5 -** $\langle\mu\rangle \cap \langle\nu\rangle = \{e\}$:

  Let $\nu^l \in \langle\mu\rangle \cap \langle\nu\rangle$. Since $\mathrm{ord}(\nu) = p$, we have $0 \leq l < p$. If $l \neq 0$, then $\gcd(l,p) = 1$. By Bezout's Theorem, there exist α, β such that $\alpha l + \beta p = 1$. Then:

  $$\nu = \nu^{\alpha l+\beta p} = (\nu^l)^\alpha(\nu^p)^\beta = (\nu^l)^\alpha \in \langle\mu\rangle$$

  which contradicts our choice of ν. Thus $l = 0$ and the intersection is trivial.

- **Claim 6 -** $\bar{\mu} \in \bar{G} := G/\langle\nu\rangle$ has order p^m:

  Clearly $\bar{\mu}^{p^m} = e_{\bar{G}}$. Suppose $\mathrm{ord}(\bar{\mu}) = p^u$ for some $u < m$. Then $\mu^{p^u}\langle\nu\rangle = e\langle\nu\rangle$, meaning $\mu^{p^u} \in \langle\nu\rangle$. By Claim 5:

  $$\mu^{p^u} \in \langle\mu\rangle \cap \langle\nu\rangle = \{e\}$$

  which contradicts $\mathrm{ord}(\mu) = p^m$. Thus, $\bar{\mu}$ retains the maximal order p^m in $\bar{G}$.

- **Claim 7 -** The map $\pi|_K : K \to \bar{K}$ has $\ker(\pi|_K) = \langle\nu\rangle$:

  Since $|\bar{G}| = p^{a-1}$, by the inductive hypothesis, there exists a subgroup $\bar{K} \leq \bar{G}$ such that $\bar{G} \cong \langle\bar{\mu}\rangle \times \bar{K}$. Let $\pi : G \to \bar{G}$ be the natural projection and define $K := \pi^{-1}(\bar{K})$. Then:

  $$x \in \ker(\pi|_K) \iff \pi(x) = e_{\bar{G}} \iff x \in \langle\nu\rangle.$$

- **Claim 8 -** $\langle\mu\rangle \cap K = \{e\}$ in G:

  Let $\mu^i \in \langle\mu\rangle \cap K$. Then $\pi(\mu^i) = \bar{\mu}^i \in \bar{K}$. Since $\bar{G} = \langle\bar{\mu}\rangle \times \bar{K}$, every element is uniquely represented. Thus:

  $$\bar{\mu}^i = e_{\bar{G}} \implies \mu^i \in \langle\nu\rangle.$$

  By Claim 5, $\mu^i \in \langle\mu\rangle \cap \langle\nu\rangle = \{e\}$.

Finally, consider the homomorphism $\theta : \langle\mu\rangle \times K \to G$ defined by $\theta(\mu^i, k) := \mu^i k$. By Claim 8, θ is injective. By Claim 7 and the First Isomorphism Theorem, the order of K is:

$$|K| = p \cdot |\bar{K}| = p \cdot \frac{|\bar{G}|}{p^m} = p \cdot \frac{p^{a-1}}{p^m} = p^{a-m}.$$

Thus, the order of the product group is:

$$|\langle\mu\rangle \times K| = p^m \cdot p^{a-m} = p^a = |G|.$$

Therefore, θ is a bijection, and $G \cong \langle \mu \rangle \times K$. □

Example 2.91. Consider an abelian group G with $|G| = 4$. By Lagrange's Theorem, the possible orders for elements in G are 1, 2, and 4.

(i) If G contains an element m of order 4, then $G = \langle m \rangle \cong \mathbb{Z}_4$.

(ii) If every non-identity element of G has order 2, let $m \in G$ be an element of order 2. By the previous proposition, $G \cong \langle m \rangle \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Corollary 2.92. *If G is an abelian p-group with $|G| = p^a$, then*

$$G \cong \mathbb{Z}_{p^{b_1}} \times \mathbb{Z}_{p^{b_2}} \times \cdots \times \mathbb{Z}_{p^{b_\ell}}$$

where $\sum_{j=1}^{\ell} b_j = a$.

Proof. The proof follows by induction on $|G| = p^a$, using the proposition that $G \cong \mathbb{Z}_{p^m} \times K$ to repeatedly factor out cyclic components until the remaining group is trivial. □

Example 2.93. To classify all abelian groups of order $|G| = 360 = 2^3 \times 3^2 \times 5$:

- **By Step 1:** The group decomposes into its Sylow p-subgroups:

$$G \cong G_8 \times G_9 \times G_5$$

  where $|G_8| = 2^3$, $|G_9| = 3^2$, and $|G_5| = 5$.

- **By Step 2:** We find all possible structures for each p-group:
  - G_8 can be $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
  - G_9 can be $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$.
  - G_5 can only be $\mathbb{Z}_5$.

Thus, the total number of non-isomorphic abelian groups of order 360 is $3 \times 2 \times 1 = 6$. The possible structures are:

$$G \cong \left\{ \begin{matrix} \mathbb{Z}_8 \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \\ \mathbb{Z}_2^3 \end{matrix} \right\} \times \left\{ \begin{matrix} \mathbb{Z}_9 \\ \mathbb{Z}_3 \times \mathbb{Z}_3 \end{matrix} \right\} \times \mathbb{Z}_5$$

Corollary 2.94 (Smith Normal Form / Invariant Factors)**.** *Every finite abelian group G is isomorphic to a group of the form:*

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k}$$

where each $d_i > 1$ is an integer and $d_i \mid d_{i+1}$ for all $i = 1, \ldots, k-1$.

Furthermore, this representation is unique: if $H \cong \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_\ell}$ with $e_i \mid e_{i+1}$, then $G \cong H$ if and only if $k = \ell$ and $d_i = e_i$ for all i.

Chapter 3

Rings

3.1 Basic Definition

Rings

Definition 3.1 (Ring)**.** A ring $(R, +, \cdot)$ is a set equipped with 2 binary operations $+, \cdot : R \times R \to R$ such that

1. $(R, +)$ is an abelian group with additive identity $0_R \in R$.
2. $(R, \cdot)$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$.
3. $(R, +, \cdot)$ is distributive:

$$\begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (a + b) \cdot c = a \cdot c + b \cdot c \end{cases} \quad \forall a, b, c \in R.$$

Example 3.2.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings.
- $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ where $i = \sqrt{-1}$ (Gaussian integers)
  $(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i$
  $(a + bi) + (c + di) := (a + c) + (b + d)i$
- More generally, $\mathbb{Z}[e^{\frac{2\pi i}{n}}] = \{a_0 + a_1 e^{\frac{2\pi i}{n}} + \cdots + a_k e^{\frac{2\pi k i}{n}} + \cdots + a_{n-1} e^{\frac{2\pi (n-1) i}{n}} \mid a^i \in \mathbb{Z}\}$
  Since $e^{\frac{2\pi i}{n}} := cos\frac{2\pi i}{n} + i(sin\frac{2\pi i}{n})$, then $n = 4$, $e^{\frac{2\pi i}{4}} = i$.
- $2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\}$ is a ring,
  but $(\{\cdots, -3, -1, 1, 3, \cdots\}, +, \cdot)$ is **NOT** a ring.
- $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ is a ring
- $M_{n \times n}(\mathbb{Z})$ is a ring
- $\mathbb{Z}[x] = \{$all polynomials with integer coefficients$\}$
  For $f(x) = a_m x^m + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$,

$$(f \cdot g)(x) := a_m b_n x^{n+m} + \cdots + \sum_{\substack{p\geq 0\\ q\geq 0\\ p+q=i}} a_p b_q x^i + \cdots + a_0 b_0.$$

Mativation
Solve $x^2 + y^2 = z^2$ for integers x, y, z. $\Rightarrow (x+iy)(x-iy) = z^2$ in $\mathbb{Z}[i]$,
so we wish to study more about properties of the Gaussian integers $\mathbb{Z}[i]$, e.g.: does the **fundamental theorem of arithmetic** hold for $\mathbb{Z}[i]$, i.e.: can every element in $\mathbb{Z}[i]$ be factorized into product of prime numbers uniquely?

Fermat's Last Theorem: $x^n + y^n = z^n$ for $n \geq 3$, $x^n + y^n = (x - e^{\frac{2\pi i}{n}} y) \cdots (x - e^{\frac{2\pi(n-1)i}{n}} y)$ in $\mathbb{Z}[e^{\frac{2\pi i}{n}}]$

Definition 3.3 (Unital Rings and Commutative Rings)**.** Let $(R, +, \cdot)$ be a ring. We say:

1. R is **unital** if $\exists\ 1_R \in R$ such that
   $1_R \cdot r = r \cdot 1_R = r\ \forall\ r \in R$
   (1_R is the multiplication identity of R)
   (non-example: $R = 2\mathbb{Z}$ or $n\mathbb{Z}$)

2. If R is unital, then the **units** of R are the elements
   $U(R) = \{a \in R \mid \exists a^{-1} \in R \text{ s.t. } aa^{-1} = a^{-1}a = 1_R\}$
   (e.g.: $U(\mathbb{Z}) = \{\pm 1\}$, $U(M_{n\times n}(R)) = GL(n, \mathbb{R})$), and $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, why they are the only units?)

3. R is **commutative** if $a \cdot b = b \cdot a\ \forall a, b \in R$
   (non-example: $R = M_{n\times n}(\mathbb{Z})$)

Example 3.4. $(\mathbb{Z}_n, +, \cdot)$ is a commutative and unital ring with the multiplication identity $1_R = [1]$. The units of $\mathbb{Z}_n$ are $U(\mathbb{Z}) = \mathbb{Z}_n^* = \{a \mid gcd(a, n) = 1\}$

Remark 3.5.

- The additive identity $0_R \in R$ is unique in R. If R is unital, then the multiplication ifentity $1_R \in R$ is also unique
- We write $-r \in R$ to be the additive inverse of $r \in R$, i.e.: $(-r) + r = r + (-r) = 0_R$
- If $r \in U(R)$ is a unit in a (commutative) unital ring, then we write r^{-1} to be the multiplication inverse of r, i.e.: $r^{-1}r = rr^{-1} = 1_R$
- We write $nr := r + \cdots + r$ (n terms of r) for $n \in \mathbb{N}$ and $r \in R$.
- For $a, b \in R$, we write $a \mid b$ if $\exists c \in R$ s.t.: $ac = b$

Proposition 3.6.

1. $0_R \cdot r = r \cdot 0_R = 0_R$

2. $(-1_R) \cdot r = r \cdot (-1_R) = -r$

3. $(-1_R) \cdot (-r) = (-r) \cdot (-1_R) = r$

Proof:

1. For any $a \in R$, $a \cdot r = (0_R + a) \cdot r = 0_R \cdot r + a \cdot r$
   By the uniqueness of 0_R, $0_R \cdot r = 0_R$

2. $0_R = 0_R \cdot r = (1_R + (-1_R)) \cdot r = 1_R \cdot r + (-1_R) \cdot r = r + (-1_R) \cdot r$
   $\Rightarrow -r = (-r) + 0_R = (-r) + (r + (-1_R) \cdot r) = (-1_R) \cdot r$
   Similarly for $r \cdot (-1_R) = -r$, by taking $0_R \cdot r = ((-1_R) + 1_R) \cdot r$

3. Directly proved by proposition 3.5(2). □

Definition 3.7 (Product Rings)**.** Let $(R_1, +_1, \cdot_1)$ and $(R_2, +_2, \cdot_2)$ be two rings. Then $R_1 \times R_2$ is called a **product ring** with
$(r_1, r_2) +_{R_1 \times R_2} (r_1' + r_2') := (r_1 +_1 r_1', r_2 +_2 r_2')$
$(r_1, r_2) \cdot_{R_1 \times R_2} (r_1 \cdot_1 r_1', r_2 \cdot_2 r_2')$

Definition 3.8 (Subrings)**.** Let $(R, +, \cdot)$ be a ring. A subset $S \subset R$ is a subring if
$+ |_{S \times S}$: $S \times S \to S$ and $\cdot |_{S \times S}$: $S \times S \to S$ give a ring substructure of S.

Example 3.9.
- $\mathbb{Z}[i] \subset \mathbb{C}$ is a subring
- $n\mathbb{Z} \subset \mathbb{Z}$ is a subring
- $\{\cdots, -3, -1, 1, 3, \cdots\} \subset \mathbb{Z}$ is **NOT** a subring

Proposition 3.10. *$S \subset R$ is a subring $\Leftrightarrow$ $\forall a, b \in S$: $a + b \in S$, $-a \in S$, and $a \cdot b \in S$*

Definition 3.11 (Field)**.** Let R be a commutative unital ring. We say R is a **field** if all nonzero elemens of R are in the units U(R) of R.
(Field is a very special kind of ring)

Example 3.12.
- $\mathbb{Q}$ is a field, since all nonzero elements $\frac{a}{b}$ of $\mathbb{Q}$ has a multiplication inverse $(\frac{a}{b})^{-1} = \frac{b}{a}$
- $\mathbb{R}$ and $\mathbb{C}$ are fields
- $\mathbb{Z}$ is **NOT** a field: $u(\mathbb{Z}) = \{\pm 1\} \neq \mathbb{Z} \setminus \{0\}$
- $\mathbb{Z}_p$ is a field for all p prime

More examples:
- $n\mathbb{Z}$(**NOT** unital) $\subset \mathbb{Z}$(**NOT** field) $\subset \mathbb{Q}$(field) $\subset \mathbb{R}$(field) $\subset \mathbb{C}$(field)
- $R[x] = \{\sum_i a_i x^i \mid a_i \in R\}$ is commutative if R is commutative, and is unital if R is unital
- $M_{n \times n}(R) = \{(a_{ij}) \mid a_{ij} \in R\}$ is **NOT** commutative for $n \geq 2$

3.2 Ring Homomorphism

Definition 3.13 (Ring Homomorphism)**.** Let R and S be rings. A map ϕ: $R \to S$ is a **homomorphism of rings** if
$\phi(a +_R b) = \phi(a) +_S \phi(b)$ and $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$

- If R and S are unital, we say a homomorphism $\phi : R \to S$ is **unital** if $\phi(1_R) = 1_S$

- If ϕ is bijective,then ϕ is called a **ring isomorphism**

Example 3.14. • $\phi : \mathbb{Z} \to \mathbb{Z}$, $\phi(n) := 2n$. Then:

1. $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is a group homomorphism, **BUT**
2. $\phi : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}, +, \cdot)$ is **NOT** a ring homomorphism, since $\phi(a \cdot b) = 2ab \neq 4ab = (2a) \cdot (2b) = \phi(a) \cdot \phi(b)$ for $a, b \neq 0$

- Similarly, $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ with $\phi(n) = 2n$ is a group homomorphism, but **NOT** a ring homomorphism.
  But $\phi(n) := 5n$ is a ring homomorphism.
- $\phi : \mathbb{Z} \to \mathbb{Z}_m$ with $\phi(n)$:=n(mod m) is a ring homomorphism
- Let R be a commutative unital ring. $\phi : R[x] \to R$ with $\phi(p(x)) := p(1_R)$
  Check $\phi(p + q) = (p + q)(1_R) = p(1_R) + q(1_R) = \phi(p) + \phi(q)$ and $\phi(p \cdot_{R[x]} q) = \phi(p) \cdot_R \phi(q)$
- $\mathbb{Z} \mapsto \mathbb{Q}$, $\mathbb{Q} \mapsto \mathbb{R}$, $\mathbb{R} \mapsto \mathbb{C}$

Proposition 3.15. *Let $\phi : R \to S$ be a ring homomorphism.*

1. $\phi(0_R) = 0_S$

2. $\phi(-a) = -\phi(a)$

3. If ϕ is unital and $a \in U(R)$, then $\phi(a) \in U(S)$ with $\phi(a)^{-1} = \phi(a^{-1})$

4. If $\phi : R \xrightarrow{\cong} S$ is an isomorphism, then $\phi^{-1} : S \to R$ is a ring isomorphism as well

Proof:

1. $\phi(r) = \phi(0_R + r) = \phi(0_R) + \phi(r)$. By uniqueness of additive identity $\phi(0_r) = 0_S$
2. Same as group homomorphism
3. $\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1}a) = \phi(1_R) = 1_S$ and similarly we have $\phi(a)\phi(a^{-1}) = 1_S$. Hence, $\phi(a)$ is a unit with $\phi(a)^{-1} = \phi(a^{-1})$
4. Let α and $\beta \in S$. Then $\exists a, b \in R, s.t. : \phi(a) = \alpha$ and $\phi(b) = \beta$——(*)
   (WTS: $\phi^{-1}(\alpha\beta) = \phi^{-1}(\alpha)\phi^{-1}(\beta)$)
   $\phi^{-1}(\alpha) \cdot \phi^{-1}(\beta) = a \cdot b = \phi^{-1}(\phi(ab)) = \phi^{-1}(\phi(a) \cdot \phi(b)) = \phi^{-1}(\alpha \cdot \beta)$
   (HW: Check $\phi^{-1}(\alpha + \beta) = \phi^{-1}(\alpha) + \phi^{-1}(\beta)$) □

Proposition 3.16. *Let $\phi : R \to S$ be a ring homomorphism. Then $ker\phi := \{r \in R \mid \phi(r) = 0_S\} \leq R$ and $im\phi := \{\phi(r) \mid r \in R\} \leq S$ are sunrings.*

Proof: Let a,b$\in$ $ker\phi$, i.e.: $\phi(a) = \phi(b) = 0_S$. (WTS: a+b, -a, $a \cdot b \in ker\phi$)

- $\phi(a + b) = \phi(a) + \phi(b) = 0_S + 0_S = 0_S$
- $\phi(-a) = -\phi(a) = -0_S = 0_S$
- $\phi(a \cdot b) = \phi(a) \cdot \phi(b) = 0_S \cdot 0_S = 0_S$ (the last equality is left to check in the last lecture)

Remark 3.17. In groups, we know $ker\phi$ is a **normal** subroup of R. How about rings, are there any notion of "normal subring"?
Answer: We'll study **ideals**, which is the ring analogue of normal subgroups.

3.3 Integral Domain

Definition 3.18 (Zero-divisor)**.** Let R be a ring. A nonzero element r$\in R$ is a **zero-divisor** if $\exists 0 \neq s \in R, s.t. : r \cdot s = 0$ or $s \cdot r = 0$.

Example 3.19. R=$\mathbb{Z}$. Then $2 \in R$ is a zerodivisor, since $2 \cdot 3 = 6 = 0$ in R.

Definition 3.20 (Integral Domain)**.** If R has no zerodivisors, then R is a **domain**.
Moreover, if R is commutative ring with no zerodivisors, then R is an **integral domain (ID)**.

Example 3.21.

- $\mathbb{Z}_6$ is **NOT** ID. More generally, $\mathbb{Z}_m$ is ID $\Leftrightarrow$ m is prime.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[i]$ are IDs.
- If R is ID, then so is R[x].

Proposition 3.22 (Cancellation Property)**.** *Let R be commutative ring. Then R is ID $\Leftrightarrow$ whenever ca=cb for some $c \neq 0$, then a=b.*

Proof: ca=cb $\Leftrightarrow$ ca+c(-b)=0 $\Leftrightarrow$ c(a+(-b))=0 $\Leftrightarrow$ c(a-b)=0 $\Leftarrow$(R is ID)$\Rightarrow$ c=0 OR a-b=0 $\Leftrightarrow$ a-b=0 $\Leftrightarrow$ a=b. □

Remark 3.23. One can cancel the common factor on both sides of equation **exactly** when R is an ID.

Overview Fields $\subsetneq$ Euclidean Domain (ED) $\subsetneq$ Principal Ideal Domain (PID) $\subsetneq$ Unique Factorization Domain (UFD) $\subsetneq$ Itegral Domain (ID)
(HW: If R is a field, then R is integral domain.)

Lemma 3.24. *Let R be ID with $\mid R \mid < \infty$. Then R is unital.*

Proof: Let $a \in R$ be nonzero. Then $\{a, a^2, \cdots\}(\subset R)$ must repeat, since $\mid R \mid < \infty$. Say $a^m = a^n$ for some m>n.
Claim: $1_R = a^{m-n}$.
Proof of claim: $\forall x \in R$, let $xa^{m-n} = y$. Then $xa^m = xa^{m-n}a^n = ya^n = ya^m$. Then, by cancellation property, we have: x=y. Again by cancellation property and $xa^{m-n} = y$, $a^{m-n} = 1_R$.
Hence, by the claim, $1_R = a^{m-n} \in R$. Therefore, R is unital. □

Proposition 3.25. *Let R be an ID with $\mid R \mid < \infty$. Then R is a field.*

Proof: Let $R \setminus \{0_R\} = \{r_1 = 1_R, r_2, \cdots, r_m\}$. Then for all a$\neq 0$ in R, consider

$$S := \{ar_1, ar_2, \cdots, ar_m\}$$

Suppose this set has repetitions, i.e.: $\exists i \neq j, s.t. : ar_i = ar_j$. Then by cancellation property, $r_i = r_j$. Then i=j.

Hence, S has no repetitions. Then S=$R \setminus \{0_R\}$. In particular, $\exists r_l, s.t. : ar_l = r_1 = 1_R$, and hence, a$\in U(R)$. □

3.4 ideal

Motivation A ring analogue of normal subgroup.

Definition 3.26 (Ideal)**.** Let R be a ring. We say I $\subset R$ an **ideal** if

- I is an additive subgroup of (R,+)
- For all x $\in R$, i $\in I$, we have xi,ix $\in I$.

Remark 3.27.

- We write I $\lhd$ R if I is an ideal
- If I $\lhd$ R, then I $\leq$ R automatically. (REASON: Take x $\in$ I, then ax=xa$\in I$)

Example 3.28.

- (Nonexample:)$\mathbb{Z} \leq \mathbb{Q}$ is **NOT** an ideal, since 2$\in \mathbb{Z}$ and $\frac{1}{3} \in \mathbb{Q}$, **BUT** $2 \cdot \frac{1}{3} = \frac{2}{3} \notin \mathbb{Z}$
- R=$\mathbb{Z}$, I=$n\mathbb{Z}$. Take na$\in I$, m$\in R$. Then $(na)m = n(am) \in I$
- R=$\mathbb{Z}[x]$, I=$\{p(x) \in R \mid p(0) = 0\}$(=$\{$polynomials with no constant term$\}$)
  (HW: Check I is subring.)
  Now take $p(x) = a_n x^n + \cdots + a_1 x \in I$ and $q(x) = b_m x^m + \cdots + b_1 x + b_0 \in R$. Then $p(x)q(x) = a_n b_m x^{n+m} + \cdots + a_1 b_0 x \in I$.
  (Alternatingly, $p(0)q(0) = 0 \cdot q(0) = 0$, and hence p(x)q(x)$\in I$)
- $R = \mathbb{Z}[x]$, $I = \{p(x) \in R \mid$constant term is an even integer$\}$
  e.g.: $1 + x \notin I, 10002 + x^2 \notin I, (0+)x^3 + 15x^5 \in I$
  (HW: Check that this is an ideal)

Question: For any R, how to construct I?

Definition 3.29. Let R be a ring, V $\subset$ R subset. Then the **ideal generated by V** is <V>, which is the smallest ideal in R containing all elements in V.

Example 3.30.

- R=$\mathbb{Z}$, V=n. What's <V>=<n>?
  For any ideal I s.t.: $n \in I$, then $n + \cdots + n$ and $(-n) + \cdots + (-n) \in S$, since I is a subgroup of (R,+). Then $n\mathbb{Z} \subset I$. But $n\mathbb{Z}$ itself is an ideal. So <n>=$n\mathbb{Z}$
- How about general case? Let R be a unital commutative ring, and let $V = \{a_1, \cdots, a_n\}$ is a finite set. Then <V>=<$a_1, \cdots, a_n$>=$\{r_1 a_1 + \cdots + r_n a_n \mid r_1, \cdots, r_n \in R\}$=:S
  1. Check S contains $a_1, \cdots, a_n$, e.g.: $a_2 = 0a_1 + 1a_2 + 0a_3 + \cdots + 0a_n \in S$
  2. Check S $\lhd$ R. (Check $s \in S$, $r \in R$, then $s \cdot r \in S$)

3. For any ideal I satisfying: $a_1, \cdots, a_n \in I$, check $S \subset I$
   (**Proof:** $a_1, \cdots, a_n \in S$. Then by the definition of ideal, $a_1 r_1, \cdots, a_n r_n \in I$. Since I is an additive subgroup, then $a_1 r_1 + \cdots + a_n r_n \in I$)

- R= $\mathbb{Z}[x]$, $I =< 2, x >= \{2p(x) + xq(x) \mid p(x), q(x) \in R\} = \{$all polynomials with even constant term$\}$.

Lemma 3.31. *Suppose $I_1, \cdots, I_k \lhd R$, then*

1. $I_1 + \cdots + I_k := \{i_1 + \cdots + i_k \mid i_r \in I_r\} \lhd R$
2. $\bigcap_{i=1}^{k} I_i \lhd R$

Proof:

1. Let $(i_1 + \cdots + i_k)$ and $(i'_1 + \cdots + i'_k) \in I_1 + \cdots + I_k$.Then $(-i_r) \in I_r$ $\forall r = 1, \cdots, k$.
   $\Rightarrow -(i_1 + \cdots + i_k) = (-i_1) + \cdots + (-i_k) \in I_1 + \cdots + I_k$
   Also, $(i_1 + \cdots + i_k) + (i'_1 + \cdots + i'_k) = (i_1 + i'_1) + \cdots + (i_k + i'_k) \in I_1 + \cdots + I_k$
   Hence, $I_1 + \cdots + I_k$ is an additive subgroup.
   Now, take any $r \in R$, then $r \cdot (i_1 + \cdots + i_k) = ri_1 + \cdots + ri_k \in I_1 + \cdots + I_k$. Similarly, $(i_1 + \cdots + i_k) \cdot r \in I_1 + \cdots + I_k$
2. Left to the readers. □

Example 3.32. $R = \mathbb{Z}$, $I_r = a_r\mathbb{Z}$ where $a_r \in \mathbb{N}$
Then $I_1 + \cdots + I_k = gcd(a_1, \cdots, a_k)\mathbb{Z}$ and $I_1 \bigcap \cdots \bigcap I_k = lcm(a_1, \cdots, a_k)\mathbb{Z}$

Definition 3.33 (Principle Ideal Domain)**.** 1. Let R be a commutative ring. An ideal I $\lhd$ R is called **principal** if I=<a> for some a$\in R$.

2. Let R be an ID. We say r is a **principal ideal domain(PID)** if all ideals in R are principal.

Proposition 3.34. *Let $\phi : R \to S$ be a ring homomorphism. Then $ker\phi \lhd R$.*

Proof: We only need to show that $\forall r \in R, i \in ker\phi \Rightarrow ri, ir \in ker\phi$, since we know $ker\phi \leq R$ already.
Indeed, $\phi(ri) = \phi(r)\phi(i) = \phi(r) \cdot 0_S = 0_S$. Hence, $ri \in ker\phi$. Similarly for ir. □

3.5 Quotient Ring

Definition 3.35 (Quotient Ring)**.** Let R be a ring, and I $\lhd$ R ideal. Consider the collection of left cosets of (R,+), $R/I := \{r + I \mid r \in R\}$ (Then (R/I,+) has a group structure) with the operations:
$(r_1 + I) +_{R/I} (r_2 + I) := (r_1 + r_2) + I$
$(r_1 + I) \cdot_{R/I} (r_2 + I) := (r_1 \cdot r_1) + I$.
Then $(R/I, +_{R/I}, \cdot_{R/I})$ is a ring, and it's called the **quotient ring of R** by I.

Check:

- $\cdot_{R/I}$ is well-defined:
  Take $r_1 + I = r'_1 + I$ and $r_2 + I = r'_2 + I$ (*).
  (*) $\Leftrightarrow r_1 - r'_1 \in I$ and $r_2 - r'_2 \in I \Rightarrow r'_1 = r_1 + i_1$ and $r'_2 = r_2 + i_2$ for some $i_1, i_2 \in I \Rightarrow r'_1 r'_2 = r_1 r_2 + r_1 i_2 + i_1 r_2 + i_1 i_2 \Rightarrow r'_1 r'_2 - r_1 r_2 \in I \Leftrightarrow r'_1 r'_2 + I = r_1 r_2 + I \Leftrightarrow (r'_1 + I) \cdot_{R/I} (r'_2 + I) = (r_1 + I) \cdot_{R/I} (r_2 + I)$
- $+_{R/I}$ is well-defined by quotient theory
- Check $(R/I, +_{R/I}, \cdot_{R/I})$ is associative:
  $(r_1 + I) \cdot_{R/I} ((r_2 + I) \cdot_{R/I} (r_3 + I)) = ((r_1 + I) \cdot_{R/I} (r_2 + I)) \cdot_{R/I} (r_3 + I)$
- Check $(R/I, +_{R/I}, \cdot_{R/I})$ is distributive, e.g.:
  $(r_1 + I) \cdot_{R/I} ((r_2 + I) +_{R/I} (r_3 + I)) = (r_1 + I) \cdot_{R/I} (r_2 + I) +_{R/I} (r_1 + I) \cdot_{R/I} (r_3 + I)$ □

Easy Exercise

- If R is commutative, then R/I is commutative.
- If $1_R \in R$ unital, then $1_{R/I} := 1_R + I$ unital.

Example 3.36.

- $\mathbb{R}[x]/\langle x^2 - 1 \rangle = \{p(x) + \langle x^2 - 1 \rangle \mid p(x) \in \mathbb{R}[x]\} = \{(ax + b) + \langle x^2 - 1 \rangle \mid a, b \in \mathbb{R}\}$
  (shorthand: $\overline{p(x)} := p(x) + \langle x^2 - 1 \rangle$)

  $$\overline{x-1}, \overline{x+1} \in \mathbb{R}[x]/\langle x^2 - 1 \rangle \quad \textit{and} \quad (x-1) \cdot (x+1) = x^2 - 1 \in \langle x^2 - 1 \rangle$$

  $\Rightarrow$

  $$\overline{x-1} \cdot \overline{x+1} = \overline{0} \in \mathbb{R}[x]/\langle x^2 - 1 \rangle$$

  $\therefore \overline{x-1}, \overline{x+1}$ are zerodivisors of $\mathbb{R}[x]/\langle x^2 - 1 \rangle$ and hence it is **NOT integral domain (ID)**
  (issue: $x^2 - 1 = (x+1)(x-1)$ is not irreducible in $\mathbb{R}[x]$)
- $\mathbb{R}[x]/\langle x^2 + 1 \rangle$. Then

  $$\overline{x} \cdot \overline{x} = \overline{x^2} = \overline{x^2 - (x^2 + 1)} = \overline{-1} \Rightarrow (\overline{x})^2 = \overline{-1}$$

- $\mathbb{Z}/\langle 2, x \rangle = \{(a_n x^n + \cdots + a_1 x + a_0) + \langle 2, x \rangle\} = \{a_0 + \langle 2, x \rangle\} = \{0 + \langle 2, x \rangle, 1 + \langle 2, x \rangle\} \cong \mathbb{Z}_2$

Theorem 3.37 (First Isomorphism Theorem of Rings)**.** *Let $\Phi : R \to S$ be a ring homomorphism. Then the map $\phi : R/ker\Phi \to im\Phi$ defined by $\phi(r + ker\Phi) := \Phi(r)$ is a well-defined ring isomorphism.*

Proof:

- ϕ is well-defined, i.e.: if (*)"$r + ker\Phi = r' + ker\Phi$", then $\Phi(r) = \Phi(r')$.
  (Exercise: recall (*) $\Leftrightarrow r - r' \in ker\Phi$)
- ϕ is a ring homomorphism: only need to check $\phi(rr') = \phi(r)\phi(r')$, since we know ϕ is group homomorphism already by the 1_{st} isomorphism theorem of groups.

- ϕ is bijective as in the 1_{st} isomorphism theorem of groups. □

Example 3.38.
- Let $\Phi : \mathbb{R}[x] \to \mathbb{C}$ be defined by $\Phi(p(x)) := p(i)$ where $(i = \sqrt{-1})$. Then ϕ is a homomorphism. (Exercise: $\phi(pq) = \phi(p)\phi(q)$)
  Now, $im\phi = \mathbb{C}$, e.g.: $\Phi(bx + a) := a + bi \in \mathbb{C}$ and

$$p(x) \in ker\Phi$$

$$\Leftrightarrow p(i) = 0$$

$$\Leftrightarrow \overline{p(i)} = p(i) = 0$$

$$\Leftrightarrow p(-i) = p(i) = 0$$

$$\Leftarrow (Factor\ theorem\ on\ \mathbb{C}[x]) \Rightarrow (x - i), (x - (-i)) \mid p(x)$$

$$\Leftrightarrow (x - i)(x + i) = x^2 + 1 \mid p(x)\ in\ \mathbb{R}[x]$$

  $\therefore\ ker\Phi = \{(x^2 + 1)q(x) \mid q(x) \in \mathbb{R}[x]\} = \langle x^2 + 1\rangle$.
  $\therefore$ 1_{st} isomorphism theorem says

$$\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$$

- Let $\Phi : \mathbb{Z}[x] \to \mathbb{Z}_2$ with $\Phi := p(0)(\text{mod } 2)$.
  Check that $im\Phi = \mathbb{Z}_2,\ ker\Phi = \langle 2, x\rangle$. (Exercise)

$$\Rightarrow\ \mathbb{Z}[x]/\langle 2, x\rangle \cong \mathbb{Z}_2$$

3.6 Chinese Remainder Theorem

Definition 3.39 (Product Ring)**.** Let R_i be rings. Then the **product ring** $\Pi_i R_i (= R_1 \times \cdots \times R_k)$ has a ring structure given by

$$(r_1, \cdots, r_k) +_{\Pi_i R_i} (r_1', \cdots, r_k') := (r_1 + r_1', \cdots, r_k + r_k')$$

$$(r_1, \cdots, r_k) \cdot_{\Pi_i R_i} (r_1', \cdots, r_k') := (r_1 r_1', \cdots, r_k r_k')$$

Remark 3.40. If R_1, R_2 are ID, then $R_1 \times R_2$ is **NOT** an ID:

$$(r_1, 0) \cdot (0, r_2) = (0, 0) = 0_{R_1 \times R_2}$$

Definition 3.41. Let R be a commutative ring. We say $I_1, I_2 \lhd R$ **coprime** if $I_1 + I_2 = R$.

Example 3.42. Let $R = \mathbb{Z}$ and $I_1 = \langle m\rangle = m\mathbb{Z}$, $I_2 = \langle n\rangle = n\mathbb{Z}$.
Then $I_1 + I_2 := \{mp + nq \mid p, q \in \mathbb{Z}\} = \langle gcd(m, n)\rangle$. (Exercise: prove the second equality.)
$\therefore\ I_1$ & I_2 are coprime $\Leftrightarrow I_1 + I_2 = \mathbb{Z} \Leftrightarrow \langle gcd(m, n)\rangle = \mathbb{Z} \Leftrightarrow gcd(m, n) = 1 \Leftrightarrow$ m,n coprime as integers.

The above example generalizes our understanding of "coprime" frome $\mathbb{Z}$ to any commutative ring R: Two elements r_1, r_2 are coprime in R means $\langle r_1\rangle + \langle r_2\rangle = R$.

Theorem 3.43. *Let R be commutative unital, and $I_1, \cdots, I_k \lhd R, s.t. : I_i, I_j$ are pairwise coprime. Then we have a ring isomorphism*

$$\phi : R/I_1 \cap \cdots \cap I_k \to R/I_1 \times \cdots \times R/I_k \quad defined\ by \quad \phi(r + I_1 \cap \cdots \cap I_k) := (r + I_1, \cdots, r + I_k).$$

Proof: Let $\Phi : R \to R/I_1 \times \cdots \times R/I_k$ be a ring homomorphism with $\Phi(r) := (r+I_1, \cdots, r+I_k)$. By the first isomorphism theorem, we need to show:

1. $ker\Phi = I_1 \cap \cdots \cap I_k$ and
2. $im\Phi = R/I_1 \times \cdots \times R/I_k$

1. $r \in ker\Phi \Leftrightarrow r + I_l = 0 + I_l\ \forall l \Leftrightarrow r - 0 \in I_l\ \forall l = 1, \cdots, k \Leftrightarrow r \in I_1 \cap \cdots \cap I_k$
2. Fix $j \in \{1, \cdots, k\}$. Since R is unital and I_j, I_i coprime for all $i \neq j$, so we have $z_i \in I_j \quad w_i \in I_i$, s.t.:

$$(*) : z_i + w_i = 1 \ \ (1 \in I_i + I_j = R)\ \forall i \neq j$$

Consider $1 = (1 - \Pi_{i\neq j} w_i) + (\Pi_{i\neq j} w_i)$.

$$Set \quad x_j := 1 - \Pi_{i\neq j} w_i = 1 - \Pi_{i\neq j}(1 - z_i) = sum\ of\ products\ of\ z_i's\ with\ no\ constants \in I_j$$

$$Set \quad y_j := \Pi_{i\neq j} w_i \in \bigcap_{i\neq j} I_i,\ since\ I_i\ ideals$$

$\therefore$ For each fixed j, we have

$$(**) : \quad 1 = x_j(\in I_j) + y_j(\in \bigcap_{i\neq j} I_i)$$

We already to check Φ is surjective:
For each $(u_1 + I_1, \cdots, u_k + I_k) \in R/I_1 \times \cdots \times R/I_k$, we **CLAIM** that $\Phi(u_1y_1 + \cdots + u_ky_k) = (u_1 + I_1, \cdots, u_k + I_k)$:
REASON: $\Phi(u_1y_1 + \cdots + u_ky_k) = (\cdots, u_1y_1 + \cdots + u_ky_k + I_l, \cdots) = (u_1 + I_1, \cdots, u_k + I_k)$, since

$$(u_1y_1 + \cdots + u_ly_l + \cdots + u_ky_k + I_l) = u_ly_l + I_l \overset{(**)}{=} u_l(1 - x_l) + I_l = u_l - u_lx_l + I_l = u_l + I_l$$

□

Corollary 3.44. *Let $p_1, \cdots, p_n$ be distinct prime numbers. Then*

$$\mathbb{Z}/\langle p_1^{a_1} \cdots p_n^{a_n}\rangle \cong \mathbb{Z}/\langle p_1^{a_1}\rangle \times \cdots \times \mathbb{Z}/\langle p_n^{a_n}\rangle.$$

Therefore, for each $b_i \in \mathbb{Z}/\langle p_i^{a_i}\rangle \cong \mathbb{Z}_{p_i^{a_i}}$, there exists $x \in \mathbb{Z}, s.t. : \Phi(x) = (b_1 + \langle p_1^{a_1}\rangle, \cdots, b_n +$

$\langle p_n^{a_n}\rangle)$ $x \equiv b_i \pmod{\mathbb{Z}_{p_i^{a_i}}}$ for all i.

3.7 Prime and Maximal Ideals

Motivation: Define "prime" in any commutative unital R.
(Kummer, mid 1800's): Rather thaan studying $r \in R$, study ideals $I \lhd R$.
Basic case: $R = \mathbb{Z}$
All ideals $I \lhd \mathbb{Z}$ are of the form $I = \langle n\rangle$. So study $\langle n\rangle$ instead of n.
e.g.: in $R = \mathbb{Z}$,

$$(\langle p\rangle, \langle q\rangle\ coprime\ (as\ ideals)) \Leftrightarrow (p, q\ are\ coprime\ (as\ integers))$$

Definition 3.45. Let R be a commutative, unital ring. We say a proper ($I \neq R$) ideal $I \lhd R$ is

1. **prime** if for all a,b ∈ R such that ab ∈ R, then we must have $a \in I\ or\ b \in R$;
2. **maximal** if for all ideals $J \lhd R$ s.t. $I \subset J \subset R$, then J=I or J=R.

Example 3.46.

- R=$\mathbb{Z}$. Let's check

$$(p \in \mathbb{Z},\ prime) \Leftrightarrow (I = \langle p\rangle\ is\ a\ prime\ ideal)$$

Proof: Let $a, b \in \mathbb{Z}$ s.t.

$$ab \in \langle p\rangle \Leftrightarrow ab = pk\ for\ some\ k \in \mathbb{Z} \Leftrightarrow p \mid ab \Leftrightarrow p \mid a\ or\ p \mid b \Leftrightarrow a \in \mathbb{Z}\ or\ b \in \mathbb{Z}$$

(**Exercise:** $\langle n\rangle$ is a maximal ideal ⇔ n is prime ⇔ $\langle n\rangle$ is prime)
(**Nonexample:** $\langle 6\rangle$ is **NOT** maximal since $\langle 6\rangle \subsetneq \langle 2\rangle \subsetneq \mathbb{Z}$)

- R=$\mathbb{Z}_{12}$. All the ideals of R are:

$$I_0 = \{0\},\ I_1 = \{0, 2, 4, 6, 8, 10\}(maximal\ and\ prime),\ I_2 = \{0, 3, 6, 9\}(maximal\ and\ prime),$$

$$I_3 = \{0, 4, 8\}(\textbf{NOT}\ \ prime,\ since\ 2{\cdot}2 = 4),\ I_4 = \{0, 6\}(\textbf{NOT}\ \ prime,\ since\ 2{\cdot}3 = 6),\ I_5 = R$$

- $R = \mathbb{Z}[x]$. $I = \langle x\rangle$=polynomials with 0 constant term is a prime ideal:
Take $p(x) = a_0 + a_1x + \cdots + a_mx^m$, $q(x) = b_0 + b_1x + \cdots + b_nx^n \in I$. Then

$$pq \in I \Leftrightarrow a_0b_0 = 0 \Leftrightarrow a_0 = 0\ or\ b_0 = 0 \Leftrightarrow p(x) \in I\ or\ q(x) \in I$$

But I is **NOT** maximal:

$$I \subsetneq \langle 2, x\rangle \subsetneq R$$

Proposition 3.47. *Let R be commutative unital, and $I \lhd R$. Then*

1. *I is prime ⇔ R/I is ID*

2. I is maximal ⇔ R/I is a field

Example 3.46.(3) revisited: Consider $\langle x\rangle \subset \mathbb{Z}[x]$. Then

$$R/I = \mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}.$$

$\mathbb{Z}$ is ID ⇔ $\langle x\rangle$ is prime
$\mathbb{Z}$ is **NOT** a field ⇔ $\langle x\rangle$ is **NOT** maximal

Proof:

1. Let (a+I), (b+I) $\in R/I$. Then (*): $(a+I)\cdot(b+I) = 0+I \Leftrightarrow ab \in I$.
   If I is prime, then (*) says

   $$(a+I)(b+I) = 0_{R/I} \Leftrightarrow ab \in I \Leftrightarrow a \in I \text{ or } b \in I \Leftrightarrow a+I = 0_{R/I} \text{ or } b+I = 0_{R/I} \Leftrightarrow R/I \text{ is } ID$$

2. Suppose $I \subset J \subset R$ for some $J \lhd R$. Then $I/I \subset J/I \subset R/I$. (HW9: J/I ◁ R/I)
   Recall: $\mathbb{F}$ is a field ⇔ the only ideals of $\mathbb{F}$ are 0 and $\mathbb{F}$
   (**Proof** of "Recall": Let $I \lhd \mathbb{F}$ be nonzero. Take $0 \neq a \in I$. Then $1 = a\cdot a^{-1} \in I \Rightarrow \forall x \in \mathbb{F}$, $x = x \cdot 1 \in I$)
   Therefore,

   $$\mathbb{F} = R/I \text{ is a field} \Leftrightarrow J/I \lhd R/I \text{ must be } \{0\} \text{ or } R/I \Leftrightarrow J = \{0\} \text{ or } J = R$$

□

Corollary 3.48. *Let R be commutative unital. Then $I \lhd R$ is maximal ⇒ $I \lhd R$ is prime.*

Proof. All fields are IDs. □

Definition 3.49. Let R be commutative unital. We say $a \in R$ is **prime** if $\langle a\rangle$ is a prime ideal. (Generalization of "prime number" in $R = \mathbb{Z}$)

Definition 3.50. Let $a, b \in R$ (commutative unital). We say a **divides** b (or $a \mid b$ in short) if $\langle b\rangle \subseteq \langle a\rangle$. (or equivalently, $b \in \langle a\rangle$, or $\exists x \in R$, s.t.: $ax = b$.)

We say a and b are **associates** ($a \sim b$) if ($a \mid b$ & $b \mid a$), (or $\langle a\rangle = \langle b\rangle$).

Lemma 3.51. *Suppose R is an integral domain. Then $(a \sim b) \Leftrightarrow \exists$ unit $x \in U(R)$ s.t.: $a = xb$.*

Proof:
(⇐): $a = xb \Rightarrow a \in \langle b\rangle \Rightarrow \langle a\rangle \subseteq \langle b\rangle$,
AND $x^{-1}a = b \Rightarrow \langle b\rangle \subseteq \langle a\rangle$ Similarly.
$\therefore \langle a\rangle = \langle b\rangle$
(⇒): Suppose $a \sim b$, i.e.: $\langle a\rangle = \langle b\rangle$. Then we have $a \in \langle b\rangle$.
$\Rightarrow a = p\cdot b$ for $p \in R$. Similarly, $b \in \langle a\rangle \Rightarrow b = q \cdot a$ $(q \in R)$
$\Rightarrow a = p\cdot q\cdot a \xrightarrow{\text{cancellation property}} 1_R = p\cdot q \Rightarrow p, q \in U(R)$. □

3.8 Principal Ideal Domain

Recall: I maximal $\Rightarrow$ I prime for R unital commutative.
Converse NOT holds in general (e.g. $\mathbb{Z}[x] = R$).
Goal: Study R s.t.: (I maximal) $\Leftrightarrow$ (I prime).

Definition 3.52 (Principal Integral Domain)**.** Let R be ID. We call R a **principal ideal domain (PID)** if all ideals $I \triangleleft R$ are principal, i.e.: all I are of the form $I = \langle a \rangle$.

Example 3.53.

- $\mathbb{Z}$ is PID.

  Proof: Let I be a nonzero ideal of $\mathbb{Z}$. (Otherwise $I = \{0\} = \langle 0 \rangle$)
  Let $\mu > 0$ be the smallest positive integer in I.
  Claim: $I = \langle \mu \rangle$.
  Suppose on contrary that $I \setminus \langle \mu \rangle$ is nonempty. Take $\lambda > 0$ be the smallest integer in $I \setminus \langle \mu \rangle$. By minimality of μ, we have $\lambda > \mu$. Then $\lambda - \mu \in I$ and $\lambda - \mu \notin \langle \mu \rangle$, since otherwise $(\lambda - \mu) + \mu = \lambda \in \langle \mu \rangle$, contradicting the choice of λ.
  Hence, $(\lambda - \mu)$ is an element in $I \setminus \langle \mu \rangle$, which is smaller than λ, contradicting the minimality of λ in $I \setminus \langle \mu \rangle$.
  $\therefore I = \langle \mu \rangle$ and hence $\mathbb{Z}$ is PID.

- $\mathbb{Z}[x]$ is NOT PID, since $I = \langle 2, x \rangle \neq \langle p \rangle$ for any $p \in \mathbb{Z}[x]$ which could be proven in HW9.

- For any field $\mathbb{F}$ (e.g. $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$), $\mathbb{F}[x]$ is PID.

  Proof: Let I be an ideal of $\mathbb{F}$ which is nonzero. For any elements $p(x) \in I$, we can multiply unit $u \in \mathbb{F}$ st.: $u \cdot p(x) \in I$ is a **monic** polynomial (leading power coefficient is 1). Take a monic polynomial $p(x) \in I$ of smallest possible degree in I.
  Claim: $I = \langle p(x) \rangle$.
  Proof of claim: Suppose on contrary. Take monic $q(x) \in I \setminus \langle p(x) \rangle$ such that q is of smallest positive degree in $I \setminus \langle p \rangle$. Then $\deg(p) \leq \deg(q)$ by the minimality of $\deg(p)$ in I.
  Let $h(x) := q(x) - x^{\deg(q) - \deg(p)} \cdot p(x)$. Then:

  - $h(x) \in I$
  - $h(x) \notin \langle p(x) \rangle$
  - $\deg(h) < \deg(q)$

  Then $h \in I \setminus \langle p \rangle$ with degree $< \deg(q)$. Contradict! □

Note: We have division algorithm for $\mathbb{F}[x]$ just like the case of $\mathbb{Z}$:

$$p(x) = q(x)a(x) + r(x) \quad (\deg(r) < \deg(q))$$

and so we have Euclidean algorithm to find $\gcd(p(x), q(x))$ in $\mathbb{F}[x]$

3.9 Irreducible Elements and Unique Factorization Domain

Definition 3.54 (Irreducibility)**.** Let R be unital commutative ring. An element $a \in R$ is **irreducible** if the followings hold:
Whenever $\langle a \rangle \subseteq \langle b \rangle \subseteq R$ for some $b \in R$, we have $\langle a \rangle = \langle b \rangle$ or $\langle b \rangle = R$, i.e.: $\langle a \rangle$ is maximal among all principal ideals of R.

To understand what it means for $a \in R$ irreducible:

Lemma 3.55. *Let R be ID. Then:*
$(a \in R$ irreducible$) \Leftrightarrow ($whenever $a = xy$, we have $a \sim x$ or $a \sim y)$
(Recall $a \sim x \Leftrightarrow a = ux$ for unit u)

Proof: $(a \in R$ is irreducible $\Rightarrow (a = xy \Rightarrow a \sim x$ or $a \sim y))$:
Suppose $a = xy$. Then $a \in \langle x \rangle$ and $a \in \langle y \rangle$. $\Rightarrow \langle a \rangle \subseteq \langle x \rangle$ and $\langle a \rangle \subseteq \langle y \rangle$. By definition of "a irreducible", $\langle a \rangle = \langle x \rangle$ or $\langle x \rangle = R$.

- $\langle a \rangle = \langle x \rangle \Leftrightarrow a \sim x$, then we're done
- $\langle x \rangle = R \Rightarrow \exists x' \in R$, s.t.: $xx' = 1 \in \langle x \rangle = R \Rightarrow x$ is a unit $\Rightarrow a \sim y$.

$((a = xy \Rightarrow a \sim x$ or $a \sim y) \Rightarrow (a \in R$ is irreducible$))$:
Suppose $\langle a \rangle \subseteq \langle b \rangle$ for some b. (WTS: $\langle b \rangle = \langle a \rangle$ or $\langle b \rangle = R$).
$\Rightarrow a = b \cdot b'$ for some $b' \in R \Rightarrow a \sim b$ or $a \sim b'$. Then

- $\langle a \rangle = \langle b \rangle$, then we're done
- $a = ub'$ for some unit $u \Rightarrow u = b$ by cancellation $\Rightarrow \langle b \rangle = R$, then we're done. □

Remark 3.56. As a corollary of lemma, a is irreducible $\Leftrightarrow \nexists b, c$ such that $a = bc$, and $b, c \notin U(R)$ (non-units).
$\therefore$ we can "factorize" a into "smaller" elements b & c. So we can factorize all $a \in R$ into product of irreducibles.
$\therefore$ Irreducible elements are "building blocks" of R.

Proposition 3.57. *Let R be ID. If $0 \neq a \in R$ is prime, then a is irreducible.*

Proof: Suppose $a = xy$ (WTS: $a \sim x$ or $a \sim y$)
Then $a \in \langle x \rangle$ and $a \in \langle y \rangle \Rightarrow \langle a \rangle \subseteq \langle x \rangle$ and $\langle a \rangle \subseteq \langle y \rangle$
On the other hand, we have $a \mid xy \xrightarrow{\text{(a prime)}} a \mid x$ or $a \mid y$
WLOG, assume $a \mid x$. Then $aa' = x \Rightarrow \langle x \rangle \subseteq \langle a \rangle \Rightarrow \langle a \rangle = \langle x \rangle$. □

CONCLUSION: R **PID.**
$\langle a \rangle$ maximal $\Leftrightarrow \langle a \rangle$ prime $\Leftrightarrow a$ is irreducible
(e.g.: $\langle x \rangle$ in $\mathbb{Z}[x]$ is prime but $\underline{\text{NOT}}$ maximal ;
3 in $\mathbb{Z}[\sqrt{-5}]$ is irreducible but $\overset{\langle 3 \rangle}{\text{NOT}}$ prime)

WRAP-UP:

- All $a \in R$ can be factorized into irreducibles
- Primes are irreducibles

If we want $a \in R$ to be factorized into primes, we need "all irreducibles are primes" instead.

Proposition 3.58. *Let R be PID. Then all irreducibles are primes.*

Proof: Let $x \in R$ be irreducible. Then $\langle x \rangle$ is maximal among all ideals of the form $\langle b \rangle$.
Since all ideals are of the form $\langle b \rangle$ in PID, then $\langle x \rangle$ is a maximal ideal.
$\Leftrightarrow \langle x \rangle$ is prime ideal $\Rightarrow x$ is prime. □

Definition 3.59. Let R be ID. We say R is a **factorization domain** if for all $0 \neq x \in R$, there exists irreducible elements $x_1, \dots, x_r$ such that $x \sim x_1 x_2 \dots x_r$ (or $x = u x_1 x_2 \dots x_r$ for some unit $u \in U(R)$), i.e.: one can factorize any x into a <u>finite</u> product of irreducibles.

Theorem 3.60. *R is PID $\Rightarrow$ R is factorization domain.*

Definition 3.61. Let R be unital commutative. We say R has the **ascending chain condition** on **principal ideals** (ACCP) if all $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ ($I_n \triangleleft R$ principal ideals), there exists N such that $I_N = I_{N+1} = I_{N+2} = \dots$

Lemma 3.62. *All PIDs satisfies (ACCP).*

Proof: Suppose $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ principal ideals in R. Consider $I := \bigcup_{n=1}^{\infty} I_n$ (HW 10: $I \triangleleft R$).
So $I = \langle r \rangle$ for some $r \in R$.
Since R is PID, then $r \in I_M$ for $M \in \mathbb{N} \Rightarrow r \in I_n \quad \forall n \geq M$.
$\Rightarrow I = \langle r \rangle \subseteq I_n \quad \forall n \geq M$.
Since $I_n \subseteq I$ by defn of I, then $I_n = I \quad \forall n \geq M$. □

Lemma 3.63. *If R satisfies (ACCP), then R is a factorization domain.*
(Consequently, all PIDs are factorization domains)

Proof: Let $F := \{x \in R \mid x \sim x_1 \dots x_r, x_i \text{ irreducibles}\}$ (W.T.S.: $R = F$).
Then: (a) $1 \in F$ (by convention); (b) all irreducibles $x \in R$ are in F ($r = 1$); (c) F is closed under multiplication.
Suppose on contrary, $\exists x_0 \in R \setminus F$. Then by (b), x_0 is reducible.
Then $x_0 = y_0 z_0$ where y_0, z_0 are <u>NOT</u> units. ($x_0 \nsim y_0$ & $x_0 \nsim z_0$)
$\Leftrightarrow \langle x_0 \rangle \neq \langle y_0 \rangle$
By (c), either $y_0 \in R \setminus F$ or $z_0 \in R \setminus F$ (or both). WLOG let $x_1 := y_0 \in R \setminus F$. Hence, $x_0 = x_1 z_0 \Rightarrow x_0 \in \langle x_1 \rangle \Rightarrow \langle x_0 \rangle \subsetneq \langle x_1 \rangle$ (and $\langle x_1 \rangle \neq R$, since x_1 is NOT unit).
Continue same argument on x_1, we have $\langle x_0 \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \dots$ contradicting (ACCP) which says $\exists N$ s.t.: $\langle x_N \rangle = \langle x_{N+1} \rangle = \dots$
$\therefore$ There's no such $x_0 \in R \setminus F$ and hence $R = F$. □

CONCLUSION: In PID, one can factorize any $x \in R$ into finite product of irreducibles.
Q: Is the factorization unique?

Proposition 3.64. *Let R be an ID. Then any factorizations of $x \in R$ into PRIME factors are unique (up to permutation and units), i.e.: if $x_1 \dots x_r \sim y_1 \dots y_s$ (x_i, y_j nonunit PRIMES). Then: (1) $r = s$, and (2) $\exists \sigma \in S_r$ s.t.: $x_i \sim y_{\sigma(i)}$*

(Consequently, if R is PID, then we can factorize any $x \in R$ uniquely into (irreducibles $\Leftrightarrow$ primes).)

Proof: We'll prove the following stronger statement:
Let $x_1, \dots, x_r$ primes, $y_1, \dots, y_n$ irreducibles (e.g.: y_j primes) s.t.:
$(*) : x_1 x_2 \dots x_r \sim y_1 y_2 \dots y_n$, then $r = n$ & $\exists \sigma \in S_r$ s.t.: $x_i \sim y_{\sigma(i)}$
Proof by induction on r.
Basic Case: $r = 0$, then the left-hand-side $= 1$. $\therefore y_1 y_2 \dots y_n \sim 1$
$\therefore y_j$ units $\forall j$. Since we assume x_i, y_j nonunits, must have $n = 0$.
Inductive Step: Suppose $(*)$ holds for $0 \leq r \leq s-1$. Consider $r = s$ and $u x_1 \dots x_{s-1} x_s = y_1 y_2 \dots y_n$ with u unit. (x_i primes, y_j irreducible, nonunits)
$\Rightarrow x_s \mid y_1 y_2 \dots y_n \Rightarrow x_s \mid y_j$ for some j. $\Rightarrow y_j = x_s \cdot a$ for some $a \in R$.
$\Rightarrow y_j \sim x_s$ or $y_j \sim a \xleftrightarrow{y_j \text{ irreducible}} y_j \sim x_s \Rightarrow x_1 \dots x_{s-1} \sim y_1 \dots y_{j-1} y_{j+1} \dots y_n$
Then by inductive hypothesis, $s - 1 = n - 1$ and $\exists \sigma \in S_{s-1}$ s.t.: $x_i \sim y_{\sigma(i)} \forall i$
$\therefore$ Let $\sigma' \in S_s$ by $\sigma' := \begin{cases} \sigma(i), \text{if } i = 1, \dots, s-1 \\ j, \text{if } i = s \end{cases}$
$\therefore x_1 \dots x_{s-1} x_s \sim y_1 \dots y_n$ implies $\exists \sigma' \in S_s$ s.t.: $x_i \sim y_{\sigma'(i)} \quad \forall i = 1, \dots, s$. □

Corollary 3.65. *Let R be PID. Then $\forall x \in R, x$ can be uniquely factorized into a finite product of irreducibles ($\Leftrightarrow$ primes).*
(This generalizes the fundamental thm of arithmetic from $R = \mathbb{Z}$ to any PID)

Definition 3.66. (UFD) Let R be ID. We say R is a **unique factorization domain** (UFD) if we have unique factorization into irreducible elements in R.
(Of course: R is PID $\Rightarrow$ R is UFD).

CONCLUSION:
ID $\supsetneq$ UFD $\supsetneq$ PID $\supsetneq$ ED (Euclidean domain) $\supsetneq$ Fields
(eg.: $\mathbb{Z}[\sqrt{-5}]$ is an ID (HW9: $(2 + \sqrt{-5}) \cdot (2 - \sqrt{-5}) = 3 \cdot 3$ is a non-unique factorization into irreducibles) ; $\mathbb{Z}[x]$ is a UFD (HW9: NOT PID ; later: it's UFD (Gauss' Lemma)) ; $\mathbb{Q}[x]$ is an ED.)

As in the case of PID, one has:
Proposition: Let R be UFD. Then p is prime iff p is irreducible.
Proof: p prime $\Rightarrow$ p irreducible $\forall$ ID. Now suppose p is irreducible. Consider $p \mid ab$ i.e.: $pc = ab$ for some $c \in R$. Factorize $a = a_1 \dots a_x$ and $b = b_1 \dots b_y$ into irreducibles. Then UF implies that either a_i or b_j associates p. Thus $p \mid a$ or $p \mid b$. □

Definition 3.67. (Euclidean Function) Let R be ID. A **<u>Euclidean function</u>** on R is $N : R\backslash\{0\} \to \mathbb{N}\setminus\{0\}$ s.t.: $\forall a, b \in R$, either (i) $b \mid a$, or (ii) $\exists q \in R, r \in R\setminus\{0\}$, s.t.: $a = bq + r$ with $N(r) < N(b)$.

Example 3.68.

- $R = \mathbb{Z}$, $N(m) := |m|$. Then (ii) is simply the division algorithm for integers.
- $R = \mathbb{F}[x]$, $N(p(x)) := \deg(p)$. Then (ii) is division algorithm for polynomials.

Definition 3.69. (Euclidean Domain) An ID R is a **Euclidean Domain** if R has (at least) one Euclidean function.
So $\mathbb{Z}, \mathbb{F}[x]$ are EDs.
If the Euclidean function ("norm function") N satisfies $N(ab) = N(a)N(b) \quad \forall a, b \in R$ we say N is **multiplicative**.
(eg.: $R = \mathbb{Z}, N(a) = |a|$ (multiplicative) ; $R = \mathbb{F}[x], N(p) = \deg(p)$ (**NOT** multiplicative))

Proposition 3.70. *$\mathbb{Z}[i]$ is a Euclidean domain with $N(a+bi) = a^2+b^2, \forall a, b \in \mathbb{Q}$. ($\mathbb{Z}[i] := \{a+bi \mid a, b \in \mathbb{Z}\}$ is called **Gaussian integers**)*
Proof: *Let $\alpha, \beta \in \mathbb{Z}[i]$. Assume $\beta \neq 0$. Then consider $\alpha/\beta = c_1 + c_2 i, c_i \in \mathbb{Q}$. Let $n_1, n_2 \in \mathbb{Z}$ be the closest integers of $c_1, c_2 \in \mathbb{Q}$ (so that $|n_i - c_i| \leq \frac{1}{2}$), and let $q := n_1 + n_2 i$. Hence, $\alpha/\beta = q + ((c_1 - n_1) + (c_2 - n_2)i)$.*
$\Rightarrow \alpha = \beta q + ((c_1-n_1)+(c_2-n_2)i)\beta$. Then $N[((c_1-n_1)+(c_2-n_2)i)\beta] = N((c_1-n_1)+(c_2-n_2)i) \cdot N(\beta)$ $\leq [(\frac{1}{2})^2 + (\frac{1}{2})^2]N(\beta) = \frac{1}{2}N(\beta) < N(\beta)$. □

Theorem 3.71. *If $R \in ED$, then $R \in PID$.*

Therefore, $\mathbb{Z}[i]$ is PID.
Q: What are the (primes $\Leftrightarrow$ irreducibles) in the Gaussian integer $\mathbb{Z}[i]$?
(eg. 5 is prime in $\mathbb{Z}$, but $5 = (2+i)(2-i)$ not prime in $\mathbb{Z}[i]$)
Simple Observations:

- If $n \in \mathbb{Z}$ is **NOT** prime in $\mathbb{Z}$, then n is <u>NOT</u> prime in $\mathbb{Z}[i]$.
- $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Therefore, $\alpha \in U(\mathbb{Z}[i]) \Leftrightarrow N(\alpha) = 1$.
- If $N(\beta) = p$ is prime in $\mathbb{Z}$, then β is prime in $\mathbb{Z}[i]$. (e.g.: $\beta = 2 + i$ is prime in $\mathbb{Z}[i]$, since $N(\beta) = 5$ in $\mathbb{Z}$)
  $\Rightarrow p = N(\beta) = N(\gamma)N(\delta) \Rightarrow N(\gamma) = 1$ or $N(\delta) = 1$. $\Rightarrow \gamma$ or δ is a unit in $\mathbb{Z}[i] \Rightarrow \beta \sim \gamma$ or $\beta \sim \delta$, i.e.: β is irreducible $\Leftrightarrow$ prime.

Lemma 3.72. *Let p be a prime integer. Then either (i) p is a Gaussian prime in $\mathbb{Z}[i]$, or (ii) $p = (a+bi)(a-bi)$ for some $(a+bi), (a-bi)$ Gaussian primes.*

Proof: Suppose p is **NOT** a Gaussian prime. Then $p = \gamma \cdot \delta$ for nonunits γ, δ. $\Rightarrow p^2 = N(p) = N(\gamma)N(\delta) \Rightarrow N(\gamma) = N(\delta) = p$
$\Rightarrow \gamma, \delta$ Gaussian primes.
$p = (a+bi)(c+di) \Rightarrow \bar{p} = p = (a-bi)(c-di) \Rightarrow p = (a+bi)(a-bi)$. □

Now let's study Gaussian primes of the form $a + bi$ $(a, b \neq 0)$.

Lemma 3.73. *Let $a+bi \in \mathbb{Z}[i]$ with $a,b \neq 0$. Then ($a+bi$ is Gaussian prime) $\Leftrightarrow$ ($a^2+b^2=p$, p prime integer).*

Proof: ($\Leftarrow$): is done in the simple observations.
($\Rightarrow$): Suppose $a+bi$ Gaussian prime. Then $a-bi = \overline{a+bi}$ is also Gaussian prime. Consider $(a+bi)(a-bi) = p_1 \dots p_r$, p_i prime in $\mathbb{Z}$, this is a factorization in $\mathbb{Z}[i]$. By $\mathbb{Z}[i]$ ED, $\mathbb{Z}[i]$ is PID $\Rightarrow$ UFD, $r \leq 2$. Suppose on contrary $r=2$. Then $(a+bi)(a-bi) = p_1p_2$.
By UFD again, p_1, p_2 must be (prime as irreducible) in $\mathbb{Z}[i]$.
$\therefore$ By UFD again, $p_1 \sim (a \pm bi)$, $p_2 \sim (a \mp bi) \Rightarrow p_1 = u \cdot (a \pm bi)$ where $u \in U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, contradicting $a, b \neq 0$.
$\therefore r = 1 \Rightarrow (a+bi)(a-bi) = p_1 \Rightarrow a^2+b^2 = p_1$. □

CONCLUSION:

(i) If $n \in \mathbb{Z}$ is **NOT** a prime number in $\mathbb{Z}$, then n is NOT Gaussian prime.

(ii) Prime $p \in \mathbb{Z}$ is either a Gaussian prime or $p = (a+bi)(a-bi)$, $a \pm bi$ Gaussian primes.

(iii) $a+bi \in \mathbb{Z}[i], a, b \neq 0$ is Gaussian prime $\Leftrightarrow a^2+b^2 = p$, $p \in \mathbb{Z}$ prime number.

Theorem 3.74. *Let p be a prime integer. Then p is Gaussian prime $\Leftrightarrow p \equiv 3 \pmod 4$.*

Proof: ($\Leftarrow$) contrapositive. If p is NOT Gaussian prime. Then (ii) says $p = (a+bi)(a-bi) = a^2+b^2 \equiv 0 \pmod 4$ or $1 \pmod 4$ or $2 \pmod 4$.
$\Rightarrow p \not\equiv 3 \pmod 4$.
($\Rightarrow$) Contrapositive. Suppose $p \equiv 1 \pmod 4$. Then by [Lagrange's Lemma], $p \mid m^2+1$ for some integer m. $\Rightarrow p \mid (m+i)(m-i)$. But $p \nmid m+i$, otherwise we have $p \cdot \gamma = m+i$ for $\gamma \in \mathbb{Z}[i] \Rightarrow \gamma = \frac{m}{p} + \frac{1}{p}i \notin \mathbb{Z}[i]$. Similarly $p \nmid m-i$.
$\therefore p$ is **NOT** a prime in $\mathbb{Z}[i]$. □

Corollary 3.75. *The Gaussian primes in $\mathbb{Z}[i]$ must be of the form*
(i) $p \in \mathbb{Z}$, $p \equiv 3 \pmod 4$ or (ii) $a+bi \in \mathbb{Z}[i]$, $a,b \neq 0$, $a^2+b^2 = p$
(or $p \in \mathbb{Z}$, $p \equiv 3 \pmod 4$)
(This is classification of all primes in $\mathbb{Z}[i]$.)

Corollary 3.76. *(Fermat's Theorem of 2 squares).*
If $p = 4n+1$ is a prime , then $\exists\ a,b \in \mathbb{Z}$ s.t.: $p = a^2+b^2$
(e.g.: $5 = 1^2+2^2$, $13 = 2^2+3^2$, $17 = 1^2+4^2$, $1013 = ?^2 + ?^2$)

Proof: By above, p is **NOT** a Gaussian prime, so $p = (a+bi)(a-bi)$ by (ii). $\therefore p = a^2+b^2$. □

One other application: (HW 10)
The integer solutions (x,y,z) of the equation $x^2+y^2=z^2$ are all of the form $x = (m^2-n^2)k$, $y = (2mn)k$, $z = (m^2+n^2)k$ for integers m,n,k.

Theorem 3.77. *If R is ED , then R is PID .*

Proof: Let N be the "norm function" of R . For any $I \lhd R$, take any $a \in I \setminus \{0\}$ such that $N(a) > 0$ is minimal among all $r \in R$. Now for any $i \in R$, one has $a|i$ or $i = aq + r$ with $N(r) < N(a)$. But $r = i - aq \in I$ with smaller norm than a. Contradict.
$\therefore a|i \Rightarrow i = aq \in \langle a \rangle$ Hence , $I = \langle a \rangle$. □

3.10 Polynomial

In this section, we'll study ring of polynomials $R[x]$. A main reason why it is important is the following:

Theorem 3.78. *Let $\mathbb{F}$ be a field. Suppose $f(x) \in \mathbb{F}[x]$ is irreducible, then $\mathbb{F}[x]/\langle f(x) \rangle$ is a field.*

Proof: Since $\mathbb{F}[x]$ is ED, then PID. $I = \langle f(x) \rangle$ is prime, since $f(x)$ is irreducible $\Leftrightarrow$ prime. Therefore, $I = \langle f(x) \rangle$ is a maximal ideal, and the result follows from Section on max/prime ideals. As a consequence, one has an injective homomorphism of fields $\phi : \mathbb{F} \to \mathbb{F}[x]/\langle f(x) \rangle =: \mathbb{K}$ with $\phi(a) := a + \langle f(x) \rangle$, i.e.: we can "extend" $\mathbb{F}$ to a large field.

> **Galois theory**: Understand roots of (irreducible) polynomials $f(x) \in \mathbb{F}[x]$
> As before, we write $\overline{x} := x + \langle f(x) \rangle \in \mathbb{K}$.
> Then in $\mathbb{K}$, $f(\overline{x}) = f(x) + \langle f(x) \rangle = 0_{\mathbb{K}}$.
> So $\overline{x}$ is a root of $f(x)$ in $\mathbb{K}$!

Now we know the importance of studying when a polynomial is irreducible. In this section, we'll offer ways to check whether $p \in \mathbb{Q}[x]$ (or $\mathbb{Z}[x]$) is irreducible.
Although $\mathbb{Z}$ is **NOT** a field, it is useful in understanding whether $p(x) \in \mathbb{Q}[x]$ with $\mathbb{Z}$-coefficients in irreducible or not.

Lemma 3.79. *Let $\phi : R \to S$ be unital ring homomorphism (e.g.: $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_p$). Then $\tilde{\phi} : R[x] \to S[x]$ with $\tilde{\phi}(a_0 + a_1 x + \cdots + a_n x^n) := \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$ is a unital ring homomorphism.*

Theorem 3.80. *(Reduction Test) Let $f \in \mathbb{Z}[x]$ monic, p prime such that $\tilde{\phi}(f) \in \mathbb{Z}_p[x]$ is irreducible. Then f is irreducible.*

Proof: Let $f = gh$ (WTS: g or $h \in \mathbb{Z}[x]$ are constant)
$\Rightarrow \tilde{f} = \tilde{g}\tilde{h}$ in $\mathbb{Z}_p[x]$
Since f is monic, g and h are monic (up to units ± 1) and hence $\tilde{f}, \tilde{g}, \tilde{h}$ monic with $\deg(\tilde{g}) = \deg(g)$, $\deg(\tilde{h}) = \deg(h)$.
But since $\tilde{f}$ is irreducible, then $\deg(\tilde{g})$ or $\deg(\tilde{h}) = 0$.
$\Rightarrow \deg(g)$ or $\deg(h) = 0$. □

Example 3.81. $f(x) = x^3 + 3x + 7 \xrightarrow{p=2} \tilde{f} = \tilde{\phi}(f) = x^3 + x + 1$
$\tilde{f}$ cannot be factorized into $\tilde{g} \cdot \tilde{h}$, since if so either $\deg(\tilde{g})$ or $\deg(\tilde{h}) = 1$, i.e.: $\tilde{g}$ or $\tilde{h} = x$ or $x + 1$.
By factor theorem, this implies $\tilde{f}(0)$ or $\tilde{f}(1) = 0$ in $\mathbb{Z}_2$.

Theorem 3.82. *(Eisenstein's criterion) Suppose $f(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ is such that* $\gcd(a_n, \ldots, a_1) = 1$ *(f is primitive) and p prime number such that:*
(1) $p \mid a_i \quad \forall 0 \le i < n$; (2) $p \nmid a_n$; (3) $p^2 \nmid a_0$.
Then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

(e.g.: $f(x) = x^4 + 4x + 6 \quad (p = 2)$ is irreducible)

Proof: Use $\sim: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Then consider $f = gh \in \mathbb{Z}[x]$
(WTS: g or h is constant) .
$\tilde{f} = [a_n]x^n \in \mathbb{Z}_p[x]$ by (1) where $[a_n] \neq [0]$ in $\mathbb{Z}_p$ by (2)
$\Rightarrow \tilde{g} \cdot \tilde{h} = \tilde{f} \sim x^n$. Then $\tilde{g} \sim x^i$; $\tilde{h} \sim x^{n-i} \quad (0 \le i \le n)$
Suppose $i \neq 0, n$. Then $\tilde{g} \sim x^i \Rightarrow$ constant term of g is a multiple of p . Similarly , $\tilde{h} \sim x^{n-i} \Rightarrow$ constant term of h is also multiple of p .
$\Rightarrow$ constant term of $f = gh$ is a multiple of p^2 , which contradict (3) of Eisenstein's criterion .
$\therefore \tilde{g}$ or $\tilde{h}$ is a constant function in $\mathbb{Z}_p[x]$ —— (*)
Now:

- $\deg(g) + \deg(h) = \deg(f) = \deg(\tilde{f}) = \deg(\tilde{g}) + \deg(\tilde{h})$.
- $\deg(\tilde{g}) \le \deg(g)$; $\deg(\tilde{h}) \le \deg(h)$

$\therefore \deg(\tilde{g}) = \deg(g)$; $\deg(\tilde{h}) = \deg(h)$
$\therefore \deg(g)$ or $\deg(h) = 0$ by (*) , so either g or h is constant polynomial. □

Example 3.83. $g(x) = x^4+1$. Consider $f(x) = g(x+1) = (x+1)^4+1 = x^4+4x^3+6x^2+4x+1+1 = x^4 + 4x^3 + 6x^2 + 4x + 2$. Since $2 \mid 4, 6, 4, 2$ and $2^2 \nmid 2$, then $f(x)$ (and $g(x)$) is irreducible.

Q: How about irreducibility in $\mathbb{Q}[x]$?

Theorem 3.84. *(Gauss' Lemma) A nonconstant polynomial $f \in \mathbb{Z}[x]$ is irreducible $\Leftrightarrow$ $f \in \mathbb{Q}[x]$ is irreducible and f is primitive.*

Proof: ($\Leftarrow$) Suppose $f \in \mathbb{Z}[x]$ and $f = g \cdot h$, $g, h \in \mathbb{Z}[x]$.
(WTS: g or h is a unit in $\mathbb{Z}[x]$)
By hypothesis, f is irreducible in $\mathbb{Q}[x]$ and $g, h \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, therefore, $\deg(g) = 0$ or $\deg(h) = 0$.
$\Rightarrow g$ or h must be a constant integer.
By hypothesis again, since f is primitive, this constant integer can only be 1 or -1. $\Rightarrow g$ or h is a unit in $\mathbb{Z}[x]$.
($\Rightarrow$) If f is irreducible in $\mathbb{Z}[x]$, then obviously f is primitive. Otherwise $f = a_nx^n + \cdots + a_0$ and $2 \le d = \gcd(a_n, \ldots, a_0)$, then $f = d \cdot [\frac{a_n}{d}x^n + \cdots + \frac{a_0}{d}]$ where d and $[\frac{a_n}{d}x^n + \cdots + \frac{a_0}{d}]$ are both NOT units in $\mathbb{Z}[x]$ contradicting f irreducible in $\mathbb{Z}[x]$.
To see why f is irreducible in $\mathbb{Q}[x]$, suppose $f = g \cdot h$, $g, h \in \mathbb{Q}[x]$.
(WTS: g, h are units in $\mathbb{Q}[x]$, i.e.: $g, h \in \mathbb{Q} \setminus \{0\}$)
Let $\lambda, \mu \in \mathbb{N}$ be the smallest positive integers such that $\lambda \cdot g$ and $\mu \cdot h \in \mathbb{Z}[x]$. Let $g' = \lambda \cdot g$, $h' = \mu \cdot h \in \mathbb{Z}[x]$.

Claim: $\lambda = 1$: Suppose on contrary, $\exists p \mid \lambda$. Then "$p \mid \lambda f$" (which means the coefficients of $\lambda f \in \mathbb{Z}[x]$ are multiples of p).
$\Rightarrow p \mid (\lambda\alpha^{-1}g) \cdot (\alpha h) \Rightarrow$ "$p \mid g'h'$" in $\mathbb{Z}[x]$
Therefore, $\tilde{g}' \cdot \tilde{h}' \equiv 0$ in $\mathbb{Z}_p[x] \Rightarrow \tilde{g}' \equiv 0$ or $\tilde{h}' \equiv 0$ in $\mathbb{Z}_p[x]$
$\Rightarrow$ "$p \mid g'$" — (*) or "$p \mid h'$" — (**) in $\mathbb{Z}[x]$
In (*), "$p \mid g'$" $\Leftrightarrow$ "$p \mid \lambda\alpha^{-1}g$" $\Rightarrow (\frac{\lambda}{p})\alpha^{-1}g$, $\alpha h \in \mathbb{Z}[x]$, contradicting the minimality of λ.
In (**), "$p \mid \alpha h$" $\Rightarrow (\frac{\lambda}{p})(\frac{\alpha}{p})^{-1}g = \lambda\alpha^{-1}g \in \mathbb{Z}[x]$ and $(\frac{\alpha}{p})h \in \mathbb{Z}[x]$, contradicting the minimality of λ.
$\therefore p \nmid \lambda$ for any prime number, and $\lambda = 1$.
Therefore, we have $\alpha \in \mathbb{Q} \setminus \{0\}$ s.t.: $f = gh$ in $\mathbb{Q}[x]$ and $f = (\alpha^{-1}g)(\alpha h)$ in $\mathbb{Z}[x]$, since we have f irreducible in $\mathbb{Z}[x]$ by hypothesis, $\alpha^{-1}g$ or αh is a unit in $\mathbb{Z}[x] \Rightarrow \alpha^{-1}g = \pm 1$ or $\alpha h = \pm 1$.
$\Rightarrow g = \alpha'$ where $\alpha' \in \mathbb{Q} \setminus \{0\}$ or $h = \alpha''$ where $\alpha'' \in \mathbb{Q} \setminus \{0\}$. □

Theorem 3.85. *$\mathbb{Z}[x]$ is a UFD (but not PID by HW).*

Proof: Let $f \in \mathbb{Z}[x]$ be primitive.
Claim: f can be factorized into $f = g_1 \dots g_n$, $g_i \in \mathbb{Z}[x]$ primitive irreducible. To see why, use induction on $\deg(f)$. True for $\deg(f) = 0$ or 1. So assume claim holds for $\deg(f) < k$ Then for f with $\deg(f) = k$ and primitive:
• f is irreducible ; • $f = h_1h_2$, $h_1, h_2 \in \mathbb{Z}[x]$ NOT units.
If $\deg(h_1)$ or $\deg(h_2) = 0$, then h_1 or h_2 equal to constant $\neq \pm 1$ contradicting f is primitive. Hence, $\deg(h_1) \& \deg(h_2) > 0$ by induction. To see why $\mathbb{Z}[x]$ is UFD, note that we can factorize any primitive $f \in \mathbb{Z}[x]$ into irreducibles (primitive).
To see the factorization is unique, suppose $f = g_1 \dots g_n = h_1 \dots h_m$, $g_i, h_j \in \mathbb{Z}[x]$ primitive irreducible. Then since $\mathbb{Z}[x] \subseteq$ ($\mathbb{Q}[x]$ UFD) and by Gauss' Lemma $g_i, h_j \in \mathbb{Q}[x]$ irreducible by unique factorization of $\mathbb{Q}[x]$, we have $n = m$, and $\exists \sigma \in S_n$, s.t.: $g_i \sim h_{\sigma(i)}$ (in $\mathbb{Q}[x]$) $\Rightarrow g_i = h_{\sigma(i)} \cdot u$ where $u \in$ (unit in $\mathbb{Q}[x]$) Since $g_i, h_{\sigma(i)}$ primitive, $u \in \{\pm 1\} \Rightarrow g_i \sim h_{\sigma(i)}$ in $\mathbb{Z}[x]$. □

Remark (more generally):
If R is a UFD, then $R[x]$ is UFD. To prove it, use Field of Fractions (HW ?) $F = \mathrm{Frac}(R)$ and the fact that $F[x]$ is a PID ($\Rightarrow$ UFD).

Chapter 4

Fields

Recall: F is a field if F is an integral domain (unital) and for all $x \in F \setminus \{0\}$, there exists a multiplicative inverse $x^{-1} \in F \setminus \{0\}$.

In general, there are 3 kinds of fields:

1. **Number field** (a subfield of $\mathbb{C}$)
   (e.g., $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}(i)$, ...)
2. **Finite field** (a field F with $|F| < \infty$)
   (e.g., $\mathbb{Z}_p = \mathbb{F}_p$ for p prime. $\mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$ has $8 = 2^3$ elements.)
3. **Function fields**
   (e.g., $\mathbb{C}(x) = \text{Frac}(\mathbb{C}[x]) = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{C}[x], g(x) \neq 0\}$)

We'll only focus on (1) or (2).

4.1 Field Extension and Degree

Motivation: Given a field F, construct a "bigger" field K that "contains" F.

For example, let $F = \mathbb{F}_2$ and $K = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$. Then we have an injective unital ring (or field) homomorphism $i : F \to K$ where $i(0) = 0 + \langle x^3 + x + 1\rangle$ and $i(1) = 1 + \langle x^3 + x + 1\rangle$. So we say K "contains" F.

Definition 4.1. Let F and K be fields. We say F is a **subfield** of K or K is a **field extension** of F if there is an injective unital field homomorphism $i : F \to K$.

In this case, K is a vector space over F. There is a scalar multiplication map $\cdot : F \times K \to K$ defined by $\alpha \cdot x = i(\alpha)x$ for $\alpha \in F, x \in K$, that satisfies:

- $0 \cdot x = 0$
- $1 \cdot x = x$
- $\alpha \cdot (x + y) = (\alpha \cdot x) + (\alpha \cdot y)$
- ...

The **degree** of extension is defined as:

$$[K : F] := \dim_F(K) \quad \text{(as a vector space over } F\text{)}$$

Example 4.2. 1. $F = \mathbb{R}$, $K = \mathbb{C}$, with the inclusion $i : \mathbb{R} \hookrightarrow \mathbb{C}$.
Then $[\mathbb{C} : \mathbb{R}] = 2$, since $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\} = \mathrm{span}_{\mathbb{R}}\{1, i\}$.
Thus, $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ (since $\{1, i\}$ is linearly independent over $\mathbb{R}$).

2. $F = \mathbb{Q}$, $K = \mathbb{R}$, with the inclusion $i : \mathbb{Q} \hookrightarrow \mathbb{R}$.
To find $[\mathbb{R} : \mathbb{Q}]$, consider that $\mathbb{R} = \mathrm{span}_{\mathbb{Q}}\{1, \sqrt{2}, \sqrt{3}, e, \pi, \dots\}$.
The set of transcendental numbers like e, π is infinite and they are linearly independent over $\mathbb{Q}$. Thus, $[\mathbb{R} : \mathbb{Q}] = \infty$.

4.2 Splitting Extension

In field theory, we want to understand roots of polynomials $p(x) \in F[x]$. More precisely, we would like to construct $E : F$ such that E contains some (or all) roots of $F[x]$. The first step is the following:

Theorem 4.3 (Kronecker)**.** *Let F be a field, and $p(x) \in F[x]$ be an irreducible polynomial of degree m. Then $K = F[x]/\langle p(x)\rangle$ is a field extension of F such that $[K : F] = m$. Moreover, there exists an element $\alpha \in K$ such that:*

- $K = F[\alpha] := \{a_n\alpha^n + \cdots + a_1\alpha + a_0 \mid a_i \in F, n \in \mathbb{N}\}$.
- $p(\alpha) = 0$ *in* K.

Proof. Since $p(x) = b_m x^m + \cdots + b_1 x + b_0 \in F[x]$ is irreducible, the ideal $\langle p(x)\rangle$ is a maximal ideal in $F[x]$. This implies that $K = F[x]/\langle p(x)\rangle$ is a field.

Let's study the dimension, $\dim_F(K)$. Consider the element $\alpha := x + \langle p(x)\rangle \in K$. Then in K,

$$\begin{aligned} p(\alpha) &= b_m\alpha^m + \cdots + b_1\alpha + b_0 \\ &= b_m(x + \langle p(x)\rangle)^m + \cdots + b_1(x + \langle p(x)\rangle) + b_0(1 + \langle p(x)\rangle) \\ &= (b_m x^m + \cdots + b_1 x + b_0) + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle = 0_K \end{aligned}$$

So, the second part of the theorem is proved. Moreover, this also implies that

$$\alpha^m = -\frac{1}{b_m}(b_{m-1}\alpha^{m-1} + \cdots + b_0)$$

i.e. the set $\{1, \alpha, \dots, \alpha^m\}$ is linearly dependent in K. More precisely, α^m is a linear combination of $\{1, \alpha, \dots, \alpha^{m-1}\}$. Similarly, for any $n \geq m$, α^n is also a linear combination of $\{1, \alpha, \dots, \alpha^{m-1}\}$.

Claim: The set $\{1, \alpha, \dots, \alpha^{m-1}\}$ is a basis of K over F.

Spanning set: Take any element $k \in K$. By definition, $k = (c_l x^l + \cdots + c_1 x + c_0) + \langle p(x) \rangle$ for some $c_i \in F$. This is equal to $c_l \alpha^l + \cdots + c_1 \alpha + c_0$. Since all powers α^j for $j \geq m$ can be reduced to a linear combination of $\{1, \alpha, \ldots, \alpha^{m-1}\}$, any element $k \in K$ can be written as a linear combination of these basis elements. Thus, $K = \text{Span}_F\{1, \alpha, \ldots, \alpha^{m-1}\}$.

Linearly independent: Suppose $d_{m-1}\alpha^{m-1} + \cdots + d_1\alpha + d_0 = 0_K$ for some $d_i \in F$, not all zero. This is equivalent to $(d_{m-1}x^{m-1} + \cdots + d_1 x + d_0) + \langle p(x) \rangle = 0_K$. Let $g(x) = d_{m-1}x^{m-1} + \cdots + d_0$. The equation means $g(x) \in \langle p(x) \rangle$. This implies that $p(x)$ divides $g(x)$, i.e., $g(x) = p(x) \cdot r(x)$ for some $r(x) \in F[x]$. But this is a contradiction, because $\deg(g(x)) \leq m - 1$ while $\deg(p(x)) = m$. The degree of a non-zero polynomial $g(x)$ cannot be less than the degree of a non-zero polynomial $p(x)$ that divides it. Thus, $g(x)$ must be the zero polynomial, which means all d_i must be zero. The set is linearly independent.

Since $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis for K over F, the dimension is m. Therefore, $[K : F] = m$. □

Example 4.4. Let $F = \mathbb{Q}$, $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ (irreducible by Eisenstein's criterion). Then $[K : \mathbb{Q}] = 3$ for $K = \mathbb{Q}[x]/\langle x^3 - 2 \rangle$. Let $\alpha = x + \langle x^3 - 2 \rangle$. Then $K = \text{Span}_{\mathbb{Q}}\{1, \alpha, \alpha^2\} = \{a_2\alpha^2 + a_1\alpha + a_0 \mid a_i \in \mathbb{Q}\}$. We know $\alpha^3 - 2 = 0$, so $\alpha^3 = 2$. K is a field that contains $\mathbb{Q}$ and a cube root of 2. We also know how to do arithmetic in K, for instance:

$$\begin{aligned}(2\alpha^2 + \tfrac{3}{4}) \cdot (\alpha - 6) &= 2\alpha^3 - 12\alpha^2 + \tfrac{3}{4}\alpha - \tfrac{18}{4} \\ &= 2(2) - 12\alpha^2 + \tfrac{3}{4}\alpha - \tfrac{9}{2} \\ &= 4 - 12\alpha^2 + \tfrac{3}{4}\alpha - \tfrac{9}{2} \\ &= -12\alpha^2 + \tfrac{3}{4}\alpha - \tfrac{1}{2}\end{aligned}$$

Exercise: What is $\alpha^{-1} \in K$?

In the above example, under the extension $K : \mathbb{Q}$, one can treat the polynomial $p(x) = x^3 - 2 \in \mathbb{Q}[x] \subseteq K[x]$ under the extended field. By Kronecker's theorem, $p(x) \in K[x]$ has a root:

$$p(x) = (x - \alpha)(x^2 + \alpha x + \alpha^2) \in K[x]$$

However, K does not contain all the roots of $p(x)$.

Definition 4.5. Let F be a field, and $p(x) \in F[x]$. We say a field extension $E : F$ splits $p(x)$ if $p(x) = a(x - a_1) \cdots (x - a_n)$.

Proposition 4.6. *For any field F and any polynomial $p(x) \in F[x]$, there exists a field extension $E : F$ such that E splits $p(x)$.*

Proof. Prove by induction on the degree of $p(x)$ (for any base field F). If $p(x) \in F$ is of degree 1, we are done. By induction hypothesis, assume the theorem holds for all polynomials of degree $< k$ over any field. Consider a polynomial $p(x)$ of degree k. Let $f(x)$ be an irreducible factor of $p(x)$. Then take $K = F[x]/\langle f(x) \rangle$ so that $a := x + \langle f(x) \rangle \in K$ is a root of $f(x)$ and thus of $p(x)$. So

$p(x) = (x-a)g(x)$ in $K[x]$, where $\deg(g(x)) = k-1$. By the induction hypothesis, there exists an extension $E : K$ such that $g(x)$ splits in $E[x]$, say $g(x) = c(x-a_2)...(x-a_k)$. So we have $p(x) = c(x-a)(x-a_2)...(x-a_k)$ in $E[x]$, and we are done. □

Now we know for any $p(x) \in F[x]$, there is a field extension $E : F$ such that E contains all the roots of $p(x)$. We want to find 'the smallest' extension that contains all the roots of $p(x)$.

Definition 4.7. Let $E : F$ be a field extension, and $e_1, \dots, e_n \in E$. Write $F(e_1, \dots, e_n)$ for the smallest field extension of F containing $e_1, \dots, e_n$. In other words,

$$F(e_1, \dots, e_n) := \bigcap_{K \leq E,\ e_1, \dots, e_n \in K} K$$

Proposition 4.8. $F(e_1, e_2, \dots, e_n) = (F(e_1))(e_2, \dots, e_n) = \cdots = ((F(e_1)(e_2)) \dots (e_{n-1}))(e_n)$.

Proof. Easy. □

Definition 4.9. Suppose $E : F$ is a field extension such that E splits a polynomial $p(x) \in F[x] \subseteq E[x]$ with roots $a_1, \dots, a_n \in E$. Then a **splitting field** of $p(x)$ over F is the smallest subfield $F(a_1, \dots, a_n)$ of E containing all the roots a_i of $p(x)$ in E.

Example 4.10.

1. Let $p(x) = x^2 + 3x + 3 \in \mathbb{Q}[x]$. Then for $E = \mathbb{Q}[x]/\langle p(x) \rangle$, the polynomial $p(x)$ splits automatically into $(x-a)(x-b)$. So $\mathbb{Q}(a, b) = \mathbb{Q}[x]/\langle p(x) \rangle$ is a splitting field.

   On the other hand, $p(x)$ splits in $\mathbb{C}$ and the roots are $-3/2 \pm i\sqrt{3}/2$. So $\mathbb{Q}(i\sqrt{3})$ is also a splitting field of $p(x)$.

2. Let $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Then $F = \mathbb{Q}[x]/\langle x^3 - 2 \rangle$ has a root $\alpha \in E$. We can form $E = F[x]/\langle x^2 + \alpha x + \alpha^2 \rangle$. The field E is a splitting field, which we can write as $\mathbb{Q}(a, b, c)$ where a, b, c are the roots.

   On the other hand, working in $\mathbb{C}$, the roots are $2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2$ (where $\omega = e^{i2\pi/3}$). Then $\mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2) = \mathbb{Q}(2^{1/3}, \omega)$ is also a splitting field of $p(x)$.

Theorem 4.11. *(will prove in MAT5210) All splitting fields of the same polynomial are isomorphic.*

4.3 Simple Extension

In the previous section, we begin with a irreducible polynomial $p(x) \in F[x]$, and extend to E so that E contains some (or all) roots of $p(x)$. In this section, we change our perspective a little bit – we begin with a field extension $E : F$, and see which elements in E are roots of a polynomial $p(x) \in F[x]$. Such $E : F$ always exists by the virtue of the previous section.

Definition 4.12. Let F be a field and L be a field extension of F (e.g., $F = \mathbb{Q} \subseteq L = \mathbb{C}$). An element $\alpha \in L$ is

- **algebraic** if there exists a non-zero polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$ (in L).
- Otherwise, α is called **transcendental**.

Example 4.13 (Elements over $\mathbb{Q}$)**.**

- $i = \sqrt{-1}$ is algebraic over $\mathbb{Q}$ (its polynomial is $p(x) = x^2 + 1$).
- $\sqrt[4]{2}, \sqrt{3}$ are algebraic over $\mathbb{Q}$ (their polynomials are $p(x) = x^4 - 2$ and $x^2 - 3$, respectively).
- $\sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$ (HW12).
- e, π are transcendental over $\mathbb{Q}$ (there is NO polynomial with $\mathbb{Q}$-coefficients having e or π as a root).

Theorem 4.14. *If α is transcendental over F, then $F[\alpha] \cong F[x]$ as rings (but not as fields).*

As for β algebraic:

Proposition 4.15. *Let $\beta \in L$ be algebraic over F. Consider the set $I = \{f(x) \in F[x] \mid f(\beta) = 0\}$. Then:*

1. *I is a non-zero ideal in $F[x]$.*
2. *$I = \langle p(x) \rangle$ for some unique monic polynomial $p(x) \in F[x]$. (This is because $F[x]$ is a PID).*
3. *$p(x)$ is the unique monic polynomial of smallest degree in I.*
4. *$p(x)$ is irreducible.*

*This polynomial $p(x)$ is called the **minimal polynomial** of β over F.*

Proof. (a) Let's show $p(x)$ has the smallest degree. By the division algorithm, suppose on the contrary there exists $g(x) \in I$ with $\deg(g) < \deg(p)$. Since $I = \langle p(x) \rangle$, $g(x)$ must be a multiple of $p(x)$, which is impossible unless $g(x) = 0$. Contradiction.

(b) Let's show $p(x)$ is irreducible. Suppose on the contrary that $p(x) = h_1(x)h_2(x)$ with $\deg(h_1) > 0$ and $\deg(h_2) > 0$. Then $p(\beta) = h_1(\beta)h_2(\beta) = 0$ in the field L. This implies that either $h_1(\beta) = 0$ or $h_2(\beta) = 0$. This means either $h_1(x) \in I$ or $h_2(x) \in I$. But $\deg(h_1) < \deg(p)$ and $\deg(h_2) < \deg(p)$, which contradicts the fact that $p(x)$ is a polynomial of smallest degree in I. Thus, $p(x)$ must be irreducible. □

Definition 4.16. Let F be a field, $\beta \in L$ (a field extension of F). The polynomial $m_\beta(x) := p(x)$ appearing in Proposition 4.15 above is called the **minimal polynomial** of β over F.

Example 4.17. Minimal polynomials over $\mathbb{Q}$:

- For $\beta = i$, the minimal polynomial is $m_\beta(x) = x^2 + 1$.
- For $\beta = \sqrt[4]{2}$, the minimal polynomial is $m_\beta(x) = x^4 - 2$.
- For $\beta = e^{2\pi i/5}$, the minimal polynomial is $m_\beta(x) = x^4 + x^3 + x^2 + x + 1$.
  (Since $\beta^5 = 1$, and $x^5 - 1 = (x-1)p(x)$).

Theorem 4.18. *Let $L : F$ be a field extension, and $\beta \in L$ be algebraic. Then the smallest field extension $F(\beta) : F$ containing β is equal to the polynomial ring $F[\beta]$, which is isomorphic to $F[x]/\langle m_\beta(x)\rangle$.*

Proof. Consider the ring homomorphism $\phi : F[x] \to F[\beta]$ defined by evaluation at β:

$$\phi(a_n x^n + \cdots + a_0) = a_n \beta^n + \cdots + a_0$$

The kernel of this map is precisely the ideal $I = \{f(x) \in F[x] \mid f(\beta) = 0\}$, which we know is equal to $\langle m_\beta(x)\rangle$. So the result follows by the First Isomorphism Theorem for rings. Since $\langle m_\beta(x)\rangle$ is a maximal ideal, $F[x]/\langle m_\beta(x)\rangle$ is a field, and therefore $F[\beta]$ is also a field. □

Definition 4.19. The field extension $F(\beta) := F[\beta]$ of F is called the **simple extension** of F by β.

Corollary 4.20. *If $\alpha, \beta \in L$ are algebraic over F and are roots of the same irreducible polynomial $p(x) \in F[x]$, then $F(\alpha) \cong F(\beta)$.*

Proof. $m_\alpha(x) = m_\beta(x) = p(x)$. So $F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F(\beta)$. □

Let $E : F$ be a field extension, and $\alpha_1, \ldots, \alpha_k \in E$ be algebraic over F. Then the field extension $F(\alpha_1, \ldots, \alpha_k)$ can be constructed inductively as follows: Define a sequence of fields by $F_0 = F$ and

$$F_{i+1} := F_i(\alpha_{i+1}) \cong \frac{F_i[x]}{\langle m^{F_i}_{\alpha_{i+1}}(x)\rangle} \quad \text{for } 0 \le i \le k-1.$$

where $m^{F_i}_{\alpha_{i+1}}(x) \in F_i[x]$ is the minimal polynomial of the element α_{i+1} over the field F_i. Then $F_k = F(\alpha_1, \ldots, \alpha_k)$.

4.4 Algebraic Extension

We have seen that a simple extension $F(\beta) : F$ contains an algebraic element β. What about the other elements in $F(\beta) = \mathrm{Span}_F\{1, \beta, \ldots, \beta^{\deg(m_\beta(x))-1}\}$? Are they algebraic? More generally, how about the non-simple extension $F(\beta_1, \ldots, \beta_k)$?

Definition 4.21. An extension $E : F$ is called **algebraic** if every element $\alpha \in E$ is algebraic over F.

Theorem 4.22. *If $[E : F] < \infty$ (i.e., it is a finite extension), then E is an algebraic extension of F.*

Proof. Suppose $[E : F] = n$. Then for any $\alpha \in E$, consider the set $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$. This is a set of $n+1$ elements in an n-dimensional vector space, so it must be linearly dependent over F. This implies there exist scalars $c_0, \ldots, c_n \in F$, not all zero, such that $c_0 \cdot 1 + c_1\alpha + \cdots + c_n\alpha^n = 0$. Thus, α is a root of the non-zero polynomial $p(x) = c_n x^n + \cdots + c_0 \in F[x]$, which means α is algebraic over F. Since α was arbitrary, the extension is algebraic. □

Corollary 4.23. *Let $E : F$ be a field extension, and $\beta_1, \dots, \beta_k \in E$ are algebraic over F. Then the extension $F(\beta_1, \dots, \beta_k) : F$ is algebraic.*

Proof. For the special case when $k = 1$, one has $[F(\beta) : F] = \deg(m_\beta(x))$ which is finite. The proof of the general case is given in Corollary 4.27 below. □

Theorem 4.24 (Primitive Element Theorem)**.** *Let F be a field with characteristic $char(F) = 0$. Let $a, b \in K$ be algebraic over F in some extension $K : F$. Then there exists an element $c \in F(a, b)$ such that $F(c) = F(a, b)$. (Such an element c is called a primitive element for the extension).*

Proof. Let $p(x)$ be the minimal polynomial of a over F. Let $q(x)$ be the minimal polynomial of b over F.

Take a field extension $L : K$ such that $p(x)$ and $q(x)$ split completely in $L[x]$. Suppose $a_1, \dots, a_m \in L$ are the roots of $p(x)$, with $a_1 = a$. Suppose $b_1, \dots, b_n \in L$ are the roots of $q(x)$, with $b_1 = b$.

Since $\text{char}(F) = 0$, the field F is infinite. This allows us to choose an element $d \in F$ such that

$$d \neq \frac{a_i - a_j}{b_k - b_l}$$

for all i, j and for all $k \neq l$. In particular, we choose $d \in F$ such that for any i and any $j > 1$:

$$d \neq \frac{a_i - a}{b - b_j}$$

(Note that the elements on the right-hand side may not be in F, but there are only a finite number of such values, so we can always find a $d \in F$ that avoids them).

Consider the element $c := a + db$. Then, it is clear that $F(c) \subseteq F(a, b)$ since $a, b \in F(a, b)$ and $d \in F \subseteq F(a, b)$.

To show the other inclusion, $F(a, b) \subseteq F(c)$, it is enough to show that $b \in F(c)$, because if $b \in F(c)$, then $a = c - db \in F(c)$ as well.

Consider the polynomials $r(x) = p(c - dx)$ and $q(x)$, both viewed as polynomials in $F(c)[x]$. We evaluate both polynomials at b:

- $r(b) = p(c - db) = p(a) = 0$.
- $q(b) = 0$.

Let $m(x) \in F(c)[x]$ be the minimal polynomial of b over the field $F(c)$. Since b is a root of both $r(x)$ and $q(x)$ (which are in $F(c)[x]$), it must be that $m(x)$ divides both $r(x)$ and $q(x)$ in $F(c)[x]$.

$$m(x) \mid r(x) \quad \text{and} \quad m(x) \mid q(x)$$

Now let's study the polynomial $m(x) \in F(c)[x] \subseteq L[x]$.

Since $m(x) \mid q(x)$ and $q(x)$ splits in $L[x]$, the roots of $m(x)$ must be a subset of the roots of $q(x)$, which are $\{b = b_1, b_2, \dots, b_n\}$.

Consider any root b_j of $m(x)$. Since $m(x)$ also divides $r(x)$, this b_j must also be a root of $r(x)$. So, for such a b_j, we must have $r(b_j) = p(c - db_j) = 0$. This implies that $c - db_j$ must be one of the roots of $p(x)$, say a_i.

$$c - db_j = a_i$$

Substituting $c = a + db$:

$$a + db - db_j = a_i$$

$$d(b - b_j) = a_i - a$$

If $j \neq 1$, then $b \neq b_j$. We can write:

$$d = \frac{a_i - a}{b - b_j}$$

But this contradicts our initial choice of d, which was chosen specifically to not be equal to any of these values. Therefore, the only possibility is that $j = 1$, which means $b_j = b_1 = b$, and hence

$$m(x) = x - b$$

in $F(c)[x]$, i.e. $b \in F(c)$ and the theorem is proved. □

4.5 Tower Law

Theorem 4.25 (Tower Law)**.** *Let $F \subseteq K \subseteq L$ be field extensions. (e.g., $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$). Then:*

$$[L : F] = [L : K][K : F]$$

Proof. Let $\{e_1, \ldots, e_n\}$ be a basis of K over F. This means $[K : F] = n$. Let $\{f_1, \ldots, f_m\}$ be a basis of L over K. This means $[L : K] = m$.

Claim: The set $\mathcal{B} = \{e_i f_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis of L over F. If this claim is true, then the dimension of L over F is $n \cdot m$, which proves the theorem. We need to show that $\mathcal{B}$ is a spanning set and is linearly independent over F.

Spanning set: Let x be any element in L. Since $\{f_j\}$ is a basis of L over K, we can write x as a linear combination:

$$x = \sum_{j=1}^{m} \mu_j f_j, \quad \text{where each } \mu_j \in K$$

Now, for each coefficient $\mu_j \in K$, we can express it as a linear combination of the basis elements of K over F. For each j, we have:

$$\mu_j = \sum_{i=1}^{n} \nu_{ij} e_i, \quad \text{where each } \nu_{ij} \in F$$

Substituting this back into the expression for x:

$$x = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \nu_{ij} e_i \right) f_j = \sum_{j=1}^{m} \sum_{i=1}^{n} \nu_{ij} (e_i f_j)$$

Since every element $x \in L$ can be written as a linear combination of the elements $\{e_i f_j\}$ with coefficients $\nu_{ij} \in F$, this set spans L over F.

Linear Independence: Suppose we have a linear combination of the elements $\{e_i f_j\}$ that equals zero, with coefficients β_{ij} from the field F:

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \beta_{ij} e_i f_j = 0, \quad \text{where } \beta_{ij} \in F$$

We can regroup the terms by factoring out the f_j:

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} \beta_{ij} e_i \right) f_j = 0$$

For each j, the inner sum $\sum_{i=1}^{n} \beta_{ij} e_i$ is a linear combination of elements of the basis $\{e_i\}$ with coefficients in F. This means the term in the parenthesis is an element of the field K. So, we have a linear combination of the basis elements $\{f_j\}$ with coefficients from K that equals zero. By the linear independence of the set $\{f_1, \ldots, f_m\}$ over K, all the coefficients must be zero:

$$\sum_{i=1}^{n} \beta_{ij} e_i = 0 \quad \text{for all } j = 1, \ldots, m$$

Now, for each j, we have a linear combination of the basis elements $\{e_i\}$ over F that equals zero. By the linear independence of the set $\{e_1, \ldots, e_n\}$ over F, all the coefficients must be zero:

$$\beta_{ij} = 0 \quad \text{for all } i, j$$

This shows that the set $\{e_i f_j\}$ is linearly independent over F, which completes the proof of the Tower Law. □

Example 4.26. Let $F = \mathbb{F}_2$ (which is the same as $\mathbb{Z}_2$). Let $L = \mathbb{F}_2[x]/\langle x^3+x+1 \rangle$. So, $|L| = 2^3 = 8$ and $[L : F] = 3$.

Are there any proper subfields K with $\mathbb{F}_2 \subset K \subset L$? Suppose such a subfield K exists. Then by the Tower Law, we must have:

$$[L : \mathbb{F}_2] = [L : K][K : \mathbb{F}_2]$$

Substituting the known value:

$$3 = [L : K][K : \mathbb{F}_2]$$

Since 3 is a prime number and the degrees of extensions are integers greater than or equal to 1, the only possibilities are:

1. $[L : K] = 1$ and $[K : \mathbb{F}_2] = 3$. This implies $K = L$.
2. $[L : K] = 3$ and $[K : \mathbb{F}_2] = 1$. This implies $K = \mathbb{F}_2$.

Therefore, there are no proper intermediate subfields between L and $\mathbb{F}_2$.

Corollary 4.27. *Suppose we have a tower of fields $F \subseteq E \subseteq K$. If $K : E$ is an algebraic extension and $E : F$ is an algebraic extension, then $K : F$ is also an algebraic extension.*

Proof. Let $a \in K$. Since $K : E$ is algebraic, a is a root of some polynomial $p(x) = b_n x^n + \cdots + b_1 x + b_0 \in E[x]$.

Since $E : F$ is algebraic, each coefficient $b_i \in E$ is algebraic over F. Consider the tower of fields:

$$F \subseteq F_0 := F(b_0) \subseteq F_1 := F_0(b_1) \subseteq \cdots \subseteq F_n := F_{n-1}(b_n) = F(b_0, \dots, b_n).$$

Since each b_i is algebraic over F, it is also algebraic over F_{i-1}. Therefore, each extension in this tower, $F_i : F_{i-1}$, is a finite extension. By the Tower Law, $[F_n : F]$ is finite.

$$[F_n : F] = [F_n : F_{n-1}] \dots [F_1 : F_0][F_0 : F] < \infty.$$

Now, the polynomial $p(x)$ has its coefficients in F_n, so $p(x) \in F_n[x]$. Since a is a root of $p(x)$, the extension $F_n(a) : F_n$ is finite, with $[F_n(a) : F_n] \leq \deg(p) = n$.

Consider the degree of the extension $F_n(a)$ over F:

$$[F_n(a) : F] = [F_n(a) : F_n][F_n : F].$$

This product is finite. Since $F(a)$ is a subfield of $F_n(a)$, we have $[F(a) : F] \leq [F_n(a) : F] < \infty$. Because $F(a) : F$ is a finite extension, it must be an algebraic extension. This implies that the element a is algebraic over F. Since a was an arbitrary element of K, the extension $K : F$ is algebraic. □

Corollary 4.28. *The set of all algebraic elements in an extension $E : F$ forms a subfield of E.*

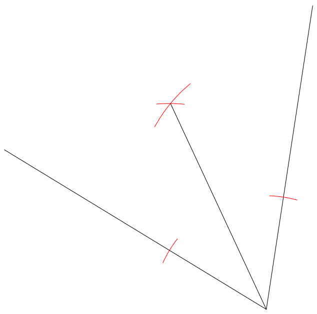
Proof. Let $a, b \in E$ be algebraic over F. We need to show that $a + b$, $a - b$, ab, and a/b (for $b \neq 0$) are also algebraic over F. Consider the field $F(a, b)$. By the Tower Law,

$$[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F].$$

Since a is algebraic over F, $[F(a) : F]$ is finite. Since b is algebraic over F, it is also algebraic over the larger field $F(a)$. Thus, $[F(a, b) : F(a)] = [F(a)(b) : F(a)]$ is also finite. Therefore, $[F(a, b) : F]$ is finite. Since $F(a, b)$ is a finite extension of F, it is an algebraic extension. Any element of $F(a, b)$ is algebraic over F. This includes $a + b, a - b, ab$, and a/b. □

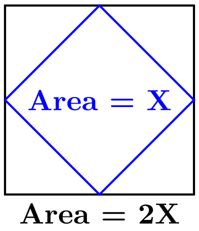
As a final application of the Tower Law: What can we do with a ruler (with no markings) and a compass?

- **Bisect an angle**



Q: Can we **tri-sect** any angle??

- **Double a square**



Q: Can you **double a cube**?