Week 1

1.1 Groups

Definition. A **group** is a set G equipped with a binary operation

$$* : G \times G \longrightarrow G$$

(called the **group operation** or "**product**" or "**multiplication**") such that the following conditions are satisfied:

- The group operation is **associative**, i.e.

  $$(a * b) * c = a * (b * c)$$

  for all $a, b, c \in G$.

- There is an element $e \in G$, called an **identity element**, such that

  $$a * e = e * a = a,$$

  for all $a \in G$.

- For every $a \in G$ there exists an element $a^{-1} \in G$, called an **inverse** of a, such that

  $$a^{-1} * a = a * a^{-1} = e.$$

Remark. We often write $a \cdot b$ or simply ab to denote $a * b$.

Definition. If $ab = ba$ for all $a, b \in G$, we say that the group operation is **commutative** and that G is an **abelian group**; otherwise we say that G is **nonabelian**.

Remark. When the group is abelian, we often use $+$ to denote the group operation.

Definition. The **order** of a group G, denoted by $|G|$, is the number of elements in G. We say that G is **finite** (resp. **infinite**) if $|G|$ is finite (resp. infinite).

Example 1.1.1. The following sets are groups, with respect to the specified group operations:

- $G = \mathbb{Q}$, where the group operation is the usual addition $+$ for rational numbers. The identity is $e = 0$. The inverse of $a \in \mathbb{Q}$ with respect to $+$ is $-a$. This is an infinite abelian group.
- $G = \mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$, where the group operation is the usual multiplication for rational numbers. The identity is $e = 1$, and the inverse of $a \in \mathbb{Q}^\times$ is $a^{-1} = \frac{1}{a}$. This group is also infinite and abelian.

  Note that $\mathbb{Q}$ is *not* a group with respect to multiplication. For in that case, we have $e = 1$, but $0 \in \mathbb{Q}$ has no inverse $0^{-1} \in \mathbb{Q}$ such that $0 \cdot 0^{-1} = 1$.

Exercise: Verify that the following sets are groups under the specified binary operations:

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
- $(\mathbb{R}^\times = \mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}^\times = \mathbb{C}\backslash\{0\}, \cdot)$
- $(U_m, \cdot)$, where $m \in \mathbb{Z}_{>0}$,
$$U_m = \{1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}\}$$
  and $\zeta_m = e^{2\pi\mathbf{i}/m} = \cos(2\pi/m) + \mathbf{i}\sin(2\pi/m) \in \mathbb{C}$.
- The set of bijective functions $f : \mathbb{R} \longrightarrow \mathbb{R}$, where $f * g := f \circ g$ (i.e. composition of functions).
- More generally, one can consider any nonempty set X. Then the set
$$S_X := \{\sigma : X \to X : \sigma \text{ is bijective}\}$$
  of all bijective maps from X onto X is a group under composition of maps.

Example 1.1.2. The set $G = \mathrm{GL}(2, \mathbb{R})$ of real 2×2 matrices with nonzero determinants is a group under matrix multiplication, with identity element:
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
In the group G, we have:
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Note that there are matrices $A, B \in \mathrm{GL}(2, \mathbb{R})$ such that $AB \neq BA$. Hence $\mathrm{GL}(2, \mathbb{R})$ is nonabelian (and infinite).

More generally, for any $n \in \mathbb{Z}_{>0}$, the set $\mathrm{GL}(n, \mathbb{R})$ of $n \times n$ real matrices M, such that $\det M \neq 0$, is a group under matrix multiplication, called the **General Linear Group**. The group $\mathrm{GL}(n, \mathbb{R})$ is nonabelian for $n \geq 2$.

Exercise: The set $\mathrm{SL}(n, \mathbb{R})$ of real $n \times n$ matrices with determinant 1 is a group under matrix multiplication, called the **Special Linear Group**.

Example 1.1.3. Let $n \in \mathbb{Z}_{>0}$. Consider the finite set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

We define a binary operation $+_n$ on $\mathbb{Z}_n$ by

$$a +_n b = \begin{cases} a+b & \text{if } a+b < n, \\ a+b-n & \text{if } a+b \geq n. \end{cases}$$

for any $a, b \in \mathbb{Z}_n$.

Exercise: Then $(\mathbb{Z}_n, +_n)$ is a finite abelian group. (By abuse of notation, we will usually use the usual symbol $+$ to denote the additive operation for this group.)

Proposition 1.1.4. *The identity element e of a group G is unique.*

Proof. Suppose there is an element $e' \in G$ such that $e'g = ge'$ for all $g \in G$. Then, in particular, we have:

$$e'e = e$$

But since e is an identity element, we also have $e'e = e'$. Hence, $e' = e$. □

Proposition 1.1.5. *Let G be a group. For all $g \in G$, its inverse g^{-1} is unique.*

Proof. Suppose there exists $g' \in G$ such that $g'g = gg' = e$. By the associativity of the group operation, we have:

$$g' = g'e = g'(gg^{-1}) = (g'g)g^{-1} = eg^{-1} = g^{-1}.$$

Hence, g^{-1} is unique. □

Let G be a group with identity element e. For $g \in G$, $n \in \mathbb{N}$, let:

$$g^n := \underbrace{g \cdot g \cdots g}_{n \text{ times}}.$$
$$g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}$$
$$g^0 := e.$$

Proposition 1.1.6. *Let G be a group.*

1. *For all $g \in G$, we have:*
$$(g^{-1})^{-1} = g.$$

2. *For all $a, b \in G$, we have:*
$$(ab)^{-1} = b^{-1}a^{-1}.$$

3. *For all $g \in G$, $n, m \in \mathbb{Z}$, we have:*
$$g^n \cdot g^m = g^{n+m}.$$

Proof. **Exercise.** □

Week 2

2.1 Cyclic groups

Definition. Let G be a group, with identity element e. The **order** of an *element* $g \in G$, denoted by $|g|$, is the smallest positive integer n such that $g^n = e$; if no such n exists, we say that g has **infinite order** and write $|g| = \infty$.

Exercise: If G has finite order, then every element of G has finite order.

Proposition 2.1.1. *Let G be a group with identity element e. Let g be an element of G. If $g^n = e$ for some $n \in \mathbb{Z}_{>0}$, then $|g|$ divides n.*

Proof. Let $m = |g|$. Suppose $g^n = e$. By the Division Theorem, there exist (uniquely) integers q and $0 \leq r < m$ such that $n = mq + r$. So $g^n = (g^m)^q \cdot g^r$ which implies that $g^r = e$. This forces $r = 0$ (since otherwise this violates the definition of $|g| = m$). Hence $m \mid n$. □

Given an element g in a group G, we define the subset $\langle g \rangle \subset G$ as the set of all integral powers of g:

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

Recall that

$$|g| = \begin{cases} \min\{n \in \mathbb{Z}_{>0} : g^n = e\} & \text{if } \exists n \in \mathbb{Z}_{>0} \text{ such that } g^n = e, \\ \infty & \text{otherwise.} \end{cases}$$

Proposition 2.1.2. *If $|g| = \infty$, then $\langle g \rangle$ is an infinite set; in fact, the map $\mathbb{Z} \to \langle g \rangle$, $n \mapsto g^n$ is a bijection. If $|g| = m < \infty$, then*

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}.$$

Proof. Suppose $|g| = \infty$. It follows from the definition of $\langle g \rangle$ that the map $\mathbb{Z} \to \langle g \rangle$, $n \mapsto g^n$ is surjective. So we only need to show that it is also injective.

Suppose $g^{n_1} = g^{n_2}$ for some $n_1, n_2 \in \mathbb{Z}$. If $n_1 \neq n_2$, then without loss of generality, we can assume that $n_1 > n_2$. Then we have $g^{n_1 - n_2} = e$ with $n_1 - n_2 \in \mathbb{Z}_{>0}$. But this violates the assumption that $|g| = \infty$. Hence we must have $n_1 = n_2$, showing the required injectivity.

When $|g| = m < \infty$, we want to show that $\langle g \rangle = \{e, g, g^2, \dots, g^{m-1}\}$. Clearly we have $\langle g \rangle \supset \{e, g, g^2, \dots, g^{m-1}\}$, so we only need to prove the reverse inclusion. Take an element $g^n \in \langle g \rangle$. Then the Division Theorem implies that there exist integers q and $0 \leq r < m$ such that $n = mq + r$. So $g^n = (g^m)^q \cdot g^r = g^r \in \{e, g, g^2, \dots, g^{m-1}\}$. This completes the proof. □

Definition. A group G is **cyclic** if there exists $g \in G$ such that every element of G is equal to g^n for some integer n. In this case, we write $G = \langle g \rangle$, and say that g is a **generator** of G.

Remark. The generator of of a cyclic group might not be unique, i.e. there may exist *different* elements $g_1, g_2 \in G$ such that $G = \langle g_1 \rangle = \langle g_2 \rangle$.

Example 2.1.3.

- $(\mathbb{Z}, +)$ is cyclic, generated by 1 or -1.
- $(\mathbb{Z}_n, +)$ is cyclic, generated by 1, or $k \in \mathbb{Z}_n$ such that $\gcd(k, n) = 1$.
- $(U_m, \cdot)$ is cyclic, generated by $\zeta_m = e^{2\pi \mathbf{i}/m}$, or ζ_m^n for any integer $n \in \mathbb{Z}_m$ such that $\gcd(m, n) = 1$.

Exercise: A finite cyclic group G has order n if and only if each of its generators has order n.

Exercise: The group $(\mathbb{Q}, +)$ is not cyclic.

Example 2.1.4. Let p be a prime. Let $G = (\mathbb{Z}_p, +)$. For all $g \neq 0$ in G, the order of g is p.

Proof. **Exercise.** □

Proposition 2.1.5. *Every cyclic group is abelian*

Proof. Let G be a cyclic group. Then $G = \langle g \rangle$ for some element $g \in G$ and every element is of the form g^n for some $n \in \mathbb{Z}$. Now

$$g^{n_1} \cdot g^{n_2} = g^{n_1 + n_2} = g^{n_2 + n_1} = g^{n_2} \cdot g^{n_1}.$$

So G is abelian. □

Remark. The converse is not true, namely, there are non-cyclic abelian groups (e.g. the *Klein 4-group* $\mathbb{Z}_2 \times \mathbb{Z}_2$).

2.2 Symmetric groups

Definition. Let X be a set. A **permutation** of X is a bijective map $\sigma : X \longrightarrow X$.

Claim 2.2.1. *The set S_X of permutations of a set X is a group with respect to $\circ$, the composition of maps.*

Proof.

- Let σ, γ be permutations of X. By definition, they are bijective maps from X to itself. It is clear that $\sigma \circ \gamma$ is a bijective map from X to itself, hence $\sigma \circ \gamma$ is a permutation of X. So $\circ$ is a well-defined binary operation on S_X.
- For $\alpha, \beta, \gamma \in S_X$, it is clear that $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.
- Define a map $e : X \longrightarrow X$ as follows:

  $$e(x) = x, \quad \text{for all } x \in X.$$

  It is clear that $e \in S_X$, and that $e \circ \sigma = \sigma \circ e = \sigma$ for all $\sigma \in S_X$. Hence, e is an identity element in S_X.
- Let σ be any element of S_X. Since $\sigma : X \longrightarrow X$ is by assumption bijective, there exists a bijective map $\sigma^{-1} : X \longrightarrow X$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e$. So σ^{-1} is an inverse of σ with respect to the operation $\circ$.

□

Terminology: We call S_X the **symmetric group** on X.

Notation. Let n be a positive integer. Consider the set $I_n := \{1, 2, \ldots, n\}$. Then we denote S_{I_n} by S_n and call it the **n-th symmetric group**.

For $n \in \mathbb{Z}_{>0}$, the group S_n has $n!$ elements.

For $n \in \mathbb{Z}_{>0}$, by definition an element of S_n is a bijective map $\sigma : I_n \longrightarrow I_n$, where $I_n = \{1, 2, \ldots, n\}$. We often describe σ using the following notation:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Example 2.2.2. In S_3,

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

is the permutation on $I_3 = \{1, 2, 3\}$ which sends 1 to 3, 2 to itself, and 3 to 1, i.e. $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 1$.

For $\alpha, \beta \in S_3$ given by:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

we have:

$$\alpha\beta = \alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

(since, for example, $\alpha \circ \beta : 1 \overset{\beta}{\mapsto} 2 \overset{\alpha}{\mapsto} 3$.).

We also have:

$$\beta\alpha = \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Since $\alpha\beta \neq \beta\alpha$, the group S_3 is non-abelian.

In general, for $n \geq 3$, the group S_n is non-abelian (**Exercise:** Why?).

For the same $\alpha \in S_3$ defined above, we have:

$$\alpha^2 = \alpha \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

and:

$$\alpha^3 = \alpha \cdot \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

Hence, the order of α is 3.

More on S_n

Consider the following element in S_6:

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

We may capture the action of $\sigma : \{1, 2, \dots, 6\} \longrightarrow \{1, 2, \dots, 6\}$ using the notation:

$$\sigma = (15)(246),$$

where $(i_1 i_2 \cdots i_k)$ denotes the permutation:

$$i_1 \mapsto i_2, i_2 \mapsto i_3, \dots, i_{k-1} \mapsto i_k, i_k \mapsto i_1$$

and $j \mapsto j$ for all $j \in \{1, 2, \dots, n\} \backslash \{i_1, i_2, \dots, i_k\}$. We call $(i_1 i_2 \cdots i_k)$ a **k-cycle** or a **cycle of length k**. Note that 3 is missing from $(15)(246)$, meaning that 3 is fixed by σ.

Proposition 2.2.3. *Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.*

Proof. Later. $\square$

Exercise: Disjoint cycles commute with each other.

A 2-cycle is often called a **transposition**, for it switches two elements with each other.

2.3 Dihedral groups

Consider the subset $\mathcal{T}$ of transformations of $\mathbb{R}^2$, consisting of all rotations by fixed angles about the origin, and all reflections over lines through the origin.

Consider a regular polygon P_n with n sides in $\mathbb{R}^2$, centered at the origin. Identify the polygon with its n vertices, which form a subset $P_n = \{x_1, x_2, \ldots, x_n\}$ of $\mathbb{R}^2$. If $\tau(P_n) = P_n$ for some $\tau \in \mathcal{T}$, we say that P_n is **symmetric** with respect to τ.

Intuitively, it is clear that P_n is symmetric with respect to n rotations

$$\{r_0, r_1, \ldots, r_{n-1}\},$$

and n reflections

$$\{s_1, s_2, \ldots, s_n\}$$

in $\mathcal{T}$. In particular $|D_n| = 2n$.

Proposition 2.3.1. *The set $D_n := \{r_0, r_1, \ldots, r_{n-1}, s_1, s_2, \ldots, s_n\}$ is a group, with respect to the group operation defined by composition of transformations: $\tau * \gamma = \tau \circ \gamma$.*

Terminology: D_n is called the **n-th dihedral group**.

Let $r = r_1 \in D_n$ be the rotation by the angle $2\pi/n$ in the anticlockwise direction (and similarly r_k denotes the rotation by the angle $2k\pi/n$ in the anticlockwise direction). Then the set of rotations in D_n is given by

$$\langle r \rangle = \{\text{id}, r, r^2, \ldots, r^{n-1}\}.$$

Furthermore, the composition of two reflections is a rotation (which can be seen, e.g. by flipping a Hong Kong 2-dollar coin). So if we let $s = s_1 \in D_n$ be one of the reflections, then the set of reflections in D_n is given by

$$\{s, rs, r^2 s, \ldots, r^{n-1} s\}.$$

So we can enumerate the elements of D_n as

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

Week 3

3.1 Subgroups

Definition. Let G be a group. A subset H of G is a **subgroup** of G (denoted as $H < G$) if it is a group under the induced operation from G.

More precisely, a subset $H \subset G$ is a subgroup of G if

- H is *closed* under the operation on G, i.e.

  $$a * b \in H \text{ for any } a, b \in H,$$

  so that the restriction of the binary operation $G \times G \to G$ to the subset $H \times H \subset G \times G$ gives a well-defined binary operation $H \times H \to H$, called the *induced operation* on H, and

- H is a group under this induced operation.

Example 3.1.1.

- For any group G, we have the **trivial subgroup** $\{e\} < G$ and also $G < G$. We call a subgroup $H < G$ **nontrivial** if $\{e\} \subsetneqq H$ and **proper** if $H \subsetneqq G$.
- We have $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ under addition, and $\mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$ under multiplication.
- For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.
- $\mathrm{SL}(n, \mathbb{R})$ is a subgroup of $\mathrm{GL}(n, \mathbb{R})$.
- The set of all rotations (including the trivial rotation) in a dihedral group D_n is a subgroup of D_n.
- By viewing D_n as permutations of the vertices of a regular n-gon P_n, we can regard D_n as a subgroup of S_n.

- Consider the symmetric group S_n where $n \in \mathbb{Z}_{>0}$.

  Proposition 3.1.2. *Each element of S_n is a product of (not necessarily disjoint) transpositions.*

  Sketch of proof. Show that each permutation not equal to the identity is a product of cycles, and that each cycle is a product of transpositions:

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

  □

  Example 3.1.3.

  $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = (15)(246) = (15)(26)(24) = (15)(46)(26)$$

  Note that a given element σ of S_n may be expressed as a product of transpositions in different ways, but:

  Proposition 3.1.4. *In every factorization of σ as a product of transpositions, the number of factors is either always even or always odd.*

  Proof. **Exercise.** One approach: There is a unique $n \times n$ matrix, with either 0 or 1 as its coefficients, which sends any vector $(x_1, x_2, \ldots, x_n)$ to $(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. Use the fact that the determinant of the matrix corresponding to a transposition is -1, and that the determinant function of matrices is multiplicative. □

  We say that $\sigma \in S_n$ is an **even** (resp. **odd**) **permutation** if it is a product of an even (resp. odd) number of transpositions. The subset A_n of S_n consisting of even permutations is a subgroup of S_n. A_n is called the n-th **alternating group**.

Proposition 3.1.5. *A nonempty subset H of a group G is a subgroup of G if and only if, for all $a, b \in H$, we have $ab^{-1} \in H$.*

Proof. Suppose $H \subseteq G$ is a subgroup. For any $a, b \in H$, existence of inverse implies that $b^{-1} \in H$, and then closedness implies that $ab^{-1} \in H$.

Conversely, suppose H is a nonempty subset of G such that $xy^{-1} \in H$ for all $x, y \in H$.

- (Identity:) Let e be the identity element of G. Since H is nonempty, it contains at least one element h. Since $e = h \cdot h^{-1}$, and by hypothesis $h \cdot h^{-1} \in H$, the set H contains e.

- (Inverses:) Since $e \in H$, for all $a \in H$ we have $a^{-1} = e \cdot a^{-1} \in H$.
- (Closure:) For all $a, b \in H$, we know that $b^{-1} \in H$. Hence, $ab = a \cdot (b^{-1})^{-1} \in H$.
- (Associativity:) This follows from that in G.

Hence, H is a subgroup of G. □

One can use this criterion to check that all the previous examples are indeed subgroups.

3.2 Cyclic subgroups

Recall that for any group G and any element $g \in G$, we have the subset

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

Proposition 3.2.1. *Let G be a group. Then for any element $g \in G$, the subset $\langle g \rangle$ is the smallest subgroup of G containing g, which we call the* **cyclic subgroup** *generated by g.*

Proof. Let g^k, g^l be two arbitrary elements in $\langle g \rangle$. Then $g^k (g^l)^{-1} = g^{k-l} \in \langle g \rangle$. So $\langle g \rangle$ is a subgroup of G by Proposition 3.1.5.

Now let $H < G$ be any subgroup containing g. Then $g^k \in H$ for any $k \in \mathbb{Z}$ since H is a subgroup. Hence $\langle g \rangle \subset H$. □

Proposition 3.2.2. *The intersection of any collection of subgroups of a group G is also a subgroup of G.*

Proof. **Exercise.** □

Corollary 3.2.3. *Let G be a group. Then for any $g \in G$, we have*

$$\langle g \rangle = \bigcap_{\{H : g \in H < G\}} H.$$

Week 4

4.1 Cyclic subgroups (cont'd)

Proposition 4.1.1. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle g \rangle$ be a cyclic group, and $H < G$ a subgroup. If H is trivial, then it is cyclic (generated by the identity e). If H is nontrivial, then there exists $k \in \mathbb{Z}_{>0}$ such that $g^k \in H$. We set

$$m := \min\{k \in \mathbb{Z}_{>0} : g^k \in H\}.$$

We claim that H is generated by g^m. First of all, we obviously have $\langle g^m \rangle \subset H$. Conversely, let g^n be an arbitrary element in H. By the Division Theorem, there exist (uniquely) integers q and $0 \leq r \leq m-1$ such that $n = mq + r$. So $g^n = (g^m)^q \cdot g^r$ which implies that $g^r = (g^m)^{-q} \cdot g^n \in H$. This forces $r = 0$. Thus $g^n \in \langle g^m \rangle$, and we have shown that $H \subset \langle g^m \rangle$. This completes the proof. $\square$

Corollary 4.1.2. *Any subgroup of* $(\mathbb{Z}, +)$ *is of the form* $n\mathbb{Z}$ *for some* $n \in \mathbb{Z}$.

Because of this corollary, we can define the gcd of two integers as follows. For any $a, b \in \mathbb{Z}$, the subset

$$\langle a, b \rangle := \{ma + nb : m, n \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$ using Proposition 3.1.5 (check this!). Corollary 4.1.2 implies that $\langle a, b \rangle$ is of the form $d\mathbb{Z}$ for some positive integer d. We then define the **greatest common divisor (gcd)**, denoted as $\gcd(a, b)$, to be this positive integer d. One can check that this gcd satisfies the following properties (as expected):

- $d \mid a$ and $d \mid b$,
- $d = ka + lb$ for some $k, l \in \mathbb{Z}$, and
- if $k \mid a$ and $k \mid b$, then $k \mid d$.

Proposition 4.1.3. *Let G be a cyclic group of order n and $g \in G$ be a generator of G, i.e. $G = \langle g \rangle$. Let $g^s \in G$ be an element in G. Then*

$$|g^s| = n/d,$$

where $d = gcd(s, n)$. Moreover, $\langle g^s \rangle = \langle g^t \rangle$ if and only if $gcd(s, n) = gcd(t, n)$.

Proof. Let us write $a = g^s$ and let $m := |a|$. First of all, we have $a^{n/d} = (g^s)^{n/d} = (g^n)^{s/d} = e$ since $|G| = n$. Proposition 2.1.1 implies that $m \mid (n/d)$. On the other hand, we have $e = a^m = g^{sm}$ which implies, again by Proposition 2.1.1, that $n \mid sm$. Dividing both sides by d gives $(n/d) \mid (s/d)m$. But n/d and s/d are relatively prime, so we must have $(n/d) \mid m$. This proves that $|g^s| = m = n/d$ where $d = \gcd(s, n)$.

To prove the second assertion, we first show that there is an equality of subgroups $\langle g^s \rangle = \langle g^d \rangle$ where $d = \gcd(s, n)$. One inclusion is clear: as $d \mid s$, we have $g^s \in \langle g^d \rangle$ which implies $\langle g^s \rangle \subset \langle g^d \rangle$. Conversely, note that there exist $k, l \in \mathbb{Z}$ such that $d = ks + ln$. So we have $g^d = (g^s)^k \cdot (g^n)^l = (g^s)^k \in \langle g^s \rangle$ and hence $\langle g^d \rangle \subset \langle g^s \rangle$. This proves the equality we claimed.

Now, $\langle g^s \rangle = \langle g^t \rangle$ implies that $|g^s| = |g^t|$ which in turn gives $\gcd(s, n) = \gcd(t, n)$. Conversely, if we have $\gcd(s, n) = \gcd(t, n) =: d$, then $\langle g^s \rangle = \langle g^d \rangle = \langle g^t \rangle$. □

Corollary 4.1.4. *All generators of a cyclic group $G = \langle g \rangle$ of order n are of the form g^r where r is relatively prime to n.*

4.2 Generating sets

Let G be a group, S a nonempty subset of G. Then similar to the case of a cyclic subgroup, it can be proved using Proposition 3.1.5 that the subset:

$$\langle S \rangle := \{a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n} : n \in \mathbb{N}, a_i \in S, m_i \in \mathbb{Z}\}$$

is the smallest subgroup of G containing S. We call $\langle S \rangle$ the subgroup of G **generated** by S. If $G = \langle S \rangle$, then we say S is a **generating set** for G.

Remark. Similar to the cyclic subgroup generated by a single element, we have

$$\langle S \rangle = \bigcap_{\{H : S \subset H < G\}} H.$$

If $S = \{a_1, a_2, \ldots, a_l\}$ is a finite set, we often write

$$\langle a_1, a_2, \ldots, a_l \rangle$$

to denote the subgroup generated by S.

Example 4.2.1.

- The set of cycles and the set of transpositions are two examples of generating sets for S_n.
- We also have $S_n = \langle (12), (12 \cdots n) \rangle$.
- We have $D_n = \langle r, s \rangle$ where r is the rotation by the angle $2\pi/n$ in the anticlockwise direction and s is any reflection.

If there exists a finite number of elements $a_1, a_2, \ldots, a_l \in G$ such that

$$G = \langle a_1, a_2, \ldots, a_l \rangle,$$

then we say that G is **finitely generated**.

For example, every cyclic group is finitely generated, for it is generated by one element. Every finite group is also finitely generated, since we may take the finite generating set S to be G itself. Finitely generated groups are much easier to understand. For instance, there is a simple classification for finitely generated abelian groups but not for those which are not finitely generated.

Exercise: The group $(\mathbb{Q}, +)$ is not finitely generated.

4.3 Equivalence relations and partitions

Let S be a set.

A **partition** P of S is a collection of subsets $\{S_i : i \in I\}$ of S (here I is some index set) such that

- $S_i \neq \emptyset$ for each $i \in I$,
- $S_i \cap S_j =$ if $i \neq j$, and
- $\bigcup_{i \in I} S_i = S$.

We may also say that P is a subdivision of S into a disjoint union of nonempty subsets, written as

$$S = \bigsqcup_{i \in I} S_i.$$

An **equivalence relation** on S is a relation $\sim$ (i.e. a subset of $S \times S$) which is

- (Reflexive:) $a \sim a$ for any $a \in S$,
- (Symmetric:) if $a \sim b$, then $b \sim a$, and
- (Transitive:) if $a \sim b$ and $b \sim c$, then $a \sim c$.

In fact, partition and equivalence relation are two equivalent concepts.

First of all, given a partition $\{S_i : i \in I\}$ of S, we can define a relation on S by the rule $a \sim b$ if $a, b \in S_i$ for some $i \in I$. Then it is easy to check that $\sim$ is an equivalence relation on S.

Conversely, suppose we are given an equivalence relation $\sim$ on S. For any $a \in S$, the set

$$C_a = \{b \in S : a \sim b\}$$

is called the **equivalence class** of a. The reflexive axiom implies that $a \in C_a$; in particular, $C_a \neq \emptyset$ for all $a \in S$. Also, S is the union of all the equivalence classes C_a. Finally, we claim that if $C_a \cap C_b \neq \emptyset$, then $C_a = C_b$.

Proof of claim. Suppose there exists $c \in C_a \cap C_b$. So we have $a \sim c$ and $b \sim c$. The symmetric and transitive axioms then imply that $a \sim b$ (and $b \sim a$). Now for any $d \in C_a$, we have $d \sim a$, so $d \sim b$ by $a \sim b$ and the transitive axiom. Thus $d \in C_b$ and this shows that $C_a \subset C_b$. Reversing the roles of a and b in the same argument shows that $C_b = C_a$. Therefore $C_a = C_b$. □

We conclude that the collection of equivalence classes C_a, $a \in S$ gives a partition of S.

As an application, we give a proof of the fact that any permutation $\sigma \in S_n$ is a product of disjoint cycles:

Proof of Proposition 2.2.3. Let $\sigma \in S_n$ be a permutation on the set $I_n = \{1, 2, \ldots, n\}$. For $a, b \in I_n$, we say $a \sim b$ if and only if $b = \sigma^k(a)$ for some $k \in \mathbb{Z}$. **Exercise:** This defines an equivalence relation on I_n. So it produces a partition of I_n into a disjoint union of equivalence classes:

$$I_n = O_1 \sqcup O_2 \sqcup \cdots \sqcup O_m.$$

(The equivalence classes $O_1, O_2, \ldots, O_m \subset I_n$ are called **orbits** of σ.) Then, for $j = 1, 2, \ldots, m$, we define a permutation $\mu_j \in S_n$ by

$$\mu_j(a) = \begin{cases} \sigma(a) & \text{if } a \in O_j, \\ a & \text{if } a \notin O_j. \end{cases}$$

Each μ_j is a cycle (of length $|O_j|$). They are disjoint since the O_j's form a partition. Also we have

$$\sigma = \mu_1 \mu_2 \cdots \mu_m.$$

□

Week 5

5.1 Cosets

Let G be a group, H a subgroup of G. We are interested in knowing how large H is relative to G.

We define a relation $\sim_L$ on G as follows:

$$a \sim_L b \text{ if and only if } b = ah \text{ for some } h \in H,$$

or equivalently:

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

Exercise: $\sim_L$ is an equivalence relation.

We may therefore partition G into a disjoint union of equivalence classes with respect to $\sim_L$. We call these equivalence classes the **left cosets** of H in G; each left coset of H has the form

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

We could likewise define a relation $\sim_R$ on G by

$$a \sim_R b \text{ if and only if } b = ha \text{ for some } h \in H,$$

or equivalently:

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

$\sim_R$ is also an equivalence relation, whose equivalence classes, which are subsets of the form

$$Hb = \{hb : h \in H\}, \quad b \in G,$$

are called the **right cosets** of H in G.

Example 5.1.1. Let $G = (\mathbb{Z}, +)$. Let:

$$H = 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

The set H is a subgroup of G. The left cosets of H in G are as follows:

$$3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z},$$

where $i+3\mathbb{Z} := \{i+3k : k \in \mathbb{Z}\}$.

In general, for $n \in \mathbb{Z}$, the left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are:

$$i+n\mathbb{Z}, \quad i=0,1,2,\ldots,n-1.$$

Definition. The number of left cosets of a subgroup H of G is called the **index** of H in G. It is denoted by:

$$[G : H]$$

Remark. In general, the numbers of left cosets and right cosets, if finite, are equal to each other. We will see why in a moment.

Example 5.1.2. Let $G = \mathrm{GL}(n,\mathbb{R})$. Let:

$$H = \mathrm{GL}^+(n,\mathbb{R}) := \{h \in G : \det h > 0\}.$$

(**Exercise:** H is a subgroup of G.)

Let:

$$s = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in G$$

Note that $\det s = \det s^{-1} = -1$.

For any $g \in G$, either $\det g > 0$ or $\det g < 0$. If $\det g > 0$, then $g \in H$. If $\det g < 0$, we write:

$$g = (ss^{-1})g = s(s^{-1}g).$$

Since $\det s^{-1}g = (\det s^{-1})(\det g) > 0$, we have $s^{-1}g \in H$. So, $G = H \sqcup sH$, and $[G : H] = 2$. Notice that both G and H are infinite groups, but the index of H in G is finite.

Example 5.1.3. Let $G = \mathrm{GL}(n,\mathbb{R})$, $H = \mathrm{SL}(n,\mathbb{R})$. For each $x \in \mathbb{R}^\times$, let:

$$s_x = \begin{pmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in G$$

Note that $\det s_x = x$.

For each $g \in G$, we have:

$$g = s_{\det g}(s_{\det g}^{-1} g) \in s_{\det g} H$$

Moreover, for distinct $x, y \in \mathbb{R}^\times$, we have:

$$\det(s_x^{-1} s_y) = y/x \neq 1.$$

This implies that $s_x^{-1} s_y \notin H$, hence $s_y H$ and $s_x H$ are disjoint cosets. We have therefore:

$$G = \bigsqcup_{x \in \mathbb{R}^\times} s_x H.$$

The index $[G : H]$ in this case is infinite.

Exercise: For the subgroup $(\mathbb{Z}, +) < (\mathbb{R}, +)$, show that the set of (left) cosets are parametrized by $[0, 1)$, so that we have

$$\mathbb{R} = \bigsqcup_{t \in [0,1)} (t + \mathbb{Z}).$$

Exercise: For a vector subspace $W \subset V$, we consider the subgroup $(W, +) < (V, +)$. Then the set of cosets are given by the *affine translates* $v + W$, $v \in V$, of W in V. Let $W' \subset V$ be a subspace complementary to W, meaning that it satisfies the following conditions:

- $\dim W' = \dim V - \dim W$, and
- $W \cap W' = \{0\}$.

Show that the set of cosets of W in V are parametrized by W', so that

$$V = \bigsqcup_{v \in W'} (v + W).$$

Example 5.1.4. Consider the dihedral group D_n, and the cyclic subgroup $\langle r \rangle$ generated by the anticlockwise rotation by $2\pi/n$. Since

$$D_n = \{\text{id}, r, r^2, \ldots, r^{n-1}, s, rs, r^2 s, \ldots, r^{n-1} s\},$$

we directly see that

$$D_n = \langle r \rangle \sqcup s\langle r \rangle.$$

Example 5.1.5. Consider the n-th symmetric group S_n, and the subgroup $A_n < S_n$ consisting of all the even permutations. Let $\tau \in S_n$ be a transposition. **Exercise:** the map $\sigma \mapsto \tau\sigma$ gives a bijection between A_n and $B_n := S_n \setminus A_n$, the set of all odd permutations. Hence we have $S_n = A_n \sqcup \tau A_n$.

Example 5.1.6. Recall that $S_3 (= D_3)$ is generated by $\rho = (123)$ and $\mu = (12)$. (In fact, $S_3 = \{\mathrm{id}, \rho, \rho^2, \mu, \rho\mu, \rho^2\mu\}$.) For the cyclic subgroup $H = \langle \mu \rangle < S_3$, the left cosets are given by $H, \rho H, \rho^2 H$ so that we have $S_3 = H \sqcup \rho H \sqcup \rho^2 H$.

Week 6

6.1 The Theorem of Lagrange

Theorem 6.1.1 (Lagrange)**.** *Let G be a finite group. Let H be subgroup of G, then $|H|$ divides $|G|$. More precisely, $|G| = [G : H] \cdot |H|$.*

Proof. We already know that the left cosets of H partition G. That is:

$$G = a_1H \sqcup a_2H \sqcup \ldots \sqcup a_{[G:H]}H,$$

where $a_iH \cap a_jH = \emptyset$ if $i \neq j$. Hence, $|G| = \sum_{i=1}^{[G:H]} |a_iH|$. Note that one of the left cosets, say a_1H, is equal to $H = eH$. The theorem follows if we show that the size of each left coset of H is equal to $|H|$.

For each left coset S of H, pick an element $a \in S$, and define a map $\psi : H \longrightarrow S$ as follows:

$$\psi(h) = ah.$$

We want to show that ψ is bijective.

For any $s \in S$, by definition of a left coset (as an equivalence class) we have $s = ah$ for some $h \in H$. Hence, ψ is surjective. If $\psi(h') = ah' = ah = \psi(h)$ for some $h', h \in H$, then $h' = a^{-1}ah' = a^{-1}ah = h$. Hence, ψ is one-to-one.

So we have a bijection between two finite sets. Hence, $|S| = |H|$. □

Corollary 6.1.2. *Let G be a finite group. The order of every element of G divides the order of G.*

Proof. Since G is finite, any element of $g \in G$ has finite order $|g|$. Since the order of the subgroup:

$$H = \langle g \rangle = \{e, g, g^2, \ldots, g^{|g|-1}\}$$

is equal to $|g|$, it follows from Lagrange's Theorem that $|g| = |H|$ divides $|G|$. □

Corollary 6.1.3. *If the order of a group G is prime, then G is a cyclic group.*

Proof. Let G be a group such that $p = |G|$ is a prime number. Since $p \geq 2$, there exists $a \in G \setminus \{e\}$. The above corollary them says that $|a| \mid p$. But $|a| \neq 1$, so we must have $|a| = p$. This means that $G = \langle a \rangle$. □

Corollary 6.1.4. *If a group G is finite, then for all $g \in G$ we have:*

$$g^{|G|} = e.$$

Proof. The previous corollary already says that $|g| \mid |G|$, i.e. $|G| = k \cdot |g|$. So $g^{|G|} = (g^{|g|})^k = e$. □

6.2 Group Homomorphisms

Definition. Let $G = (G, *)$, $G' = (G', *')$ be groups.

A **group homomorphism** ϕ from G to G' is a map $\phi : G \longrightarrow G'$ which satisfies:

$$\phi(a * b) = \phi(a) *' \phi(b),$$

for all $a, b \in G$.

If ϕ is also bijective, then ϕ is called an **isomorphism**. If there exists an isomorphism $\phi : G \longrightarrow G'$ between two groups G and G', then we say G is **isomorphic** to G', and denoted by $G \simeq G'$.

Remark. Note that if a homomorphism ϕ is bijective, then $\phi^{-1} : G' \longrightarrow G$ is also a homomorphism, and consequently, ϕ^{-1} is an isomorphism.

Isomorphic groups have the same algebraic structure and thus share the same algebraic properties – they only differ by relabeling of their elements. One of the most fundamental questions in group theory is to classify groups up to isomorphisms.

Example 6.2.1.

- Let V, W be vector spaces over $\mathbb{R}$ (or $\mathbb{C}$). Then a linear transformation $\phi : V \longrightarrow W$ is in particular a homomorphism between abelian groups $\phi : (V, +) \longrightarrow (W, +)$.
- The determinant $\det : \mathrm{GL}(n, \mathbb{R}) \longrightarrow \mathbb{R}^\times$ is a group homomorphism.
- The exponential map $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)$ is an isomorphism from the additive group of real numbers to the multiplicative group of positive real numbers, whose inverse if given by the logarithm $\log : (\mathbb{R}_{>0}, \cdot) \longrightarrow (\mathbb{R}, +)$.
- For any nonzero integer n, we have $n\mathbb{Z} < \mathbb{Z}$, and the map $\phi : n\mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $nk \mapsto k$ is an isomorphism. Note that $n\mathbb{Z} < \mathbb{Z}$ is proper whenever $|n| > 1$, so a proper subgroup can be isomorphic to the parent group!

- On the other hand, for any integer n, the map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $k \mapsto nk$ is a homomorphism but *not* an isomorphism unless $|n| = 1$.
- Given a positive integer n, the remainder map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by mapping k to its remainder when divided by n is a surjective homomorphism (check this!).
- The map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $k \mapsto k + 1$ is *not* a homomorphism.

Example 6.2.2. The group:

$$G = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \,\middle|\, \theta \in \mathbb{R} \right\}$$

is isomorphic to

$$G' = \{z \in \mathbb{C} : |z| = 1\}.$$

Here, the group operation on G is matrix multiplication, and the group operation on G' is the multiplication of complex numbers.

Proof. Each element in G' is equal to $e^{i\theta}$ for some $\theta \in \mathbb{R}$. Define a map $\phi : G \longrightarrow G'$ as follows:

$$\phi\left(\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\right) = e^{i\theta}.$$

Exercise: ϕ is a bijective group homomorphism. □

Here are some basic properties of group homomorphisms:

Claim 6.2.3. *If $\phi : G \longrightarrow G'$ is a group homomorphism, then:*

1. $\phi(e_G) = e_{G'}$.
2. $\phi(g^{-1}) = \phi(g)^{-1}$, *for all $g \in G$.*
3. $\phi(g^n) = \phi(g)^n$, *for all $g \in G$, $n \in \mathbb{Z}$.*

Proof. We prove the first claim, and leave the rest as an exercise.

Since e_G is the identity element of G, we have $e_G * e_G = e_G$. On the other hand, since ϕ is a group homomorphism, we have:

$$\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) *' \phi(e_G).$$

Since G' is a group, $\phi(e_G)^{-1}$ exists in G', hence:

$$\phi(e_G)^{-1} *' \phi(e_G) = \phi(e_G)^{-1} *' (\phi(e_G) *' \phi(e_G))$$

The left-hand side is equal to $e_{G'}$, while by the associativity of $*'$ the right-hand side is equal to $\phi(e_G)$. □

Let $\phi : G \longrightarrow G'$ be a homomorphism of groups. The **image** of ϕ is defined as:

$$\operatorname{im}\phi := \phi(G) := \{\phi(g) : g \in G\}$$

The **kernel** of ϕ is defined as:

$$\ker\phi = \{g \in G : \phi(g) = e_{G'}\}.$$

Proposition 6.2.4. *The image of ϕ is a subgroup of G'. The kernel of ϕ is a subgroup of G.*

Proof. **Exercise.** □

Claim 6.2.5. *A group homomorphism $\phi : G \longrightarrow G'$ is one-to-one if and only if* $\ker\phi = \{e_G\}$.

Proof. **Exercise.** □

As we have mentioned, isomorphisms preserve algebraic properties. Here are some examples.

Claim 6.2.6. *Let G be a cyclic group, then any group isomorphic to G is also cyclic.*

Proof. **Exercise.** □

Example 6.2.7. The cyclic group $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. Each element of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is of order at most 2. Since $|G| = 4$, G cannot be generated by any of its elements. Hence, G is not cyclic, so it cannot be isomorphic to the cyclic group $\mathbb{Z}_4$. □

Claim 6.2.8. *Let G be an abelian group, then any group isomorphic to G is abelian.*

Example 6.2.9. The group D_6 has 12 elements. We have seen that $D_6 = \langle r_2, s\rangle$, where r_2 is a rotation of order 6, and s is a reflection, which has order 2. So, it is reasonable to ask if D_6 is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$. The answer is no. For $\mathbb{Z}_6 \times \mathbb{Z}_2$ is abelian, but D_6 is not.

Remark. Both claims remain true if we replace isomorphism by a surjective homomorphism, namely, if $\phi : G \longrightarrow G'$ is a surjective homomorphism, then we have

- G is cyclic $\Rightarrow$ G' is cyclic,
- G is abelian $\Rightarrow$ G' is abelian.

Try to prove these assertions by yourself!

Exercise. Check that the restriction of a homomorphism $\phi : G \longrightarrow G'$ to a subgroup $H < G$ gives a homomorphism from H to G'.

Proposition 6.2.10. *If $\phi : G \longrightarrow G'$ is an isomorphism, then $|\phi(g)| = |g|$ for any $g \in G$.*

Proof. By the previous exercise, the restriction of ϕ to the subgroup $\langle g \rangle$ gives a homomorphism

$$\phi|_{\langle g \rangle} : \langle g \rangle \longrightarrow G',$$

which is injective and with image

$$\operatorname{im} \phi|_{\langle g \rangle} = \langle \phi(g) \rangle.$$

So $\phi|_{\langle g \rangle}$ is an isomorphism from $\langle g \rangle$ to $\langle \phi(g) \rangle$; in particular, we have $|\phi(g)| = |g|$. □

6.3 Classification of cyclic groups

Example 6.3.1. Let $H = \{r_0, r_1, r_2, \ldots, r_{n-1}\}$ be the subgroup of D_n consisting of all rotations, where r_1 denotes the anti-clockwise rotation by the angle $2\pi/n$, and $r_k = r_1^k$. Then, H is isomorphic to $\mathbb{Z}_n = (\mathbb{Z}_n, +_n)$.

Proof. Define $\phi : H \longrightarrow \mathbb{Z}_n$ as follows:

$$\phi(r_1^k) = \overline{k}, \quad k \in \mathbb{Z},$$

where $\overline{k}$ denotes the remainder of the division of k by n.

The map ϕ is well defined: If $r_1^k = r_1^{k'}$, then $r_1^{k-k'} = e$, which implies that $n = |r_1|$ divides $k - k'$. Hence, $\overline{k} = \overline{k'}$ in $\mathbb{Z}_n$.

For $i, j \in \mathbb{Z}$, we have $r_1^i r_1^j = r_1^{i+j}$; hence:

$$\phi(r_1^i r_1^j) = \phi(r_1^{i+j}) = \overline{i+j} = i +_n j = \phi(r_1^i) +_n \phi(r_1^j).$$

This shows that ϕ is a homomorphism. It is clear that ϕ is surjective, which then implies that ϕ is one-to-one, for the two groups have the same size. Hence, ϕ is a bijective homomorphism, i.e. an isomorphism. □

In fact:

Theorem 6.3.2. *Any infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$. Any cyclic group of finite order n is isomorphic to $(\mathbb{Z}_n, +_n)$.*

Proof. Write $G = \langle g \rangle$.

Suppose $|G| = \infty$. Consider the map

$$\phi : \mathbb{Z} \to G, \quad k \mapsto g^k.$$

ϕ is a homomorphism because $\phi(k_1 + k_2) = g^{k_1+k_2} = g^{k_1} \cdot g^{k_2} = \phi(k_1) \cdot \phi(k_2)$. ϕ is injective because $\phi(k_1) = \phi(k_2)$ implies that $g^{k_1} = g^{k_2}$ which forces $k_1 = k_2$ as $|g| = \infty$. ϕ is surjective because G is generated by g. We conclude that ϕ is an isomorphism.

If $|G| = n < \infty$, Claim 2.1.2 says that we can write

$$G = \langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}.$$

Consider the bijection

$$\phi : G \to \mathbb{Z}_n, \quad g^i \mapsto i.$$

We have

$$\begin{aligned}
\phi(g^{i_1} \cdot g^{i_2}) &= \phi(g^{i_1+i_2}) \\
&= \begin{cases} \phi(g^{i_1+i_2}) & \text{if } i_1 + i_2 < n, \\ \phi(g^{i_1+i_2-n}) & \text{if } i_1 + i_2 \geq n \end{cases} \\
&= \begin{cases} i_1 + i_2 & \text{if } i_1 + i_2 < n, \\ i_1 + i_2 - n & \text{if } i_1 + i_2 \geq n \end{cases} \\
&= \phi(g^{i_1}) + \phi(g^{i_2}),
\end{aligned}$$

so ϕ is an isomorphism. □

So for any $n \in \mathbb{Z} \cup \{\infty\}$, there is a unique (up to isomorphism) cyclic group of order n. In particular, we have the following:

Corollary 6.3.3. *If G and G' are two finite cyclic groups of the same order, then G is isomorphic to G'.*

For example, the multiplicative group of m-th roots of unity

$$U_m = \{z \in \mathbb{C} : z^m = 1\} = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}\},$$

where $\zeta_m = e^{2\pi \mathbf{i}/m} = \cos(2\pi/m) + \mathbf{i}\sin(2\pi/m) \in \mathbb{C}$, is cyclic of order m. So it is isomorphic to $\mathbb{Z}_m$, and an isomorphism is given by

$$\phi : \mathbb{Z}_m \longrightarrow U_m, \quad k \mapsto \zeta_m^k.$$

Week 7

7.1 Rings

Definition. A **ring** R (or $(R, +, \cdot)$) is a set equipped with two binary operations:

$$+, \cdot : R \times R \to R$$

which satisfy the following properties:

1. $(R, +)$ is an abelian group.
2. (a) The multiplication $\cdot$ is associative, i.e.

   $$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

   for all $a, b, c \in R$.

   (b) There is an element $1 \in R$ (called the *multiplicative identity*) such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
3. (Distributive laws:)

   (a) $a \cdot (b + c) = a \cdot b + a \cdot c$ and

   (b) $(a + b) \cdot c = a \cdot c + b \cdot c$

   for all $a, b, c \in R$.

Example 7.1.1. The following sets, equipped with the usual operations of addition and multiplication, are rings:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
2. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ (Polynomials with integer, rational, real, complex coefficients, respectively.)

3. $\mathbb{Q}[\sqrt{2}] = \{\sum_{k=0}^{n} a_k(\sqrt{2})^k : a_k \in \mathbb{Q}, n \in \mathbb{N}\} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

4. For a fixed n, the set of $n \times n$ matrices with integer coefficients.

5. $C[a, b] = \{f : [a, b] \to \mathbb{R} : f$ is continuous.$\}$

6. $(\mathbb{N}, +, \cdot)$ is *not* a ring because $(\mathbb{N}, +)$ is not a group.

Remark.
- For convenience's sake, we often write ab for $a \cdot b$.
- In the definition, commutativity is required of addition, but not of multiplication.
- Every element has an additive inverse, but *not necessarily* a multiplicative inverse. That is, there may be an element $a \in R$ such that $ab \neq 1$ for all $b \in R$.

Claim 7.1.2. *In a ring R, there is a unique additive identity and a unique multiplicative identity.*

Proof. We already know that the additive identity is unique.

Suppose there is an element $1' \in R$ such that $1'r = r$ or all $r \in R$, then in particular $1'1 = 1$. But $1'1 = 1'$ since 1 is a multiplicative identity element, so $1' = 1$. □

Claim 7.1.3. *For any r in a ring R, its additive inverse $-r$ is unique. That is, if $r + r' = r + r'' = 0$, then $r' = r''$.*

If r has a multiplicative inverse, then it is also unique. That is, if $rr' = 1 = r'r$ and $rr'' = 1 = r''r$, then $r' = r''$.

Claim 7.1.4. *For all elements r in a ring R, we have $0r = r0 = 0$.*

Proof. By distributive laws,

$$0r = (0 + 0)r = 0r + 0r$$

Adding $-0r$ (additive inverse of $0r$) to both sides, we have:

$$0 = (0r + 0r) + (-0r) = 0r + (0r + (-0r)) = 0r + 0 = 0r.$$

The proof of $r0 = 0$ is similar and we leave it as an exercise. □

Claim 7.1.5. *For all elements r in a ring, we have $(-1)(-r) = (-r)(-1) = r$.*

Proof. We have:

$$0 = 0(-r) = (1 + (-1))(-r) = -r + (-1)(-r).$$

Adding r to both sides, we obtain

$$r = r + (-r + (-1)(-r)) = (r + -r) + (-1)(-r) = (-1)(-r).$$

We leave it as an exercise to show that $(-r)(-1) = r$. □

Claim 7.1.6. *For all r in a ring R, we have: $(-1)r = r(-1) = -r$*

Proof. **Exercise** □

Claim 7.1.7. *If R is a ring in which $1 = 0$, then $R = \{0\}$. That is, it has only one element.*

We call such an R the **zero ring**.

Proof. **Exercise.** □

Definition. A ring R is said to be **commutative** if $ab = ba$ for all $ab \in R$.

Example 7.1.8.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all commutative rings, so are $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.
- For a fixed natural number $n > 1$, the ring of $n \times n$ matrices with integer coefficients, under the usual operations of addition and multiplication, is not commutative.

Modulo m arithmetic

Example 7.1.9. Let m be a positive integer. Consider the set

$$\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}.$$

For any integer $n \in \mathbb{Z}$, we denote by $\overline{n}$ the remainder of the division of of n by m: $n = mq + r$.

On the other hand, two integers $a, b \in \mathbb{Z}$ are said to be **congruent modulo** m, denoted as $a \equiv b \mod m$, if $m \mid (a - b)$. This defines an equivalence relation on $\mathbb{Z}$, and $\mathbb{Z}_m$ can be regarded as parametrizing the equivalence classes, namely, every $a \in \mathbb{Z}$ is congruent modulo m to exactly one element in $\mathbb{Z}_m$.

Remark. Congruence modulo m is exactly the same as the relation defined by the subgroup $m\mathbb{Z} < \mathbb{Z}$, so the above partition is the same as that given by cosets of $m\mathbb{Z}$ in $\mathbb{Z}$.

We equip $\mathbb{Z}_m$ with addition $+_m$ and multiplication $\cdot_m$ defined as follows: For $a, b \in \mathbb{Z}_m$, let:

$$a +_m b = \overline{a + b},$$
$$a \cdot_m b = \overline{a \cdot b},$$

where the addition and multiplication on the right are the usual addition and multiplication for integers.

Proposition 7.1.10. *With addition and multiplication thus defined, $\mathbb{Z}_m$ is a commutative ring.*

Proof.

1. We already know that $(\mathbb{Z}_m, +_m)$ is an abelian group.
2. Note that If $a \equiv a' \mod m$ and $b \equiv b' \mod m$, then $ab \equiv a'b' \mod m$. So for $r_1, r_2 \in \mathbb{Z}_m$, we have

   $$\overline{r_1 r_2} \equiv r_1 r_2 \equiv \overline{r_1} \cdot \overline{r_2} \equiv \overline{\overline{r_1} \cdot \overline{r_2}} \mod m.$$

   For $a, b, c \in \mathbb{Z}_m$, we have:

   $$a \cdot_m (b \cdot_m c) = a \cdot_m \overline{bc} = \overline{\overline{a} \cdot \overline{bc}} = \overline{a(bc)},$$

   which by the associativity of multiplication for integers is equal to:

   $$\overline{(ab)c} = \overline{\overline{ab} \cdot \overline{c}} = \overline{ab} \cdot_m c = (a \cdot_m b) \cdot_m c.$$

   So, $\cdot_m$ is associative.
3. **Exercise:** We can take 1 to be the multiplicative identity.
4. For $a, b \in \mathbb{Z}_m$, $a \cdot_m b = \overline{a \cdot b} = \overline{b \cdot a} = b \cdot_m a$. So $\cdot_m$ is commutative.
5. Lastly, we need to prove distributivity. For $a, b, c \in \mathbb{Z}_m$, we have:

   $$a \cdot_m (b +_m c) = \overline{\overline{a} \cdot \overline{b + c}} = \overline{a \cdot (b + c)} = \overline{ab + ac} = \overline{\overline{ab} + \overline{ac}} = a \cdot_m b +_m a \cdot_m c.$$

   It now follows from the distributivity from the left, proven above, and the commutativity for $\cdot_m$, that distributivity from the right also holds:

   $$(a +_m b) \cdot_m c = a \cdot_m c + b \cdot_m c.$$

□

Rings of polynomials

Definition. Let R be a nonzero commutative ring.

A **polynomial** with coefficients in R (in one-variable) is a formal sum

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

with $a_i \in R$ such that $a_i = 0$ for all but finitely many i's.

If $a_i \neq 0$ for some i, then the largest such i is called the **degree** of $f(x)$, denoted by $\deg f(x)$.

We denote by $R[x]$ the set of all polynomials with coefficients in R.

Given

$$f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} b_i x^i \in R[x],$$

we define the addition and multiplication as follows (as usual):

$$f(x) + g(x) := \sum_{i=0}^{\infty} (a_i + b_i) x^i,$$
$$f(x)g(x) := \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) x^i.$$

Proposition 7.1.11. *With addition and multiplication thus defined, $R[x]$ is a commutative ring.*

Proof. **Exercise.** □

Remark. A polynomial $f(x)$ defines a function $f : R \to R$ by $a \mapsto f(a)$. But $f(x)$ may not be determined by $f : R \to R$. For example, the polynomials

$$f(x) = 1 + x + x^2, g(x) = 1 \in \mathbb{Z}_2[x]$$

define the same (constant) function from $\mathbb{Z}_2$ to itself.

Week 8

Integral domains and fields

Definition. A nonzero commutative ring R is called an **integral domain** if the product of two nonzero elements is always nonzero.

Definition. A nonzero element r in a ring R is called a **zero divisor** if there exists nonzero $s \in R$ such that $rs = 0$.

So a nonzero commutative ring R is an integral domain if and only if it has no zero divisors.

Example 8.0.1.
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all integral domains, so are $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$. (More generally, if R is an integral domain, so is $R[x]$.)

2. Since $2, 3 \not\equiv 0 \mod 6$, and $2 \cdot 3 = 6 \equiv 0 \mod 6$, the ring $\mathbb{Z}_6$ is not an integral domain.

3. Consider $R = C[-1, 1]$, the ring of all continuous functions on $[-1, 1]$, equipped with the usual operations of addition and multiplication for functions. Let:

$$f = \begin{cases} -x, & x \leq 0, \\ 0, & x > 0. \end{cases} \quad , \quad g = \begin{cases} 0, & x \leq 0, \\ x, & x > 0. \end{cases}$$

   Then f and g are nonzero elements of R, but $fg = 0$. So R is not an integral domain.

Claim 8.0.2. *A commutative ring R is an integral domain if and only if the cancellation law holds for multiplication, i.e. whenever $ca = cb$ and $c \neq 0$, we have $a = b$.*

Proof. Suppose R is an integral domain. If $ca = cb$, then by distributive laws, $c(a - b) = c(a + -b) = 0$. Since R is an integral domain, we have either $c = 0$ or $a - b = 0$. So, if $c \neq 0$, we must have $a = b$.

Conversely, suppose cancellation law holds. Suppose there are nonzero $a, b \in R$ such that $ab = 0$. By a previous result we know that $0 = a0$. So, $ab = a0$, which by the cancellation law implies that $b = 0$, a contradiction. $\square$

Definition. Let R be a ring. We say that an element $a \in R$ is a **unit** if it has a multiplicative inverse, i.e. there is an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Example 8.0.3. The only units of $\mathbb{Z}$ are ± 1.

Example 8.0.4. Let R be the ring of all real valued functions on $\mathbb{R}$. Then, any function $f \in R$ satisfying $f(x) \neq 0, \forall x$, is a unit.

Example 8.0.5. Let R be the ring of all continuous real valued functions on $\mathbb{R}$, then $f \in R$ is a unit if and only if it is either strictly positive or strictly negative.

Claim 8.0.6. *The only units of* $\mathbb{Q}[x]$ *are nonzero constants.*

Proof. Given any $f \in \mathbb{Q}[x]$ such that $\deg f > 0$, for all nonzero $g \in \mathbb{Q}[x]$ we have

$$\deg fg \geq \deg f > 0 = \deg 1;$$

hence, $fg \neq 1$. If $g = 0$, then $fg = 0 \neq 1$. So, f has no multiplicative inverse.

If f is a nonzero constant, then $f^{-1} = \frac{1}{f}$ is a constant polynomial in $\mathbb{Q}[x]$, and $f\left(\frac{1}{f}\right) = \left(\frac{1}{f}\right)f = 1$. So, f is a unit.

Finally, if $f = 0$, then $fg = 0 \neq 1$ for all $g \in \mathbb{Q}[x]$, so the zero polynomial has no multiplicative inverse. $\square$

Definition. A **field** is a commutative ring, with $1 \neq 0$, in which every nonzero element is a unit.

In other words, a nonzero commutative ring F is a field if and only if every nonzero element $r \in F$ has a multiplicative inverse r^{-1}, i.e. $rr^{-1} = r^{-1}r = 1$.

Example 8.0.7.

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.
2. The polynomial rings $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ are not fields.

Note that if every nonzero element of a commutative ring has a multiplicative inverse, then that ring is an integral domain:

$$ca = cb \implies c^{-1}ca = c^{-1}cb \implies a = b.$$

So we conclude that

Proposition 8.0.8. *A field is an integral domain.*

Proposition 8.0.9. *Let* $k \in \mathbb{Z}_m \setminus \{0\}$.

- *If gcd$(k,m) > 1$, then k is a zero divisor.*
- *If gcd$(k,m) = 1$, then k is a unit.*

Proof. Let $d := \gcd(k,m)$.

If $d > 1$, then m/d is a nonzero element in $\mathbb{Z}_m$, and we have $k \cdot_m (m/d) = \overline{(k/d) \cdot m} = 0$ in $\mathbb{Z}_m$. So k is a zero divisor.

If $d = 1$, then there exist $a, b \in \mathbb{Z}$ such that $ak + bm = 1$. But this means we have $\overline{a}k = 1$ in $\mathbb{Z}_m$. So k is a unit. □

Hence, the set of zero divisors in $\mathbb{Z}_m$ is precisely given by

$$\{k \in \mathbb{Z}_m \setminus \{0\} : \gcd(k,m) > 1\}$$

and the set of units in $\mathbb{Z}_m$ is precisely given by

$$\mathbb{Z}_m^\times := \{k \in \mathbb{Z}_m \setminus \{0\} : \gcd(k,m) = 1\}.$$

In particular, we have the following

Corollary 8.0.10. *$\mathbb{Z}_m$ is a field if and only if m is prime.*

Notation. For p prime, we often denote the field $\mathbb{Z}_p$ by $\mathbb{F}_p$.

Claim 8.0.11. *Equipped with the usual operations of addition and multiplications for real numbers, $F = \mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is a field.*

Proof. Observe that: $(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$ lies in F, and $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in F$. Hence, addition and multiplication for real numbers are well-defined operations on F. As operations on $\mathbb{R}$, they are commutative, associative, and satisfy the distributive laws; therefore, as F is a subset of $\mathbb{R}$, they also satisfy these properties as operations on F.

It is clear that 0 and 1 are the additive and multiplicative identities of F. Given $a + b\sqrt{2} \in F$, where $a, b \in \mathbb{Q}$, it is clear that its additive inverse $-a - b\sqrt{2}$ also lies in F. Hence, F is a commutative ring.

To show that F is a field, for every nonzero $a + b\sqrt{2}$ in F, we need to find its multiplicative inverse. As an element of the field $\mathbb{R}$, the multiplicative inverse of $a + b\sqrt{2}$ is:

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}}.$$

It remains to show that this number lies in F. Observe that:

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

We claim that $a^2 - 2b^2 \neq 0$. Suppose $a^2 - 2b^2 = 0$, then either (i) $a = b = 0$, or (ii) $b \neq 0$, $\sqrt{2} = |a/b|$. Since we have assumed that $a + b\sqrt{2}$ is nonzero, case (i) cannot hold. But case (ii) also cannot hold because $\sqrt{2}$ is know to be irrational. Hence $a^2 - 2b^2 \neq 0$, and:

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2},$$

which lies in F. □

Claim 8.0.12. *All finite integral domains are fields.*

Proof. Let R be an integral domain with n elements, where n is finite. Write $R = \{a_1, a_2, \ldots, a_n\}$. We want to show that for any nonzero element $a \neq 0$ in R, there exists i, $1 \leq i \leq n$, such that a_i is the multiplicative inverse of a. Consider the set $S = \{aa_1, aa_2, \ldots, aa_n\}$. Since R is an integral domain, the cancellation law holds. In particular, since $a \neq 0$, we have $aa_i = aa_j$ if and only if $i = j$. The set S is therefore a subset of R with n distinct elements, which implies that $S = R$. In particular, $1 = aa_i$ for some i. This a_i is the multiplicative inverse of a. □

Field of Fractions (optional)

An integral domain fails to be a field precisely when there is a nonzero element with no multiplicative inverse. The ring $\mathbb{Z}$ is such an example, for $2 \in \mathbb{Z}$ has no multiplicative inverse. But any nonzero $n \in \mathbb{Z}$ has a multiplicative inverse $\frac{1}{n}$ in $\mathbb{Q}$, which is a field. So, a question one could ask is, can we "enlarge" a given integral domain to a field, by formally adding multiplicative inverses to the ring?

An Equivalence Relation

Given an integral domain R (commutative, with $1 \neq 0$). We consider the set: $R \times R_{\neq 0} := \{(a, b) : a, b \in R, b \neq 0\}$. We define a relation $\equiv$ on $R \times R_{\neq 0}$ as follows:

$$(a, b) \equiv (c, d) \text{ if } ad = bc.$$

Lemma 8.0.13. *The relation $\equiv$ is an equivalence relation.*

In other words, the relation $\equiv$ is:

Reflexive: $(a, b) \equiv (a, b)$ for all $(a, b) \in R \times R$

Symmetric: If $(a, b) \equiv (c, d)$, then $(c, d) \equiv (a, b)$.

Transitive: If $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$, then $(a, b) \equiv (e, f)$.

Proof. **Exercise.** $\square$

In general, given an equivalence relation $\sim$ on a set S, the **equivalent class** of an element $a \in S$ is the set of all elements in $s \in S$ which are equivalent to a (i.e. $s \sim a$).

Notation: For notational convenience, to describe an equivalence class we may pick any element s (called a **representative**) belonging to the class, and label the class as $[s]$. Note that if $s \sim t$, then $[s] = [t]$.

Due to the properties (reflexive, symmetric, transitive), of an equivalence relation, the equivalent classes form a **partition** of S. Namely, equivalent classes of non-equivalent elements are disjoint:

$$[s] \cap [t] = \varnothing$$

if $s \not\sim t$; and the union of all equivalent classes is equal to S:

$$\bigcup_{s \in S} [s] = S.$$

Definition. Given an equivalence relation $\sim$ on a set S, the **quotient set** $S/\sim$ is the set of all equivalence classes of S, with respect to $\sim$.

We now return to our specific situation of $R \times R_{\neq 0}$, with $\equiv$ defined as above. We define addition $+$ and multiplication $\cdot$ on $R \times R_{\neq 0}$ as follows:

$$(a, b) + (c, d) := (ad + bc, bd)$$
$$(a, b) \cdot (c, d) := (ac, bd)$$

Claim 8.0.14. *Suppose* $(a, b) \equiv (a', b')$ *and* $(c, d) \equiv (c', d')$*, then:*

1. $(a, b) + (c, d) \equiv (a', b') + (c', d')$.
2. $(a, b) \cdot (c, d) \equiv (a', b') \cdot (c', d')$.

Proof. By definition, $(a, b) + (c, d) = (ad + bc, bd)$, and $(a', b') + (c', d') = (a'd' + b'c', b'd')$. Since by assumption $ab' = a'b$ and $cd' = c'd$, we have:

$$(ad + bc)b'd' = adb'd' + bcb'd' = a'bdd' + c'dbb' = (a'd' + b'c')bd;$$

hence, $(a, b) + (c, d) \equiv (a', b') + (c', d')$.

For multiplication, by definition we have $(a, b) \cdot (c, d) = (ac, bd)$ and $(a', b') \cdot (c', d') = (a'c', b'd')$. Since

$$acb'd' = ab'cd' = a'bc'd = a'c'bd,$$

we have $(a, b) \cdot (c, d) \equiv (a', b') \cdot (c', d')$. $\square$

Let:

$$\mathrm{Frac}(R) := (R \times R_{\neq 0})/\equiv,$$

and define $+$ and $\cdot$ on $\mathrm{Frac}(R)$ as follows:

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$
$$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$$

Corollary 8.0.15. *$+$ and $\cdot$ thus defined are well-defined binary operations on* $\mathrm{Frac}(R)$.

Namely, we get the same output in $\mathrm{Frac}(R)$ regardless of the choice of representatives of the equivalence classes.

Claim 8.0.16. *The set* $\mathrm{Frac}(R)$*, equipped with $+$ and $\cdot$ defined as above, forms a field, with additive identity* $0 = [(0,1)]$ *and multiplicative identity* $1 = [(1,1)]$*. The multiplicative inverse of a nonzero element* $[(a,b)] \in \mathrm{Frac}(R)$ *is* $[(b,a)]$.

Proof. **Exercise.** □

Definition. $\mathrm{Frac}(R)$ is called the **Fraction Field** of R.

Remark. Note that $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, if we identify $a/b \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, with $[(a,b)] \in \mathrm{Frac}(\mathbb{Z})$.

Week 9

9.1 Homomorphisms

Definition. Let R and R' be rings. A **ring homomorphism** from R to R' is a map $\phi : R \to R'$ with the following properties:

1. $\phi(1_R) = 1_{R'}$;
2. $\phi(a+b) = \phi(a) + \phi(b)$, for all $a, b \in R$;
3. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, for all $a, b \in R$.

Note that if $\phi : R \to R'$ is a homomorphism, then:

- $$\phi(0) = \phi(0+0) = \phi(0) + \phi(0),$$
  which implies that $\phi(0) = 0$.
- For all $a \in R$, $0 = \phi(0) = \phi(-a+a) = \phi(-a) + \phi(a)$, which implies that $\phi(-a) = -\phi(a)$.
- If u is a unit in R, then $1 = \phi(u \cdot u^{-1}) = \phi(u)\phi(u^{-1})$, and $1 = \phi(u^{-1} \cdot u) = \phi(u^{-1})\phi(u)$; which implies that $\phi(u)$ is a unit, with $\phi(u)^{-1} = \phi(u^{-1})$.

Example 9.1.1. The map $\phi : \mathbb{Z} \to \mathbb{Q}$ defined by $\phi(n) = n$ is a homomorphism, since:

1. $\phi(1) = 1$,
2. $\phi(n +_{\mathbb{Z}} m) = n +_{\mathbb{Q}} m$.
3. $\phi(n \cdot_{\mathbb{Z}} m) = n \cdot_{\mathbb{Q}} m$.

Example 9.1.2. Fix an integer m which is larger than 1. For $n \in \mathbb{Z}$, let $\overline{n}$ denote the remainder of the division of n by m. That is:

$$n = mq + \bar{n}, \quad 0 \leq \bar{n} < m$$

Recall that $\mathbb{Z}_m = \{0, 1, 2, \ldots, m\}$ is a ring, with $s + t = \overline{s +_{\mathbb{Z}} t}$ and $s \cdot t = \overline{s \cdot_{\mathbb{Z}} t}$, for all $s, t \in \mathbb{Z}_m$.

Define a map $\phi : \mathbb{Z} \to \mathbb{Z}_m$ as follows:

$$\phi(n) = \overline{n}, \quad \forall n \in \mathbb{Z}.$$

Then, ϕ is a homomorphism.

Proof.

1. $\phi(1) = \overline{1} = 1$,
2. $\phi(s + t) = \overline{s +_{\mathbb{Z}} t} = \overline{\overline{s} +_{\mathbb{Z}} \overline{t}} = \overline{s} + \overline{t} = \phi(s) + \phi(t)$.
3. $\phi(st) = \overline{s \cdot_{\mathbb{Z}} t} = \overline{\overline{s} \cdot_{\mathbb{Z}} \overline{t}} = \overline{s} \cdot \overline{t} = \phi(s)\phi(t)$.

□

Example 9.1.3. For any ring R, define a map $\phi : \mathbb{Z} \to R$ as follows:

$$\phi(0) = 0;$$

For $n \in \mathbb{N}$,

$$\phi(n) = n \cdot 1_R := \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}};$$

$$\phi(-n) = -n \cdot 1_R := n \cdot (-1_R) = \underbrace{(-1_R) + (-1_R) + \cdots + (-1_R)}_{n \text{ times}}.$$

The map ϕ is a homomorphism.

Proof. **Exercise.** □

Remark. In fact this is the only homomorphism from $\mathbb{Z}$ to R since we need to have $\phi(1) = 1_R$ and this implies that

$$\phi(n) = n \cdot \phi(1) = n \cdot 1_R.$$

Example 9.1.4. Let R be a commutative ring. For each element $r \in R$, we may define a map $\phi_r : R[x] \to R$ as follows:

$$\phi_r\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} a_k r^k$$

The map ϕ_r is a ring homomorphism.

Proof. *Shown in class.* □

Definition. If a ring homomorphism $\phi : R \to R'$ is a bijective map, we say that ϕ is an **isomorphism**, and that R and R' are **isomorphic** as rings.

Notation. If R and R' are isomorphic, we write $R \cong R'$.

Claim 9.1.5. *If $\phi : R \to R'$ is an isomorphism, then $\phi^{-1} : R' \to R$ is an isomorphism.*

Proof. Since ϕ is bijective, ϕ^{-1} is clearly bijective. It remains to show that ϕ^{-1} is a homomorphism:

1. Since $\phi(1_R) = 1_{R'}$, we have $\phi^{-1}(1_{R'}) = \phi^{-1}(\phi(1_R)) = 1_R$.

2. For all $b_1, b_2 \in R'$, we have

$$\begin{aligned}\phi^{-1}(b_1 + b_2) &= \phi^{-1}(\phi(\phi^{-1}(b_1)) + \phi(\phi^{-1}(b_2))) \\ &= \phi^{-1}(\phi(\phi^{-1}(b_1) + \phi^{-1}(b_2))) = \phi^{-1}(b_1) + \phi^{-1}(b_2)\end{aligned}$$

3. For all $b_1, b_2 \in R'$, we have

$$\begin{aligned}\phi^{-1}(b_1 \cdot b_2) &= \phi^{-1}(\phi(\phi^{-1}(b_1)) \cdot \phi(\phi^{-1}(b_2))) \\ &= \phi^{-1}(\phi(\phi^{-1}(b_1) \cdot \phi^{-1}(b_2))) = \phi^{-1}(b_1) \cdot \phi^{-1}(b_2)\end{aligned}$$

This shows that ϕ^{-1} is a bijective homomorphism. □

The key point here is that an isomorphism is more than simply a bijective map, for it must preserve algebraic structure. For example, there is a bijective map $f : \mathbb{Z} \to \mathbb{Q}$ since both are countable, but they cannot be isomorphic as rings: Suppose $\phi : \mathbb{Z} \to \mathbb{Q}$ is an isomorphism. Then we must have $\phi(n) = n\phi(1) = n$ for any $n \in \mathbb{Z}$. So ϕ cannot be surjective.

Theorem 9.1.6. *If F is a field, then $\mathrm{Frac}(F) \cong F$.*

Proof. Define a map $\phi : F \to \mathrm{Frac}(F)$ as follows:

$$\phi(s) = [(s, 1)], \quad \forall s \in F.$$

Exercise:

1. Show that ϕ is a homomorphism.

2. Show that ϕ is bijective.

□

Let R be a commutative ring, let $R[x,y]$ denote the ring of polynomials in x, y with coefficients in R:

$$R[x,y] = \left\{ \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j : m, n \in \mathbb{Z}_{\geq 0}, a_{ij} \in R \right\}$$

Claim 9.1.7. *$R[x,y]$ is isomorphic to $R[x][y]$.*

(Here, $R[x][y]$ is the ring of polynomials in y with coefficients in the ring $R[x]$.)

Proof. We define a map $\phi : R[x,y] \to R[x][y]$ as follows:

$$\phi\left(\sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j\right) = \sum_{j=0}^{n} \left(\sum_{i=0}^{m} a_{ij} x^i\right) y^j$$

Exercise: Show that ϕ is a homomorphism.

It remains to show that ϕ is one-to-one and onto.

For $f = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j \in \ker \phi$, we have:

$$\phi(f) = \sum_{j=0}^{n} \left(\sum_{i=0}^{m} a_{ij} x^i\right) y^j = 0_{R[x][y]} = \sum_{j=0} 0_{R[x]} \cdot y^j,$$

which implies that, for $0 \leq j \leq n$, we have:

$$\sum_{i=0}^{m} a_{ij} x^i = 0_{R[x]}, \quad 0 \leq i \leq m.$$

Hence,

$$a_{ij} = 0_R, \quad \text{for } 0 \leq i \leq m, 0 \leq j \leq n,$$

which implies that $\ker \phi = \{0\}$. Hence, ϕ is one-to-one.

Given $g = \sum_{j=0}^{n} p_j y^j \in R[x][y]$, where $p_j \in R[x]$. We want to find $f \in R[x,y]$ such that $\phi(f) = g$. Let m be the maximum degree of the p_j's. We may write:

$$g = \sum_{j=0}^{n} \left(\sum_{i=0}^{m} a_{ji} x^i\right) y^j,$$

where a_{ji} is the coefficient of x^i in p_j, with $a_{ji} = 0$ if $i > \deg p_j$. It is clear that:

$$\phi\left(\sum_{i=0}^{m} \sum_{j=0}^{n} a_{ji} x^i y^j\right) = g.$$

Hence, ϕ is onto.

□

9.1.1 Subrings

Definition. Let R be a ring. A subset S of R is said to be a **subring** of R if it is a ring under the addition $+_R$ and multiplication $\times_R$ associated with R, and its additive and multiplicative identity elements $0, 1$ are those of R.

To show that a subset S of a ring R is a subring, it suffices to show that:

- S contains the multiplicative identity of R.
- $a - b \in S$ for any $a, b \in S$.
- S is closed under multiplication, i.e. $a \cdot b \in S$ for all $a, b \in S$.

Definition. The **kernel** of a ring homomorphism $\phi : R \to R'$ is the set:

$$\ker \phi := \{a \in R : \phi(a) = 0\}$$

The **image** of ϕ is the set:

$$\operatorname{im} \phi := \{b \in R' : b = \phi(a) \text{ for some } a \in R\}.$$

Proposition 9.1.8. *Let $\phi : R \to R'$ be a ring homomorphism.*

1. *If S is a subring of R, then $\phi(S)$ is a subring of R'.*
2. *If S' is a subring of R', then $\phi^{-1}(S')$ is a subring of R.*

Proof. Let us prove 1. and leave 2. as an exercise. So let S be a subring of R.

- Since $1 \in S$, we have $\phi(1) = 1 \in \phi(S)$.
- $\phi(a) - \phi(b) = \phi(a - b) \in \phi(S)$ for any $a, b \in S$.
- $\phi(a) \cdot \phi(b) = \phi(a \cdot b) \in \phi(S)$ for any $a, b \in S$.

We conclude that $\phi(S)$ is a subring of R'. □

Corollary 9.1.9. *For a ring homomorphism $\phi : R \to R'$, $\operatorname{im} \phi$ is a subring of R'.*

Remark. Note that $\ker \phi$ is not a subring unless R' is the zero ring.

Claim 9.1.10. *A ring homomorphism $\phi : R \to R'$ is one-to-one if and only if $\ker \phi = \{0\}$.*

Proof. Suppose ϕ is one-to-one. For any $a \in \ker \phi$, we have $\phi(0) = \phi(a) = 0$, which implies that $a = 0$ since ϕ is one-to-one. Hence, $\ker \phi = \{0\}$.

Suppose $\ker \phi = \{0\}$. If $\phi(a) = \phi(a')$, then $0 = \phi(a) - \phi(a') = \phi(a - a')$, which implies that $a - a' \in \ker \phi = \{0\}$. So, $a - a' = 0$, which implies that $a = a'$. Hence, ϕ is one-to-one. □

Proposition 9.1.11. *A subring of a field is an integral domain.*

Proof. Let F be a field and $S \subset F$ be a subring. Suppose we have $a, b \in S$ with $a \neq 0$ such that $ab = 0$. We need to show that $b = 0$. Since F is a field, $a \neq 0$ implies that it is a unit, i.e. it has a multiplicative inverse a^{-1}. So we have $0 = a^{-1}(ab) = b$. □

For example, any subring of $\mathbb{C}$ is an integral domain. This produces a lot of interesting examples which are important in number theory. For instance, the *ring of Gaussian integers*:

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

is an integral domain. More generally, for any $\xi \in \mathbb{C}$, the subset

$$\mathbb{Z}[\xi] = \{f(\xi) : f(x) \in \mathbb{Z}[x]\} \subset \mathbb{C}$$

is an integral domain.

9.2 Ideals

Definition. An **ideal** I in a commutative ring R is a subset of R which satisfies the following properties:

1. $0 \in I$;
2. If $a, b \in I$, then $a + b \in I$.
3. For all $a \in I$, we have $ar \in I$ for all $r \in R$.

If an ideal I is a proper subset of R, we say it is a **proper ideal**.

Remark. Note that if an ideal I contains 1, then $r = 1 \cdot r \in I$ for all $r \in R$, which implies that $I = R$.

Example 9.2.1. For any commutative ring R, the set $\{0\}$ is an ideal, since $0+0 = 0$, and $0 \cdot r = 0$ for all $r \in R$.

R itself is also an ideal.

An ideal $I \subsetneq R$ is called **proper** and an ideal $\{0\} \subsetneq I \subset R$ is called **nontrivial**.

Example 9.2.2. For all $m \in \mathbb{Z}$, the set $I = m\mathbb{Z} := \{mn : n \in \mathbb{Z}\}$ is an ideal:

1. $0 = m \cdot 0 \in I$;
2. $mn_1 + mn_2 = m(n_1 + n_2) \in I$.

3. Given $mn \in I$, for all $l \in \mathbb{Z}$, we have $mn \cdot l = m \cdot nl \in I$.

Example 9.2.3. Generalizing the above example, consider a commutative ring R. Let $a \in R$. Then

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

is an ideal, called the **principal ideal** generated by a.

Proof. 1. $0 = 0a \in (a)$;

2. Given $r_1 a, r_2 a \in (a)$, we have $r_1 a + r_2 a = (r_1 + r_2)a \in (a)$.

3. For all $ra \in (a)$ and $a \in R$, we have $s(ra) = (sr)a \in (a)$.

□

More generally, given any nonempty subset $A \subset R$, the set of finite linear combinations of elements in A:

$$(A) := \{r_1 a_1 + r_2 a_2 + \cdots + rka_k : k \in \mathbb{Z}_{>0}, r_i \in R, a_i \in A\}$$

is an ideal in R, called the **ideal generated by** A.

Claim 9.2.4. *If $\phi : R \to R'$ is a ring homomorphism, then $\ker \phi$ is an ideal of R.*

Proof. 1. Since ϕ is a homomorphism, we have $\phi(0) = 0$. Hence, $0 \in \ker \phi$.

2. If $a, b \in \ker \phi$, then $\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$. Hence, $a + b \in \ker \phi$.

3. Given any $a \in \ker \phi$, for all $r \in R$ we have $\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0$. Hence, $ar \in \ker \phi$ for all $r \in R$.

□

Example 9.2.5. Recall the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_m$ defined by $\phi(n) = \overline{n}$. The kernel of ϕ is:

$$\ker \phi = m\mathbb{Z} = (m).$$

Proposition 9.2.6. *A nonzero commutative ring R is a field if and only if its only ideals are $\{0\}$ and R.*

Proof. Suppose a nonzero commutative ring R is a field. If an ideal I of R is nonzero, it contains at least one nonzero element a of R. Since R is a field, a has a multiplicative inverse a^{-1} is R. Since I is a ideal, and $a \in I$, we have $1 = a^{-1}a \in I$. So, I is an ideal which contains 1, hence it must be the whole field R.

Conversely, let R be a nonzero commutative ring whose only ideals are $\{0\}$ and R. Given any nonzero element $a \in R$, the principal ideal (a) generated by a is nonzero because it contains $a \neq 0$. Hence, by hypothesis the ideal (a) is necessarily the whole ring R. In particular, the element 1 lies in (a), which means that there is an $r \in R$ such that $ar = 1$. This shows that any nonzero element of R is a unit. Hence, R is a field. □

Proposition 9.2.7. *Let F be a field, and R a nonzero ring. Any ring homomorphism $\phi : F \to R$ is necessarily one-to-one.*

Proof. Since R is not a zero ring, it contains $1 \neq 0$. So, $\phi(1) = 1 \neq 0$, which implies that $\ker \phi$ is a proper ideal of F. Since F is a field, we must have $\ker \phi = \{0\}$. It now follows from a previous claim that ϕ is one-to-one. □

Week 10

10.1 Quotient Rings

Let R be a commutative ring. Let I be an ideal of R. Then in particular I is an additive subgroup of $(R,+)$. Let R/I denote the set of all cosets of I in $(R,+)$, namely, the set of elements of the form

$$\overline{r} = r + I = \{r + a : a \in I\}, \quad r \in R.$$

Terminology: We sometimes call $\overline{r}$ the **residue** of r in R/I.

Note that $\bar{r} = \bar{0}$ if and only if $r \in I$; more generally, $\bar{r} = \bar{r'}$ if and only if $r - r' \in I$.

Remark. Recall that R/I is nothing but the set of equivalence classes of the following relation on R:

$$a \sim b, \quad \text{if } b - a \in I.$$

Notation/Terminology: If $a \sim b$, we say that a is **congruent modulo** I to b, and write:

$$a \equiv b \mod I.$$

It is tempting to define addition and multiplication on R/I using those operations on R:

$$\overline{r} + \overline{r'} = \overline{r + r'},$$
$$\overline{r} \cdot \overline{r'} = \overline{rr'},$$

for any $\overline{r}, \overline{r'} \in R/I$.

Observe that: for all $r, r' \in R$, and $a, a' \in I$, we have

$$(r + a) + (r' + a') = (r + r') + (a + a') \in (r + r') + I = \overline{r + r'},$$

which implies $\overline{(r + a) + (r' + a')} = \overline{r + r'}$. So addition $+$ is indeed well-defined on R/I. Note that this only used the fact that I is an additive subgroup of $(R,+)$.

On the other hand, we have the following

Theorem 10.1.1. *Given any additive subgroup $I < (R, +)$. The multiplication*

$$\overline{r} \cdot \overline{r'} = \overline{rr'}$$

is well-defined on R/I if and only if I is an ideal in R.

Proof. Suppose that I is an ideal. Then for any $r, r' \in R$, and $a, a' \in I$, we have

$$(r + a) \cdot (r' + a') = rr' + ra' + r'a + aa' \in rr' + I = \overline{rr'}.$$

Hence the multiplication is well-defined.

Conversely, suppose the multiplication is well-defined, meaning that for any $r, r' \in R$ and $a, a' \in I$, we have $\overline{(r + a')(r' + a)} = \overline{rr'}$. In particular, we have $\overline{ra} = \overline{(r + 0)(0 + a)} = \overline{r0} = I$ which implies $ra \in I$ for any $r \in R$ and $a \in I$. So I is an ideal. □

Claim 10.1.2. *The set R/I, equipped with the addition $+$ and multiplication $\cdot$ defined above, is a commutative ring.*

Proof. We note here only that the additive identity element of R/I is $\overline{0} = 0 + I$, the multiplicative identity element of R/I is $\overline{1} = 1 + I$, and that $-\overline{r} = \overline{-r}$ for all $r \in R$.

We leave the rest of the proof (additive and multiplicative associativity, commutativity, distributive laws) as an **Exercise.** □

Claim 10.1.3. *The map $\pi : R \to R/I$, defined by*

$$\pi(r) = \overline{r}, \quad \forall r \in R.$$

is a surjective ring homomorphism with kernel $\ker \pi = I$.

Proof. **Exercise.** □

Theorem 10.1.4 (First Isomorphism Theorem)**.** *Let $\phi : R \longrightarrow R'$ be a ring homomorphism. Then:*

$$R/\ker \phi \cong \operatorname{im} \phi,$$

(i.e. $R/\ker \phi$ is isomorphic to $\operatorname{im} \phi$.)

Proof. We define a map $\overline{\phi} : R/\ker \phi \longrightarrow \operatorname{im} \phi$ as follows:

$$\overline{\phi}(\overline{r}) = \phi(r), \quad \forall\, r \in R,$$

where $\overline{r}$ is the residue of r in $R/\ker \phi$.

We first need to check that ϕ is well-defined. Suppose $\overline{r} = \overline{r'}$, then $r' - r \in \ker\phi$. We have:

$$\overline{\phi}(\overline{r'}) - \overline{\phi}(\overline{r}) = \phi(r') - \phi(r) = \phi(r' - r) = 0.$$

Hence, $\overline{\phi}(\overline{r'}) = \overline{\phi}(\overline{r})$. So, $\overline{\phi}(\overline{r})$ is defined regardless of the choice of representative for the equivalence class $\overline{r}$.

Next, we show that $\overline{\phi}$ is a homomorphism:

- $\overline{\phi}(\overline{1}) = \phi(1) = 1$;
- $\overline{\phi}(\overline{a} + \overline{b}) = \overline{\phi}(\overline{a+b}) = \phi(a+b) = \phi(a) + \phi(b) = \overline{\phi}(\overline{a}) + \overline{\phi}(\overline{b})$;
- $\overline{\phi}(\overline{a} \cdot \overline{b}) = \overline{\phi}(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(\overline{a})\overline{\phi}(\overline{b})$.

Finally, we show that $\overline{\phi}$ is a bijection, i.e. one-to-one and onto.

For any $r' \in \operatorname{im}\phi$, there exists $r \in R$ such that $\phi(r) = r'$. Since $\overline{\phi}(\overline{r}) = \phi(r) = r'$, $\overline{\phi}$ is onto.

Let r be an element in R such that $\overline{\phi}(\overline{r}) = \phi(r) = 0$. We have $r \in \ker\phi$, which implies that $\overline{r} = 0$ in $R/\ker\phi$. Hence, $\ker\overline{\phi} = \{0\}$, and it follows that $\overline{\phi}$ is one-to-one. ☐

Corollary 10.1.5. *If a ring homomorphism $\phi : R \longrightarrow R'$ is surjective, then:*

$$R' \cong R/\ker\phi$$

Example 10.1.6. Let m be a natural number. The remainder or mod m map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ defined by:

$$\phi(n) = \overline{n}, \quad \forall\, n \in \mathbb{Z},$$

where $\overline{n}$ is the remainder of the division of n by m, is a surjective homomorphism such that $\ker\phi = (m) = m\mathbb{Z}$. So, it follows from the First Isomorphism Theorem that:

$$\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}.$$

Example 10.1.7. The ring $\mathbb{Z}[i]/(1+3i)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.

Proof. Define a map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}[i]/(1+3i)$ as follows:

$$\phi(n) = \overline{n}, \quad \forall\, n \in \mathbb{Z},$$

where $\overline{n}$ is the equivalence class of $n \in \mathbb{Z}[i]$ modulo $(1+3i)$.

It is clear that ϕ is a homomorphism (**Exercise**).

Observe that in $\mathbb{Z}[i]$, we have:

$$1 + 3i \equiv 0 \mod (1 + 3i),$$

which implies that:

$$i \equiv 3 \mod (1 + 3i).$$

Hence, for all $a, b \in \mathbb{Z}$,

$$\overline{a + bi} = \overline{a + 3b} = \phi(a + 3b)$$

in $\mathbb{Z}[i]/(1 + 3i)$. Hence, ϕ is surjective.

Suppose n is an element of $\mathbb{Z}$ such that $\phi(n) = \overline{n} = 0$. Then, by the definition of the quotient ring we have:

$$n \in (1 + 3i).$$

This means that there exist $a, b \in \mathbb{Z}$ such that:

$$n = (a + bi)(1 + 3i) = (a - 3b) + (3a + b)i,$$

which implies that $3a + b = 0$, or equivalently, $b = -3a$. Hence:

$$n = a - 3b = a - 3(-3a) = 10a,$$

which implies that $\ker \phi \subseteq 10\mathbb{Z}$. Conversely, for all $m \in \mathbb{Z}$, we have:

$$\phi(10m) = \overline{10m} = \overline{(1 + 3i)(1 - 3i)m} = 0$$

in $\mathbb{Z}[i]/(1 + 3i)$. This shows that $10\mathbb{Z} \subseteq \ker \phi$. Hence, $\ker \phi = 10\mathbb{Z}$.

It now follows from the First Isomorphism Theorem that:

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}[i]/(1 + 3i).$$

□

Example 10.1.8. The rings $\mathbb{R}[x]/(x^2 + 1)$ and $\mathbb{C}$ are isomorphic.

Proof. Define a map $\phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ as follows:

$$\phi(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} a_k i^k.$$

Exercise: ϕ is a homomorphism.

For all $a + bi$ ($a, b \in \mathbb{R}$) in $\mathbb{C}$, we have:

$$\phi(a + bx) = a + bi.$$

Hence, ϕ is surjective.

It remains to compute $\ker\phi = \{f(x) = \sum_{k=0}^{n} a_k x^k : f(i) = 0\}$. Note that $f(x)$ is a real polynomial, so $f(i) = 0$ also implies that $f(-i) = 0$. Hence both $\pm i$ are roots of $f(x)$ if it lies in $\ker\phi$. Factor Theorem then tells us that $(x^2+1) = (x-i)(x+i) \mid f(x)$. So $\ker\phi \subset (x^2+1)$. On the other hand, i is a root of x^2+1, so we have $(x^2+1) \subset \ker\phi$. We conclude that $\ker\phi = (x^2+1)$.

It now follows from the First Isomorphism Theorem that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

□

Week 11

11.1 Polynomial ring as a PID

Recall that an ideal $(a) = \{ar : r \in R\}$ generated by one element $a \in R$ is called a **principal ideal**. Note that $R = (1)$ and $\{0\} = (0)$ are both principal ideals.

Definition. If R is an integral domain in which every ideal is principal, we say that R is a **Principal Ideal Domain** (*abbrev.* **PID**).

Any field is a PID because a field F contains only two ideals $(0) = \{0\}$ and $(1) = F$.

The first nontrivial example of a PID is given by $\mathbb{Z}$: Since every ideal I in $\mathbb{Z}$ is in particular an additive subgroup, the classification of subgroups of cyclic groups tells us that I can only be of the form $(m) = m\mathbb{Z}$. So any ideal is principal.

Next we claim that for any field F, the ring of polynomials $F[x]$ is also a PID.

To prove this we first establish the following:

Proposition 11.1.1. *Let R be a commutative ring. For all $d, f \in R[x]$, such that the leading coefficient of d is a unit in R, there exist $q, r \in R[x]$ such that:*

$$f = qd + r,$$

with $\deg r < \deg d$.

Proof. We prove by induction: The base case corresponds to the case where $\deg f < \deg d$; and the inductive step corresponds to showing that, for any fixed d, the claim holds for f if it holds for all f' with $\deg f' > \deg f$.

Base case: If $\deg f < \deg d$, we take $r = f$. Then, indeed $f = 0 \cdot d + r$, with $\deg r < \deg d$.

Inductive step: Let $d = \sum_{i=0}^{n} a_i x^i \in R[x]$ be fixed, where a_n is a unit in R. For any given $f = \sum_{i=0}^{m} b_i x^i \in R[x]$, $m \geq n$, suppose the claim holds for all f' with $\deg f' < \deg f$. Let:

$$f' = f - a_n^{-1} b_m x^{m-n} d.$$

Then, $\deg f' < \deg f$, hence by hypothesis there exist $q', r' \in R[x]$, with $\deg r' < \deg d$, such that:

$$f - a_n^{-1} b_m x^{m-n} d = f' = q'd + r',$$

which implies that:

$$f = (q' + a_n^{-1} b_m x^{m-n})d + r'.$$

So, $f = qd + r'$, where $q = q' + a_n^{-1} b_m x^{m-n} \in R[x]$, and $\deg r' < \deg d$. $\square$

Theorem 11.1.2. *Let F be a field. Then, $F[x]$ is a PID.*

Proof. Since F is a field, the previous claim holds for all $d, f \in F[x]$ such that $d \neq 0$.

Let I be an ideal of $F[x]$. Let d be a nonzero polynomial in I with the least leading degree. Such a d exists because the leading degree of a polynomial is a nonnegative integer. Since I is an ideal, we have $(d) \subseteq I$. It remains to show that $I \subseteq (d)$.

For all $f \in I$, by the division theorem we have:

$$f = qd + r,$$

for some $q, r \in F[x]$ such that $\deg r < \deg d$. Observe that $r = f - qd$ lies in I. Since d is a nonzero element of I with the least degree, the element r must necessarily be zero. In order words $f = qd$, which implies that $f \in (d)$. Hence, $I \subseteq (d)$, and we conclude that $I = (d)$. $\square$

11.2 Factorization of polynomials

Definition. Let F be a field. Let $f = \sum_{i=0}^{n} c_i x^i$ be a polynomial in $F[x]$. An element $a \in F$ is a **root** of f if:

$$f(a) := \sum_{i=0}^{n} c_i a^i = 0$$

in F.

Lemma 11.2.1. *For all $f \in F[x]$, $a \in F$, there exists $q \in F[x]$ such that:*

$$f = q(x - a) + f(a)$$

Proof. By the division theorem, there exist $q, r \in F[x]$ such that:

$$f = q(x - a) + r, \quad \deg r < \deg(x - a) = 1.$$

This implies that r is a constant polynomial. Viewing the polynomials as functions and evaluating both sides of the above equation at $x = a$, we have:

$$f(a) = q(a - a) + r = r.$$

□

Proposition 11.2.2. *Let F be a field, f a polynomial is $k[x]$. Then, $a \in k$ is a root of f if and only if $(x - a)$ divides f in $F[x]$.*

Proof. If $a \in F$ is a root of f, then by the previous lemma there exists $q \in F[x]$ such that:

$$f = q(x - a) + \underbrace{f(a)}_{=0} = q(x - a),$$

so $(x - a)$ divides f in $F[x]$.

Conversely, if $f = q(x - a)$ for some $q \in F[x]$, then $f(a) = q(a)(a - a) = 0$. Hence, a is a root of f. □

Theorem 11.2.3. *Let F be a field, f a nonzero polynomial in $F[x]$.*

1. *If f has degree n, then it has at most n roots in F.*

2. *If f has degree n and $a_1, a_2, \ldots, a_n \in F$ are distinct roots of f, then:*

$$f = c \cdot \Pi_{i=1}^{n}(x - a_i) := c(x - a_1)(x - a_2) \cdots (x - a_n)$$

   for some $c \in F$.

Proof.

1. We prove Part 1 of the claim by induction. If f has degree 0, then f is a nonzero constant, which implies that it has no roots. So, in this case the claim holds.

   Let f be a polynomial with degree $n > 0$. Suppose the claim holds for all nonzero polynomials with degrees strictly less than n. We want to show that the claim also holds for f. If f has no roots in F, then the claim holds for f since $0 < n$. If f has a root $a \in F$, then by the previous claim there exists $q \in F[x]$ such that:

$$f = q(x - a).$$

   For any other root $b \in F$ of f which is different from a, we have:

$$0 = f(b) = q(b)(b - a).$$

   Since F is a field, it has no zero divisors; so, it follows from $b - a \neq 0$ that $q(b) = 0$. In other words, b is a root of q. Since $\deg q < n$, by the induction hypothesis q has at most $n - 1$ roots. So, f has at most $n - 1$ roots different from a. This shows that f has at most n roots.

2. Let f be a polynomial in $F[x]$ which has $n = \deg f$ distinct roots $a_1, a_2, \ldots, a_n \in F$.

   If $n = 1$, then $f = c_0 + c_1 x$ for some $c_i \in F$, with $c_1 \neq 0$. We have:

   $$0 = f(a_1) = c_0 + c_1 a_1,$$

   which implies that: $c_0 = -c_1 a_1$. Hence,

   $$f = -c_1 a_1 + c_1 x = c_1(x - a_1).$$

   Suppose $n > 1$. Suppose for all $n' \in \mathbb{N}$, such that $1 \leq n' < n$, the claim holds for any polynomial of degree n' which has n' distinct roots in F. By the previous claim, there exists $q \in F[x]$ such that:

   $$f = q(x - a_n).$$

   Note that $\deg q = n - 1$. For $1 \leq i < n$, we have

   $$0 = f(a_i) = q(a_i) \underbrace{(a_i - a_n)}_{\neq 0}.$$

   Since F is a field, this implies that $q(a_i) = 0$ for $1 \leq i < n$. So, $a_1, a_2, \ldots, a_{n-1}$ are $n - 1$ distinct roots of q. By the induction hypothesis there exists $c \in F$ such that:

   $$q = c(x - a_1)(x - a_2) \cdots (x - a_{n-1}).$$

   Hence, $f = q(x - a_n) = c(x - a_1)(x - a_2) \cdots (x - a_{n-1})(x - a_n)$.

□

Corollary 11.2.4. *Let F be a field. Let f, g be nonzero polynomials in $F[x]$. Let $n = \max\{\deg f, \deg g\}$. If $f(a) = g(a)$ for $n + 1$ distinct $a \in F$. Then, $f = g$.*

Proof. Let $h = f - g$, then $\deg h \leq n$. By hypothesis, there are $n + 1$ distinct elements $a \in F$ such that $h(a) = f(a) - g(a) = 0$. If $h \neq 0$, then it is a nonzero polynomial with degree $\leq n$ which has $n + 1$ distinct roots, which contradicts the previous theorem. Hence, h must necessarily be the zero polynomial, which implies that $f = g$. □

Recall the theorem:

Theorem 11.2.5. *Let F be a field. The ring $F[x]$ is a PID.*

Definition. A polynomial in $F[x]$ is called a **monic polynomial** if its leading coefficient is 1.

Corollary 11.2.6. *Let F be a field. Let f, g be nonzero polynomials in $F[x]$. There exists a unique monic polynomial $d \in F[x]$ with the following properties:*

1. $(f, g) = (d)$
2. *d divides both f and g, i.e. there exists $a, b \in F[x]$ such that $f = ad$, $g = bd$.*
3. *There are polynomials $p, q \in F[x]$ such that $d = pf + qg$.*
4. *If $h \in F[x]$ is a divisor of f and g, then h divides d.*

Terminology. This $d \in F[x]$ is called the **greatest common divisor** (*abbrev.* **gcd**) of f and g.
We say that f and g are **relatively prime** if their gcd is 1.

Proof. 1. By the theorem, there exists $d = \sum_{i=0}^{n} a_i x^i \in F[x]$ such that $(d) = (f, g)$. Replacing d by $a_n^{-1} d$ if necessary, we may assume that d is a monic polynomial. It remains to show that d is unique.

Suppose $(d) = (d')$, where both d and d' are monic polynomials. Then, there exist nonzero $p, q \in F[x]$ such that:

$$d' = pd, \quad d = qd'.$$

Examining the degrees of the polynomials, we have:

$$\deg d' = \deg d + \deg p,$$

and:

$$\deg d = \deg q + \deg d' = \deg p + \deg q + \deg d.$$

This implies that $\deg p + \deg q = 0$. Hence, p and q must both have degree 0; in other words, they are constant polynomials. Moreover, we have $\deg d = \deg d'$. Comparing the leading coefficients of d' and pd, we have $p = 1$. Hence, $d = d'$.

2. $f \in (f, g) = (d)$ implies that d divides f; similarly, d divides g.
3. $d \in (d) = (f, g)$ implies that $d = pf + qg$ for some $p, q \in F[x]$.
4. Part 3. says that there are $p, q \in F[x]$ such that $d = pf + qg$. It is then clear that if h divides both f and g, then h must divide d.

□

Definition. A nonconstant polynomial $p \in F[x]$ is said to be **irreducible** if there do not exist $f, g \in F[x]$, with $\deg f, \deg g < \deg p$, such that $fg = p$.

Example 11.2.7.

- Any degree 1 polynomial $f(x) = ax + b$, $a \neq 0$, is irreducible in $F[x]$.
- x^2+1 is irreducible in $\mathbb{R}[x]$ but reducible in $\mathbb{C}[x]$. So irreducibility *is relative to* the field F.
- By the Fundamental Theorem of Algebra, which states that any nonconstant polynomial $f(x) \in \mathbb{C}[x]$ **splits over** $\mathbb{C}$ meaning that there exists $c, \alpha_1, \ldots, \alpha_n$ (where $n = \deg f(x)$) such that $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, the only irreducible polynomials in $\mathbb{C}[x]$ are degree 1 polynomials and the only irreducible polynomials in $\mathbb{R}[x]$ are polynomials of degree 1 and 2.

Week 12

12.1 Factorization of polynomials (cont'd)

Theorem 12.1.1. *Any PID D is a* **unique factorization domain** *(abbrev.* **UFD***) which means that any nonzero nonunit $r \in D$ can be factorized into a finite product of irreducible elements, and the factorization is unique up to reordering of factors (and also up to multiplication by units).*

Proof. Omitted. For those who are interested in it, see Chapter 11, Section 2 in M. Artin's *Algebra*. $\square$

Let F be a field. Then $F[x]$ is a PID.

Lemma 12.1.2. *A polynomial $f \in F[x]$ is a unit if and only if it is a nonzero constant polynomial.*

Proof. If $f, g \in F[x]$ are nonzero polynomials satisfying $fg = 1$, then comparing degrees on both sides gives $\deg f + \deg g = 0$. This is possible only if $\deg f = \deg g = 0$ which means that both f and g are constants. $\square$

So we have the following

Corollary 12.1.3. *Every nonconstant polynomial $f \in F[x]$ may be written as:*

$$f = cp_1 \cdots p_n,$$

where c is a nonzero constant, and each p_i is a monic irreducible polynomial in $F[x]$. The factorization is unique up to reordering of the factors.

Example 12.1.4. Unique Factorization does not necessarily hold if F is not a field. In $\mathbb{Z}_4[x]$, we have:

$$x^2 = x \cdot x = (x+2)(x-2).$$

All the factors are linear, so they are irreducible. But clearly $x + 2$ is not equal to x.

Theorem 12.1.5. *Let F be a field. Let p be a polynomial in $F[x]$. The following statements are equivalent:*

1. *$F[x]/(p)$ is a field.*

2. *$F[x]/(p)$ is an integral domain.*

3. *p is irreducible in $F[x]$.*

Proof. $1 \Rightarrow 2$: Clear, since every field is an integral domain.

$2 \Rightarrow 3$: If p is not irreducible, there exist $f, g \in F[x]$, with degrees strictly less than that of p, such that $p = fg$. Since $\deg f, \deg g < \deg p$, the polynomial p does not divide f or g in $F[x]$. Consequently, the equivalence classes $\overline{f}$ and $\overline{g}$ of f and g, respectively, modulo (p) is not equal to zero in $F[x]/(p)$. On the other hand, $\overline{f} \cdot \overline{g} = \overline{fg} = \overline{p} = 0$ in $F[x]/(p)$. This implies that $F[x]/(p)$ is not an integral domain, a contradiction. Hence, p is irreducible if $F[x]/(p)$ is an integral domain.

$3 \Rightarrow 1$: By definition, the multiplicative identity element 1 of a field is different from the additive identity element 0. So we need to check that the equivalence class of $1 \in F[x]$ in $F[x]/(p)$ is not 0. Since p is irreducible, by definition we have $\deg p > 0$. Hence, $1 \neq (p)$, for a polynomial of degree > 0 cannot divide a polynomial of degree 0 in $F[x]$. We conclude that that $1 \neq 0$ in $F[x]$.

Next, we need to prove the existence of the multiplicative inverse of any nonzero element in $F[x]/(p)$. Given any $f \in F[x]$ whose equivalence class $\overline{f}$ modulo (p) is nonzero in $F[x]/(p)$, we want to find its multiplicative inverse $\overline{f}^{-1}$. If $\overline{f} \neq 0$ in $F[x]/(p)$, then by definition $f - 0 \notin (p)$, which means that p does not divide f. Since p is irreducible, this implies that gcd$(p, f) = 1$. By Corollary 11.2.6, there exist $g, h \in F[x]$ such that $fg + hp = 1$. It is then clear that $\overline{g} = \overline{f}^{-1}$, since $fg - 1 = hp$ implies that $fg - 1 \in (p)$, which by definition means that $\overline{f} \cdot \overline{g} = \overline{fg} = 1$ in $F[x]/(p)$. □

12.2 Polynomials over $\mathbb{Z}$ and $\mathbb{Q}$

We are interested in determining which polynomials in $\mathbb{Q}[x]$ are irreducible.

Proposition 12.2.1. *Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $\mathbb{Q}[x]$, with $a_i \in \mathbb{Z}$. Every rational root r of f in $\mathbb{Q}$ has the form $r = b/c$ ($b, c \in \mathbb{Z}$ with gcd$(b, c) = 1$) where $b|a_0$ and $c|a_n$.*

Proof. Let $r = b/c$ be a rational root of f, where b, c are relatively prime integers. We have:

$$0 = \sum_{i=0}^{n} a_i (b/c)^i$$

Multiplying both sides of the above equation by c^n, we have:

$$0 = a_0c^n + a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_nb^n,$$

or equivalently:

$$a_0c^n = -(a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_nb^n).$$

Since b divides the right-hand side, and b and c are relatively prime, b must divide a_0. Similarly, we have:

$$a_nb^n = -(a_0c^n + a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_{n-1}cb^{n-1}).$$

Since c divides the right-hand side, and b and c are relatively prime, c must divide a_n. $\square$

This proposition is useful mainly for polynomials $f \in \mathbb{Q}[x]$ of $\deg \leq 3$, because such a polynomial is reducible only if it has a root in $\mathbb{Q}$.

Example 12.2.2. Consider the polynomial $f(x) = x^3 + 3x + 2 \in \mathbb{Q}[x]$. The above proposition says that the only possible roots of $f(x)$ are ± 1 or ± 2, but one directly checks that none of these is a root. So $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example 12.2.3. In fact the same argument applies to polynomials of $\deg \leq 3$ with coefficients in other fields. For example, we may consider $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$. Then one checks that f has no root in $\mathbb{Z}_5$ (by directly computing the values of $f(k)$ for each $k \in \mathbb{Z}_5$). So $f(x)$ is also irreducible in $\mathbb{Z}_5[x]$.

For a polynomial of arbitrary degree in $\mathbb{Q}[x]$, we will discuss some general methods to determine whether it is irreducible; these methods stem from a theorem of Gauss.

Definition. A polynomial $f \in \mathbb{Z}[x]$ is said to be **primitive** if the gcd of its coefficients is 1.

Remark. Note that if $f \in \mathbb{Z}[x]$ is monic, i.e. its leading coefficient is 1, then it is primitive.

More generally, if d is the gcd of the coefficients of $f \in \mathbb{Z}[x]$, then $\frac{1}{d}f$ is a primitive polynomial in $\mathbb{Z}[x]$.

Lemma 12.2.4 (Gauss's Lemma)**.** *If $f, g \in \mathbb{Z}[x]$ are both primitive, then fg is primitive.*

Proof. Write $f = \sum_{k=0}^{m} a_kx^k$, $g = \sum_{k=0}^{n} b_kx^k$. Then, $fg = \sum_{k=0}^{m+n} c_kx^k$, where:

$$c_k = \sum_{i+j=k} a_ib_j.$$

Suppose fg is not primitive. Then, there exists a prime p such that p divides c_k for $k = 0, 1, 2, \ldots, m + n$. Since f is primitive, there exists a least $u \in \{0, 1, 2, \ldots, m\}$ such that a_u is not divisible by p. Similarly, since g is primitive, there is a least $v \in \{0, 1, 2, \ldots, n\}$ such that b_u it not divisible by p. We have:

$$c_{u+v} = \sum_{\substack{i+j=u+v \\ (i,j)\neq(u,v)}} a_i b_j + a_u b_v,$$

hence:

$$a_u b_v = c_{u+v} - \sum_{\substack{i+j=u+v \\ i<u}} a_i b_j - \sum_{\substack{i+j=u+v \\ j<v}} a_i b_j$$

By the minimality conditions on u and v, each term on the right-hand side of the above equation is divisible by p. Hence, p divides $a_u b_v$, which by Euclid's Lemma implies that p divides either a_u or b_v, a contradiction. □

Lemma 12.2.5. *Every nonzero $f \in \mathbb{Q}[x]$ has a unique factorization:*

$$f = c(f) f_0,$$

where $c(f)$ is a positive rational number, and f_0 is a primitive polynomial in $\mathbb{Z}[x]$.

Definition. The rational number $c(f)$ is called the **content** of f.

Proof. **Existence:**
Write $f = \sum_{k=0}^{n} (a_k/b_k) x^k$, where $a_k, b_k \in \mathbb{Z}$. Let $B = b_0 b_1 \cdots b_n$. Then, $g := Bf$ is a polynomial in $\mathbb{Z}[x]$. Let d be the gcd of the coefficients of g. Let $D = \pm d$, with the sign chosen such that $D/B > 0$. Observe that $f = c(f) f_0$, where

$$c(f) = D/B,$$

and

$$f_0 := \frac{B}{D} f = \frac{1}{D} g$$

is a primitive polynomial in $\mathbb{Z}[x]$.

Uniqueness:
Suppose $f = e f_1$ for some positive $e \in \mathbb{Q}$ and primitive $f_1 \in \mathbb{Z}[x]$. We have:

$$e f_1 = c(f) f_0.$$

Writing $e/c(f) = u/v$ where u, v are relatively prime positive integers, we have:

$$u f_1 = v f_0.$$

Since $gcd(u, v) = 1$, v divides each coefficient of f_1, and u divides each coefficient of f_0. But f_0 and f_1 are primitive, so we must have $u = v = 1$. Hence, $e = c(f)$, and $f_1 = f_0$. □

Corollary 12.2.6. *For $f \in \mathbb{Z}[x]$, we have $c(f) \in \mathbb{Z}$.*

Proof. Let d be the gcd of the coefficients of f. Then, $(1/d)f$ is a primitive polynomial, and

$$f = d\left(\frac{1}{d}f\right)$$

is a factorization of f into a product of a positive rational number and a primitive polynomial in $\mathbb{Z}[x]$. Hence, by uniqueness of $c(f)$ and f_0, we have $c(f) = d \in \mathbb{Z}$. □

Corollary 12.2.7. *Let f, g, h be nonzero polynomials in $\mathbb{Q}[x]$ such that $f = gh$. Then $c(f) = c(g)c(h)$ and $f_0 = g_0 h_0$.*

Proof. The condition $f = gh$ implies that:

$$c(f)f_0 = c(g)c(h)g_0h_0,$$

where f_0, g_0, h_0 are primitive polynomials and $c(f), c(g), c(h)$ are positive rational numbers. By Gauss's Lemma, g_0h_0 is primitive. The uniqueness part of Lemma 12.2.5 implies that that $c(f) = c(g)c(h)$ and $f_0 = g_0h_0$. □

Theorem 12.2.8 (Gauss)**.** *Let f be a nonzero polynomial in $\mathbb{Z}[x]$. If $f = GH$ for some $G, H \in \mathbb{Q}[x]$, then $f = gh$ for some $g, h \in \mathbb{Z}[x]$, where $\deg g = \deg G$, $\deg h = \deg H$.*

Consequently, if f cannot be factored into a product of polynomials of smaller degrees in $\mathbb{Z}[x]$, then it is irreducible as a polynomial in $\mathbb{Q}[x]$.

Proof. Suppose $f = GH$ for some G, H in $\mathbb{Q}[x]$. Then $f = c(f)f_0 = c(G)c(H)G_0H_0$, where f_0, G_0, H_0 are primitive polynomials in $\mathbb{Z}[x]$. The above corollaries tell us that $c(G)c(H) = c(f) \in \mathbb{Z}_{>0}$ and $f_0 = G_0H_0$. Hence, $g := c(f)G_0$ and $h := H_0$ are polynomials in $\mathbb{Z}[x]$, with $\deg g = \deg G$, $\deg h = \deg H$, such that $f = gh$. □

Let p be a prime. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$. It is a field, since p is prime. For $a \in \mathbb{Z}$, let $\overline{a}$ denote the residue of a in $\mathbb{F}_p$.

Theorem 12.2.9. *Let $f = \sum_{k=0}^n a_k x^k$ be a monic polynomial in $\mathbb{Z}[x]$. If $\overline{f} := \sum_{k=0}^n \overline{a_k} x^k$ is irreducible in $\mathbb{F}_p[x]$ for some prime p, then f is irreducible in $\mathbb{Q}[x]$.*

Proof. Suppose $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$, but f is not irreducible in $\mathbb{Q}[x]$. By Gauss's theorem, there exist $g, h \in \mathbb{Z}[x]$ such that $\deg g, \deg h < \deg f$ and $f = gh$. Since f is by assumption monic, and $p \nmid 1$, we have $\deg \overline{f} = \deg f$. Moreover, $\overline{gh} = \overline{g} \cdot \overline{h}$. Hence, $\overline{f} = \overline{gh} = \overline{g} \cdot \overline{h}$, where $\deg \overline{g}, \deg \overline{h} < \deg \overline{f}$. This contradicts the irreducibility of $\overline{f}$ in $\mathbb{F}_p[x]$.

Hence, f is irreducible in $\mathbb{Q}[x]$ if $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$. □

Example 12.2.10. The polynomial $f(x) = x^4 - 5x^3 + 2x + 3 \in \mathbb{Q}[x]$ is irreducible.

Proof. Consider $\overline{f} = x^4 - \overline{5}x^3 + \overline{2}x + \overline{3} = x^4 - x^3 + 1$ in $\mathbb{F}_2[x]$. If we can show that $\overline{f}$ is irreducible, then by the previous theorem we can conclude that f is irreducible.

Since $\mathbb{F}_2 = \{0, 1\}$ and $\overline{f}(0) = \overline{f}(1) = 1 \neq 0$, we know right away that $\overline{f}$ has no linear factors. So, if $\overline{f}$ is not irreducible, it must be a product of two quadratic factors:

$$\overline{f} = (ax^2 + bx + c)(dx^2 + ex + g), \quad a, b, c, d, e, g \in \mathbb{F}_2.$$

Note that by assumption a, d are nonzero elements of $\mathbb{F}_2$, so $a = d = 1$. This implies that, in particular:

$$\begin{aligned} 1 &= \overline{f}(0) = cg \\ 1 &= \overline{f}(1) = (1 + b + c)(1 + e + g) \end{aligned}$$

The first equation implies that $c = g = 1$. The second equation then implies that $1 = (2 + b)(2 + e) = be$. Hence, $b = e = 1$. We have:

$$x^4 - x^3 + 1 = (x^2 + x + 1)(x^2 + x + 1) = x^4 + 2x^3 + 3x^2 + 2x + 1 = x^4 + x^2 + 1,$$

a contradiction.

Hence, $\overline{f}$ is irreducible in $\mathbb{F}_2[x]$, which implies that f is irreducible in $\mathbb{Q}[x]$. □

Theorem 12.2.11 (Eisenstein's Criterion)**.** *Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $\mathbb{Z}[x]$. If there exists a prime p such that $p|a_i$ for $0 \leq i < n$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Q}[x]$.*

Proof. We prove by contradiction. Suppose f is not irreducible in $\mathbb{Q}[x]$. Then, by Gauss's Theorem, there exists $g = \sum_{k=0}^{l} b_k x^k$, $h = \sum_{k=0}^{n-l} c_k x^k \in \mathbb{Z}[x]$, with $\deg g, \deg h < \deg f$, such that $f = gh$.

Consider the image of these polynomials in $\mathbb{F}_p[x]$. By assumption, we have:

$$\overline{a_n} x^n = \overline{f} = \overline{g}\overline{h}.$$

This implies that $\overline{g}$ and $\overline{h}$ are divisors of $\overline{a_n} x^n$. Since $\mathbb{F}_p$ is a field, unique factorization holds for $\mathbb{F}_p[x]$. Hence, we must have $\overline{g} = \overline{b_u} x^u$, $\overline{h} = \overline{c_{n-u}} x^{n-u}$, for some $u \in \{0, 1, 2, \ldots, l\}$. If $u < l$, then $n - u > n - l \geq \deg \overline{h}$, which cannot hold. So, we conclude that $\overline{g} = \overline{b_l} x^l$, $\overline{h} = \overline{c_{n-l}} x^{n-l}$. In particular, $\overline{b_0} = \overline{c_0} = 0$ in $\mathbb{F}_p$, which implies that p divides both b_0 and c_0. Since $a_0 = b_0 c_0$, we have $p^2 | a_0$, a contradiction. □

Example 12.2.12. The polynomial $x^5 + 3x^4 - 6x^3 + 12x + 3$ is irreducible in $\mathbb{Q}[x]$ by the Eisenstein's criterion using $p = 3$.

Week 13

13.1 Field extensions

Definition. A **subfield** F of a field E is a subring of E which is a field; in this case, we also say E is an extension of F, or E/F is a **field extension**. *Caution: Note that the notation E/F does not mean a quotient ring!*

Let E/F be a field extension (or a subfield F of a field E). Let α be an element of E. Consider the evaluation map

$$\phi_\alpha : F[x] \to E, f \mapsto f(\alpha),$$

which is a homomorphism such that $\phi_\alpha|_F = \mathrm{id}_F$. The image of ϕ_α is the subring

$$F[\alpha] := \operatorname{im} \phi_\alpha = \{f(\alpha) : f \in F[x]\}$$

in E. Since E is a field, $F[\alpha]$ is an integral domain. Also, the subfield

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in F[x], g(\alpha) \neq 0 \right\}$$

in E is precisely the field of fractions of $F[\alpha]$.

There are two scenarios:

- $\ker \phi_\alpha = \{0\}$, i.e. α is not a root of any nonzero polynomial $f \in F[x]$. In this case, we say $\alpha \in E$ is **transcendental** over F. Then ϕ_α gives an isomorphism $F[x] \cong F[\alpha]$.

- $\ker \phi_\alpha \neq \{0\}$, i.e. α is a root of some nonzero polynomial $f \in F[x]$. In this case, we say $\alpha \in E$ is **algebra** over F. Since $F[x]$ is a PID, $\ker \phi_\alpha = (p)$ for some $p \in F[x]$. Then the First Isomorphism Theorem implies that

$$\overline{\phi}_\alpha : F[x]/(p) \cong F[\alpha].$$

As $F[\alpha]$, Theorem 12.1.5 tells us that p is irreducible and that $F[x]/(p) \cong F[\alpha]$ is in fact a field. Hence we have

$$F[x]/(p) \cong F[\alpha] = F(\alpha).$$

Remark. Note that $F(\alpha)$ is the *smallest* subfield of E containing F and α. We say that $F(\alpha)$ is obtained from F by **adjoining** α.

Theorem 13.1.1. *Let E/F be a field extension and α be an element of E.*

1. *If α is a root of a nonzero polynomial $f \in F[x]$ (viewed as a polynomial in $E[x]$ with coefficients in F), then α is a root of an irreducible polynomial $p \in F[x]$, such that $p \mid f$ for any $f \in F[x]$ with $f(\alpha) = 0$.*

2. *For p be an irreducible polynomial $F[x]$ of which α is a root. Then, the map $\overline{\phi}_\alpha : F[x]/(p) \longrightarrow F(\alpha)$, defined by:*

$$\phi(\sum_{j=0}^{n} c_j x^j + (p)) = \sum_{j=0}^{n} c_j \alpha^j,$$

   is a ring isomorphism mapping $x + (p)$ to α and $a + (p)$ to a for any $a \in F$. (Here, $\sum_{j=0}^{n} c_j x^j + (p)$ is the equivalence class of $\sum_{j=0}^{n} c_j x^j \in F[x]$ modulo (p).)

3. *If $\alpha, \beta \in E$ are both roots of an irreducible polynomial p in $F[x]$, then there exists a ring isomorphism $\sigma : F(\alpha) \longrightarrow F(\beta)$, with $\sigma(\alpha) = \beta$ and $\sigma(s) = s$, for all $s \in F$.*

4. *Let p be an irreducible polynomial in $F[x]$ of which α is a root. Then, each element in $F(\alpha)$ has a unique expression of the form:*

$$c_0 + c_1\alpha + \cdots c_{n-1}\alpha^{n-1},$$

   where $c_i \in F$, and $n = \deg p$.

Proof. 1. We only need to prove the last part. So let $f \in F[x]$ be such that $f(\alpha) = 0$. Then $f \in \ker \phi_\alpha = (p)$ which means that $p \mid f$.

2. This was done above.

3. By Part 2, we have an isomorphism $\overline{\phi}_\beta : F[x]/(p) \longrightarrow F(\beta)$, such that $\overline{\phi}_\beta(x + (p)) = \beta$, and $\overline{\phi}_\beta(a + (p)) = a$ for all $a \in F$. So the map $\phi_{\alpha\beta} := \overline{\phi}_\beta \circ \overline{\phi}_\alpha^{-1} : F(\alpha) \longrightarrow F(\beta)$ is the desired isomorphism between $F(\alpha)$ and $F(\beta)$.

4. Since $\overline{\phi}_\alpha$ in Part 2 is an isomorphism, we know that each element $\gamma \in F(\alpha)$ is equal to $\overline{\phi}_\alpha(f + (p)) = f(\alpha) := \sum c_j \alpha^j$ for some $f = \sum c_j x^j \in F[x]$. By the division theorem for $F[x]$. There exist $m, r \in F[x]$ such that $f = mp + r$, with $\deg r < \deg p = n$. Write $r = \sum_{j=0}^{n-1} b_j x^j$, with $b_j = 0$ if $j > \deg r$. We have:

$$\gamma = \overline{\phi}_\alpha(f + (p)) = \overline{\phi}_\alpha(r + (p)) = \sum_{j=0}^{n-1} b_j \alpha^j.$$

It remains to show that this expression for γ is unique. Suppose $\gamma = g(\alpha) = \sum_{j=0}^{n-1} b'_j \alpha^j$ for some $g = \sum_{j=0}^{n-1} b'_j x^j \in F[x]$. Then, $g(\alpha) = r(\alpha) = \gamma$ implies that $(g - r) + (p) \in F[x]/(p)$ is in the kernel of the map $\overline{\phi}_\alpha$ in Part 2. Since $\overline{\phi}_\alpha$ is one-to-one, we have $(g - r) \equiv 0$ modulo (p), which implies that $p \mid g - r$ in $F[x]$. Since $\deg g, \deg r < p$, this implies that $g - r = 0$. So, the expression $\gamma = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ is unique.

□

Remark. Suppose p is an irreducible polynomial in $F[x]$ of which $\alpha \in E$ is a root. Part 4 of the theorem essentially says that $F(\alpha)$ is a vectors space of dimension $\deg p$ over F, with basis:

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}.$$

Example 13.1.2. Consider $F = \mathbb{Q}$ as a subfield of $E = \mathbb{R}$. The element $\alpha \in \sqrt[3]{2} \in \mathbb{R}$ is a root of the the polynomial $p = x^3 - 2 \in \mathbb{Q}[x]$, which is irreducible in $\mathbb{Q}[x]$ by the Eisenstein's Criterion for the prime 2.

The theorem applied to this case says that $\mathbb{Q}(\alpha)$, i.e. the smallest subfield of $\mathbb{R}$ containing $\mathbb{Q}$ and α, is equal to the set:

$$\{c_0 + c_1\alpha + c_2\alpha^2 : c_i \in \mathbb{Q}\}$$

The addition and multiplication operations in $\mathbb{Q}(\alpha)$ are those associated with $\mathbb{R}$, in other words:

$$(c_0 + c_1\alpha + c_2\alpha^2) + (b_0 + b_1\alpha + b_2\alpha^2) = (c_0 + b_0) + (c_1 + b_1)\alpha + (c_2 + b_2)\alpha^2,$$

$$\begin{aligned} &(c_0 + c_1\alpha + c_2\alpha^2) \cdot (b_0 + b_1\alpha + b_2\alpha^2) \\ &= c_0b_0 + c_0b_1\alpha + c_0b_2\alpha^2 + c_1b_0\alpha + c_1b_1\alpha^2 + c_1b_2\alpha^3 + c_2b_0\alpha^2 + c_2b_1\alpha^3 + c_2b_2\alpha^4 \\ &= (c_0b_0 + 2c_1b_2 + 2c_2b_1) + (c_0b_1 + c_1b_0 + 2c_2b_2)\alpha + (c_0b_2 + c_1b_1 + c_2b_0)\alpha^2 \end{aligned}$$

Exercise: Given a nonzero $\gamma = c_0 + c_1\alpha + c_2\alpha^2 \in \mathbb{Q}(\alpha)$, $c_i \in \mathbb{Q}$, find $b_0, b_1, b_2 \in \mathbb{Q}$ such that $b_0 + b_1\alpha + b_2\alpha^2$ is the multiplicative inverse of γ in $\mathbb{Q}(\alpha)$.

Example 13.1.3. Since $\sqrt[3]{2}$ is a root of $x^3 - 2$, the polynomial $p = x^3 - 2$ has a linear factor in $\mathbb{Q}(\sqrt[3]{2})[x]$. More precisely,

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2).$$

13.2 Finite fields

Theorem 13.2.1 (Kronecker)**.** *If F is a field, and f is a nonconstant polynomial in $F[x]$, then there exists a field extension E of F, such that $f \in F[x] \subset E[x]$ is a product of linear polynomials in $E[x]$.*

In other words, there exists a field extension E of F, such that:

$$f = c(x - \alpha_1) \cdots (c - \alpha_n),$$

for some $c, \alpha_i \in E$.

Proof. We prove by induction on $\deg f$.

If $\deg f = 1$, we are done.

Inductive Step: Suppose $\deg f > 1$. Suppose, for any field extension F' of F, and any polynomial $g \in F'[x]$ with $\deg g < \deg f$, there exists a field extension E of F' such that g splits into a product of linear factors in $E[x]$.

If f is irreducible, then $F' := F[x]/(f)$ contains a root α of f, namely $\alpha = x+(f) \in F[x]/(f)$. Hence, $f = (x-\alpha)q$ in $F'[x]$, with $\deg q < \deg f$. Moreover, F' is a field extension of F if we identify F with the subset $\{c+(p) : c \in k\} \subset F'$, where c is considered as a constant polynomial in $F[x]$. Then, by the induction hypothesis, there is an extension field E of F' such that q splits into a product of linear factors in $E[x]$. Consequently, f splits into a product of linear factors in $E[x]$.

If f is not irreducible, then $f = gh$ for some $g, h \in F[x]$, with $\deg g, \deg h < \deg f$. So, by the induction hypothesis, there is a field extension F' of F such that g is a product of linear factors in $F'[x]$. Hence, $f = (x-\alpha_1) \cdots (x-\alpha_n)h$ in $F'[x]$. Since $\deg h < \deg f$, by the inductive hypothesis there exists a field extension E of F' such that h splits into linear factors in $E[x]$. Hence, f is a product of linear factors in $E[x]$. □

Definition. Let D be an integral domain. The **characteristic** $\operatorname{char} D$ of D is the smallest positive integer n such that:

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

If such an integer does not exist, we say that the integral domain has **characteristic zero**.

Example 13.2.2. The field $\mathbb{Q}$ has characteristic zero. $\operatorname{char} \mathbb{Z}_p = p$ for any prime p.

Exercise: If an integral domain D has positive characteristic $\operatorname{char} D$, then $\operatorname{char} D$ is a prime number. Example: $\operatorname{char} \mathbb{F}_5 = 5$, which is prime.

Note that all finite integral domains have positive characteristics, but there are integral domains with positive characteristics which have infinitely many elements, e.g. the polynomial ring $\mathbb{F}_5[x]$.

Claim 13.2.3. *Let F be a finite field. Then, the number of elements of F is equal to p^n for some prime p and $n \in \mathbb{N}$.*

Proof. Since F is finite, it has finite characteristic. Since it is a field, $\operatorname{char} F$ is a prime p.

Exercise: $\mathbb{F}_p$ is isomorphic to a subfield of F.

Viewing $\mathbb{F}_p$ as a subfield of F, we see that F is a vector space over $\mathbb{F}_p$. Since the cardinality of F is finite, the dimension n of F over $\mathbb{F}_p$ must necessarily be finite. Hence, there exist n basis elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in F, such that each element of F may be expressed uniquely as:

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n,$$

where $c_i \in \mathbb{F}_p$. Since $\mathbb{F}_p$ has p elements, it follows that F has p^n elements. □

Theorem 13.2.4 (Galois)**.** *Given any prime p and $n \in \mathbb{N}$, there exists a finite field F with p^n elements.*

Proof. Consider the polynomial:

$$f = x^{p^n} - x \in \mathbb{F}_p[x]$$

By Kronecker's theorem, there exists a field extension K of $\mathbb{F}_p$ such that f splits into a product of linear factors in $K[x]$. Let:

$$F = \{\alpha \in K : f(\alpha) = 0\}.$$

Exercise: Let $g = (x - a_1)(x - a_2)\cdots(x - a_n)$ be a polynomial in $k[x]$, where k is a field. Show that the roots $a_1, a_2, \ldots, a_n$ are distinct if and only if $gcd(g, g') = 1$, where g' is the derivative of g.

In this case, we have $f' = p^n x^{p^n - 1} - 1 = -1$ in $\mathbb{F}_p[x]$. Hence, $gcd(f, f') = 1$, which implies by the exercise that the roots of f are all distinct. So, f has p^n distinct roots in K, hence F has exactly p^n elements.

It remains to show that F is a field. Let $q = p^n$. By definition, an element $a \in K$ belongs to F if and only if $f(a) = a^q - a = 0$, which holds if and only if $a^q = a$. For $a, b \in F$, we have:

$$(ab)^q = a^q b^a = ab,$$

which implies that F is closed under multiplication. Since K, being a extension of $\mathbb{F}_p$, has characteristic p. we have $(a+b)^p = a^p + b^p$. Hence,

$$\begin{aligned}(a+b)^q = (a+b)^{p^n} = ((a+b)^p)^{p^{n-1}} &= (a^p+b^p)^{p^{n-1}} \\ = (a^p+b^p)^p)^{p^{n-2}} &= (a^{p^2}+b^{p^2})^{p^{n-2}} \\ &= \cdots = a^{p^n} + b^{p^n} = a+b,\end{aligned}$$

which implies that F is closed under addition.

Let $0, 1$ be the additive and multiplicative identity elements, respectively, of K. Since $0^q = 0$ and $1^q = 1$, they are also the additive and multiplicative identity elements of F.

For nonzero $a \in F$, we need to prove the existence of the additive and multiplicative inverses of a in F.

Let $-a$ be the additive inverse of a in K. Since $(-1)^q = -1$ (even if $p = 2$, since $1 = -1$ in $\mathbb{F}_2$), we have:

$$(-a)^q = (-1)^q a^q = -a,$$

so $-a \in F$. Hence, $a \in F$ has an additive inverse in F.

Since $a^q = a$ in K, we have:

$$a^{q-2}a = a^{q-1} = 1$$

in K. Since $a \in F$ and F is closed under multiplication, $a^{q-2} = \underbrace{a \cdots a}_{q-2 \text{ times}}$ lies in F. So, a^{q-2} is a multiplicative inverse of a in F. □

Claim 13.2.5. *Let F be a field, f a nonzero irreducible polynomial in $F[x]$, then $F[x]/(f)$ is a vector space of dimension $\deg f$ over F.*

Proof. Let $E = F[x]/(f)$, then E is a field extension of F which contains a root α of f, namely, $\alpha = \overline{x} := x + (f)$. By Theorem 13.1.1, $E = F(\alpha)$, and every element in E may be expressed uniquely in the form:

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}, \quad c_i \in k,\ n = \deg f.$$

This shows that E is a vector space of dimension $\deg f$ over F. □

Corollary 13.2.6. *If F is a finite field with $|F|$ elements, and f is an irreducible polynomial of degree n in $F[x]$, then the field $F[x]/(f)$ has $|F|^n$ elements.*

Example 13.2.7. Let $p = 2$, $n = 2$. To construct a finite field with $p^n = 4$ elements. We first start with the finite field $\mathbb{F}_2$, then try to find an irreducible polynomial $f \in \mathbb{F}_2[x]$ such that $\mathbb{F}_2[x]/(f)$ has 4 elements. Based on our discussion so far, the degree of f should be equal to $n = 2$, since n is precisely the dimension of the desired finite field over $\mathbb{F}_2$. Consider $f = x^2 + x + 1$. Since p is of degree 2 and has no root in $\mathbb{F}_2$, it is irreducible in $\mathbb{F}_2[x]$. Hence, $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a field with 4 elements.