PMATH 347 by Yuru Liu

Eason Li

2024 F

Contents

Lecture 1 - Wednesday, September 04

1 Groups

Definition 1.1: Notation

We denote

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$
$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
$$\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}\}$$
$$\mathbb{R} = \text{set of real numbers}$$
$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = 1\}$$

Definition 1.2: Integer Modulo

For $n \in \mathbb{N}$, let $\mathbb{Z}_n$ be the set of integer modulo n, i.e.

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

where the congruence classes

$$[r] = \{z \in \mathbb{Z} : z \equiv r \pmod{n}\} \qquad (0 \leq r \leq n-1)$$

We note that for the set $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}$, S consists of two operations: addition and multiplication.

1.1 Matrices

Definition 1.3: Matrices

For $n \in \mathbb{N}$, an $n \times n$ matrix over $\mathbb{R}$ ($\mathbb{R}$ can be replaced by $\mathbb{Q}$ or $\mathbb{C}$) is an $n \times n$ array

$$A = [a_{ij}]$$

with $a_{ij} \in \mathbb{R}$ $(i \leq i, j \leq n)$. We denote by $\mathcal{M}_n(\mathbb{R})$ the set of all $n \times n$ matrices over $\mathbb{R}$. We can perform addition and multiplication on $\mathcal{M}_n(\mathbb{R})$ as follows: For $A = [a_{ij}]$ and $B = [b_{ij}] \in \mathcal{M}_n(\mathbb{R})$, we define

$$A + B = [a_{ij} + b_{ij}]$$

and

$$AB = [c_{ij}] \qquad \text{with} \qquad c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

1.2 Groups

Definition 1.4: Groups, Identity, Inverse

Ler G be a ser and $*$ be an operation on $G \times G$ ($*$ can be addition, multiplication, matrix addition, or matrix multiplication). We say $G = (G, *)$ is a **group** if it satisfies the following:

1. *Closure*: if $a, b \in G$, then $a * b \in G$;
2. *Assiciativity*: if $a, b, c \in G$, then $a * (b * c) = (a * b) * c$;
3. *Identity*: there exists $e \in G$ such that

$$a * e = a = e * a \qquad \forall\, a \in G$$

   We call e an **identity** of G;

4. *Inverse*: for all $a \in G$, we can find $b \in G$ such that

$$a * b = e = b * a$$

   We call b an **inverse** of a.

Definition 1.5: Abelian

We say a group is **abelian** if $a * b = b * a$ for all $a, b \in G$.

Exercise: Prove that in the definition of a group, it suffices to only have

$$e * a = a \qquad \text{and} \qquad b * a = e$$

In other words, we can conclude the other side of the equation from each one of them (but e and b needs to be on the same side of a).

Proposition 1.1

Let G be a group and $a \in G$, then

1. The identity in G is unique;
2. The inverse of a is unique.

Proof. If e_1 and $e_2 \in G$ are both identities, then

$$e_1 = e_1 * e_2 = e_2$$

Similarly, if b_1 and b_2 are inverses of a, then

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

done. □

Example 1.1

The sets $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all abelian groups, where the additive identity is 0 and the additive inverse of an element r is $(-r)$.
The set $(\mathbb{N}, +)$ is not a group as it has no identity (also no inverse).

Example 1.2

The sets $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are not groups as 0 has no inverse in $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Definition 1.6:

For a set S, let S^* denote the subset of S containing all elements with multiplicative inverse.

Example 1.3

For an example $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$.

Result 1.1

$(\mathbb{Q}^*, \cdot)$ is an abelian group with identity 1 and the inverse of element r is $1/r$.

Exercise: What is ${\mathbb{Z}_n}^*$?
Solution: This is the set of numbers:

$$Z_n^* = \{z \in \mathbb{Z}_n : \gcd(z, n) = 1\}$$

Example 1.4: Matrix with addition is an abelian group

The set $(\mathcal{M}_n(\mathbb{R}), +)$ is an abelian group where the additive identity is the zero matrix. The inverse of $M = [a_{ij}] \in \mathcal{M}_n(\mathbb{R})$ is $-M = [-a_{ij}]$.

Example 1.5: matrix with multiplication is not a group

Consider $(\mathcal{M}_n(\mathbb{R}), \cdot)$, the identity matrix is $I_n \in \mathcal{M}_n(\mathbb{R})$. However, it is not a group since not all matrices are invertible.

Definition 1.7:

The set $GL_n(\mathbb{R})$ is defined as:

$$GL_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) : \det(M) \neq 0\}$$

Note that if $A, B \in GL_n(\mathbb{R})$, then

$$\det(AB) = \det(A)\det(B) \neq 0$$

and thus $AB \in GL_n(\mathbb{R})$. The associativity of $GL_n(\mathbb{R})$ inherits from the one of $\mathcal{M}_n(\mathbb{R})$. Also, the identity matrix is the matrix I whose diagonal entries are all 1's and all other entries are 0's (this matrix has determinant of value 1). We simply have

$$IA = A = AI$$

for all $A \in GL_n(\mathbb{R})$. Finally, for $M \in GL_n(\mathbb{R})$, there exists $M^{-1} \in GL_n(\mathbb{R})$ such that

$$MM^{-1} = I = M^{-1}M$$

Result 1.2

Therefore, we may conclude that $GL_n(\mathbb{R})$ is a group.

Definition 1.8: General Linear Group

$(GL_n(\mathbb{R}), \cdot)$ is called the **general linear group of degree** n **over** $\mathbb{R}$.

Discovery 1.1

Notice that if $n \geq 2$, the group $(GL_n(\mathbb{R}), \cdot)$ is not abelian.

Exercise: What is $GL_1(\mathbb{R})$?
Solution: This is simply $\mathbb{R}\backslash\{0\}$, or $\mathbb{R}^*$.

Example 1.6: Direct Product

Let G and H be groups. Their **direct product** is the set $G \times H$ with the component-wise operation defined as

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

One can check that $G \times H$ is a group with the identity (e_G, e_H) and the inverse $(g, h)^{-1} = (g^{-1}, h^{-1})$. Similarly, one can show that if $G_1, \ldots, G_n$ are all groups, then $G_1 \times \cdots \times G_n$ is also a group.

Definition 1.9: Notation for Groups

Given a group G and $g_1, g_2 \in G$, we often denote $g_1 * g_2$ by $g_1 g_2$ and its identity by 1. Also, the unique inverse of an element g is denoted by g^{-1}. Moreover, for $n \in \mathbb{N}$, we define

$$g^n = \underbrace{g \times \cdots \times g}_{n \text{ times}} \quad \text{and} \quad g^{-n} = (g^{-1})^n$$

Finally, we denote $g^0 = 1$.

Proposition 1.2

Let G be a group and $g, h \in G$. We have

1. $(g^{-1})^{-1} = g$;
2. $(gh)^{-1} = h^{-1}g^{-1}$;
3. $g^n g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$;
4. $(g^n)^m = g^{nm}$ for all $n, m \in \mathbb{Z}$

Proof. 1. Since we have $g^{-1}g = 1 = gg^{-1}$, we have $(g^{-1})^{-1} = g$;

2. We have

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = g1g^{-1} = gg^{-1} = 1$$

The other direction is essentially the same. Thus we have $(gh)^{-1} = h^{-1}g^{-1}$.

Exercise: (3), (4) can be proved by induction and the definition of g^{-n}.

□

Discovery 1.2

In general, it is not true that if $g, h \in G$, then $(gh)^n = g^n h^n$. For example,

$$(gh)^2 = ghgh \neq gghh = g^2h^2$$

Equality would hold if the group G is abelian.

Proposition 1.3: Cancellation

Let G be a group and $g, h, f \in G$. then

1. They satisfy the left and the right cancellation. More precisely,
   (a) If $gh = gf$, then $h = f$;
   (b) If $hg = fg$, then $h = f$.
2. Given $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions for x and y in G.

Proof. To prove statement (1), we simply multiply each equation with g^{-1} from either left or right hand side. Similar argument also applies to (2) where uniqueness follows directly from (1). $x = a^{-1}b$ and $y = ba^{-1}$. □

1.3 Symmetric Group

Definition 1.10: Bijection

Let $f : X \to Y$ be a function, we say that f is **one-to-one** if $f(x_1) = f(x_2)$ implies $x_1 = x_2$. We say f is **onto** if for all $y \in Y$, there exists $x \in X$ such that $f(x) = y$. If a function satisfies both conditions, then we say that f is a **bijection**.

Definition 1.11: Permutation

Given a non-empty group set L, a **permutation** of L is a bijection from L to L. The set of all permutations of L is denoted by S_L.

Example 1.7

Consider the set $L = \{1, 2, 3\}$, which has the following six different permutations:

$$S_L = \{123, 132, 213, 231, 312, 321\}$$

where, as an example, 132 is the bijection $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ with $\sigma(1) = 1$, $\sigma(2) = 3$, and $\sigma(3) = 2$.

Comment 1.1

For $n \in \mathbb{N}$, we use $S_n = S_{\{1,\ldots,n\}}$, the set of all permutations of $\{1, \ldots, n\}$.

Discovery 1.3: $|S_n| = n!$

Considering the order of S_n, we notice that $|S_n| = n!$.

Lecture 3 - Monday, September 09

Given $\sigma, \tau \in S_n$, we can compose them to get a third element $\sigma\tau$, where

$$\sigma\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

given by

$$x \mapsto \sigma(\tau(x)) \qquad \forall\, x \in \{1, \ldots, n\}$$

Since both σ and τ are bijections, so is $\sigma\tau$, thus $\sigma\tau \in S_n$.

Example 1.8

Compute $\sigma\tau$ and $\tau\sigma$ if

$$\sigma = 3412 \qquad \text{and} \qquad \tau = 2431$$

Solution: Note that $\sigma\tau(1) = \sigma(\tau(1)) = \sigma(2) = 4$. Compute the rest in the same way, we have

$$\sigma\tau = 4213 \qquad \text{and} \qquad \tau\sigma = 3124$$

Discovery 1.4

Note that $\sigma\tau \neq \tau\sigma$. Note that for $\sigma, \tau, \mu \in S_n$, we have

$$\sigma\tau, \tau\sigma \in S_n$$

$$\sigma(\tau\mu) = (\sigma\tau)\mu$$

The **identity permutation** $\varepsilon \in S_n$ is defined as

$$\varepsilon = 12\dots n$$

Then for any $\sigma \in S_n$, $\sigma\varepsilon = \sigma = \varepsilon\sigma$. Finally, for $\sigma \in S_n$, since it is a bijction, there exists a unique bijection $\sigma^{-1} \in S_n$, called the **inverse permutation** of σ, such that for all $x, y \in \{1, \dots, n\}$

$$\sigma^{-1}(x) = y \iff \sigma(y) = x$$

Thus $\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma$.

Example 1.9

Find the inverse of

$$\sigma = 45123$$

Solution: We see that $\sigma(1) = 4$, thus $\sigma^{-1}(4) = 1$. Using the same method, we have

$$\sigma^{-1} = 34512$$

From the above discussion, we have

Proposition 1.4: Symmetric Group

S_n is a group, it is called the **symmetirc group of order** n .

Exercise: Write down all rotations and reflections that fix a equilateral triangle. Then check why it is the same as S_3.

Consider $\sigma = 3176942581\underline{0} \in S_{10}$. If we represent the action of σ "geometrically", we obtain

$$1 \to 3 \to 7 \to 2 \to 1 \qquad 4 \to 6 \to 4 \qquad 5 \to 9 \to 8 \to 5 \qquad 10 \to 10$$

Thus σ can be **decomposed** into one 4-cycle (1372), one 2-cycle (46), one 3-cycle (598), and one 1-cycle (10). (We usually do not write 1-cycle).

Notice that these cycles are **paiewise disjoint** and we have

$$\sigma = (1372)(46)(598)$$

Note that we can also write

$$\sigma = (46)(598)(7213)$$

Discovery 1.5: Bonus 1

Although the decomposition of cycle notation is not unique, the individual cycle is unique. One can prove the following theorem.

Theorem 1.1: Cycle Decomposition Theorem

If $\sigma \in S_n$, with $\sigma \neq \varepsilon$, then σ is a product of (one or more) disjoint cycles of length at least 2. This factorization is unique up to the order of the factors.

Comment 1.2

Every permutation in S_n can be regarded as a permutation in S_{n+1} by fix the number $(n+1)$. Thus we have the chain

$$S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n \subseteq S_{n+1} \subseteq \cdots$$

1.4 Cayley Tables

Definition 1.12: Cayley Table

For all finite group G, define its operation by means of a table is sometimes convenient. Given $x, y \in G$, the product xy is the entry of the table in the row corresponding to x and the column corresponding to y. This table is called the **Cayley Table**.

Discovery 1.6

By cancellation (1.3), the entries in each row (or in each column) of the Cayley Table are all distinct,

Example 1.10

Consider the group $(\mathbb{Z}_2, +)$, its Cayley Table is

$\mathbb{Z}_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Example 1.11

Consider the group $\mathbb{Z}^* = \{1, -1\}$, its Cayley Table is

$\mathbb{Z}_2$	1	-1
1	1	-1
-1	-1	1

Discovery 1.7

Notice that if we replace 1 by [0] and -1 by [0], the Cayley Tables of $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are the same. In this case, we say that $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are **isomorphic** denoted by $\mathbb{Z}^* \cong \mathbb{Z}_2$.

Example 1.12: Cyclic Group of Order n

For $n \in \mathbb{N}$, the **cyclic group of order** n is defined by

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\}$$

with $a^n = 1$ and all elements are distinct. We write $C_n = \langle a : a^n = 1 \rangle$ and call a a **generator** of C_n. The Cayley Table of C_n is

C_n	1	a^1	a^2	$\cdots$	a^{n-1}
1	1	a^1	a^2	$\cdots$	a^{n-1}
a^1	a^1	a^2	a^3	$\cdots$	1
a^2	a^2	a^3	a^4	$\cdots$	a^1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a^{n-1}	a^{n-1}	1	a^1	$\cdots$	a^{n-2}

Proposition 1.5

Let G be a group up to isomorphism, we have

1. If $|G| = 1$, then $G = \{1\}$;
2. If $|G| = 2$, then $G \cong C_2$;
3. If $|G| = 3$, then $G \cong C_3$;
4. If $|G| = 4$, then $G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$. ($K_4$ is called the Klein 4-group).

Proof. If $|G| = 2$, then $G = \{1, g\}$ with $g \neq 1$. Then $g^2 = g$ or $g^2 = 1$. We note that if $g^2 = g$, then by cancellation we obtain $g = 1$, thus we must have $g^2 = 1$. Hence the Cayley Table of G is the following

G	1	g
1	1	g
g	g	1

which is the same as C_2.

Lecture 4 - Wednesday, September 11

If $|G| = 3$, then $G = \{1, g, h\}$ with $g \neq 1$, $h \neq 1$, and $g \neq h$. Note that $gh \neq g$ or h because otherwise we would have $h = 1$ or $g = 1$ by cancellation. Thus the only choice for gh is 1. Similarly, we also have $hg = 1$. Therefore, we can now fill out the Cayley Table:

G	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

also

C_3	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

By replacing g with a and h with a^2, we see that $G \cong C_3$. To prove statement (4), see hw1. □

Exercise: Consider the symmetry group of a non-square rectangle. How is it related to K_4?

2 Subgroup

Definition 2.1: Subgroup

Let G be a group and $H \subseteq G$ be a subset of G. If H itself is a group, then we say that H is a subgroup of G.

Discovery 2.1

Note that since G is a group, for $h_1, h_2, h_3 \in H \subseteq G$, we have

$$h_1(h_2h_3) = (h_1h_2)h_3$$

thus H is a subgroup of G if it satisfies the following conditions:

Algorithm 2.1: Subgroup Test

1. If $h_1, h_2 \in H$, then $h_1h_2 \in H$;
2. There exists $1_H \in H$ such that $1_Hh = h1_H$ for all $h \in H$;
3. If $h \in H$, then $h^{-1} \in H$.

Exercise: Prove that $1_H = 1_G$.

Example 2.1

Given a group G, $\{1\}$ and G are subgroups of G.

Example 2.2

We have a chain of subgroups:

$$(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$$

Example 2.3

Recall $GL_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) : \det(M) \neq 0\}$. Define $SL_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) : \det(M) = 1\}$. It is clear that we have

$$SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$$

We now wish to check if $SL_n(\mathbb{R})$ is a group. We obviously have the identity matrix exists in $SL_n(\mathbb{R})$, also notice that for $A, B \in SL_n(\mathbb{R})$,

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1 \quad \Rightarrow \quad AB \in SL_n(\mathbb{R})$$

Moreover

$$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1 \quad \Rightarrow \quad A^{-1} \in SL_n(\mathbb{R})$$

Definition 2.2: Special Linear Group

For the group $SL_n(\mathbb{R})$ we've shown above, we name it the **special linear group of order n over $\mathbb{R}$**.

Example 2.4: The centre of G is an abelian subgroup of G

Given a group, we define the **center** of G to be

$$Z(G) = \{z \in G : zg = gz \ \ \forall\, g \in G\}$$

Note that $Z(G) = G$ if and only if G is abelian. Here we will show that $Z(G)$ is an abelian subgroup of G. Easy to note that $1 \in Z(G)$. Let $y, z \in Z(G)$, then for all $g \in G$, we have

$$(yz)g = y(zg) = y(gz) = (yg)z = gyz = g(yz)$$

Now it suffices for us to prove the existence of inverses. For $z \in Z(G)$ and $g \in G$, we have

$$zg = gz \quad \Rightarrow \quad z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1} \quad \Rightarrow \quad gz^{-1} = z^{-1}g$$

Done.

Proposition 2.1

Let H and K be subgroups of a group G, then the intersection

$$H \cap K = \{g \in G : g \in H \wedge g \in K\}$$

is also a subgroup of G.

Proof. **Exercise**. □

Proposition 2.2: Finite Subgroup Test

If H is a finite non-empty subset of a group G, then H is a subgroup of G if and only if H is closed under its operation.

Proof. The forward direction is clear. For the other direction, for $H \neq \varnothing$, let $h \in H$. Since H is closed under its operation, we have

$$h^1, h^2, h^3, \ldots \in H$$

Since H is finite, these elements are not all distinct. Thus

$$h^n = h^{n+m} \quad \text{for some } m, n \in \mathbb{N}$$

By cancellation, $h^m = 1 \in H$. Also $1 = h^{m-1}h$ implies that $h^{-1} = h^{m-1}$, thus $h^{-1} \in H$. By the subgroup test, we conclude that H is a subgroup of G. □

2.1 Alternating Groups

Recall that for $\sigma \in S_n$ with $\sigma \neq \varepsilon$, σ can be decomposed uniquely (up to the order) as disjoint cycles of length at least 2.

Definition 2.3: Transposition

A **transposition** $\sigma \in S_n$ is a cycle of length 2. i.e., $\sigma = (a, b)$ with $a, b \in \{1, \ldots, n\}$ and $a \neq b$.

Lecture 5 - Friday, September 13

Example 2.5

Consider the permutation $(1, 2, 4, 5) \in S_5$. Also, the composition $(12)(24)(45)$ can be computed as

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

Thus we have $(1245) = (12)(24)(45)$. Moreover, we can also show that (as an example):

$$(1245) = (23)(12)(25)(13)(24)$$

We see from the example that the factorization into transpositions are NOT unique. However, one can prove the following theorem:

Theorem 2.1: Parity Theorem

If a permutation σ has two factorizations

$$\sigma = \gamma_1 \dots \gamma_r = \mu_1 \dots \mu_s$$

where each γ_i and μ_j is transposition, then

$$r \equiv s \pmod 2$$

Proof. See Bonus 2. □

Definition 2.4: Even/ Odd Permutation

A permutation σ is **even** (or **odd**) if it can be written as a product of an even (or odd) number of transpositions.

Theorem 2.2

For $n \geq 2$, let A_n denote the set of all even permutations in S_n, then

1. $\varepsilon \in A_n$;
2. If $\sigma, \tau \in A_n$, then $\sigma\tau \in A_n$ and $\sigma^{-1} \in A_n$;
3. $|A_n| = \dfrac{1}{2} \cdot n!$.

Definition 2.5: Alternating Group

From (1) and (2), we see that A_n is in fact a subgroup of S_n, we call A_n the **alternating group of degree** n.

Proof. We can write $\varepsilon = (12)(21)$, thus ε is even. If $\sigma, \tau \in A_n$, we can write $\sigma = \sigma_1 \cdots \sigma_r$ and $\tau = \tau_1 \cdots \tau_s$, where σ_i and τ_j are transpositions and r, s are even numbers. Then

$$\sigma\tau = \sigma_1 \cdots \sigma_r \tau_1 \cdots \tau_s$$

which is a product of $(r + s)$ transpositions and thus $\sigma\tau \in A_n$. Moreover, we note that since σ_i is a transposition, so we have $\sigma_i^2 = \varepsilon$ and thus $\sigma^{-1} = \sigma$. It follows that

$$\sigma^{-1} = (\sigma_1 \cdots \sigma_r)^{-1} = \sigma_r^{-1} \cdots \sigma_1^{-1} = \sigma_r \cdots \sigma_1$$

which is an even permutation. To prove (3), let O_n denote the set of all odd permutations in S_n. Thus $S_n = A_n \sqcup O_n$ and the parity theorem implies that

$$A_n \cap O_n = \varnothing$$

Since $|S_n| = n!$, to prove $|A_n| = \frac{1}{2} \cdot n!$, it suffices to prove that $|A_n| = |O_n|$. Let $\gamma = (1, 2)$ and define $f : A_n \to O_n$ be denoted by $f(\sigma) = \gamma\sigma$. Since σ is even, we have $\gamma\sigma$ is odd. Thus the map is well-defined. Also, if we have $\gamma\sigma_1 = \gamma\sigma_2$, then by cancellation, we have $\sigma_1 = \sigma_2$. Thus f is one-to-one. Finally, if we have $\tau \in O_n$, then $\sigma = \gamma\tau \in A_n$ and

$$f(\sigma) = \gamma\tau = \gamma(\gamma\tau) = \gamma^2\tau = \tau$$

It follows that f is onto, thus bijective. We may now conclude that $|A_n| = |O_n|$. □

2.2 Order of Elements

Definition 2.6:

If G is a group and $g \in G$, we denote

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

Note that $1 = g^0 \in \langle g \rangle$. Also, if $x = g^m$, $y = g^n \in \langle g \rangle$ for $m, n \in \mathbb{Z}$, then $xy = g^{m+n} \in \langle g \rangle$ and $x^{-1} = g^{-m} \in \langle g \rangle$. By the subgroup test, we have

Proposition 2.3

If G is a group and $g \in G$, then $\langle g \rangle$ is a subgroup of G.

Definition 2.7: Cyclic Subgroup

Let G be a group and $g \in G$, we call $\langle g \rangle$ the **cyclic subgroup of G generated by** g. If $G = \langle g \rangle$ for some $g \in G$, then we say G is a **cyclic group** and g is a **generator** of G.

Example 2.6

Consider $(\mathbb{Z}, +)$. Note that we have

$$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$

Observe that for any $n \in \mathbb{Z} \backslash \{1, -1\}$, there exists no $k \in \mathbb{Z}$ such that $n \cdot k = 1$. Thus ± 1 are the only generator of $(\mathbb{Z}, +)$.

Let G be a group and $g \in G$. Suppose that there exists $k \in \mathbb{Z}$ with $k \neq 0$ such that $g^k = 1$, then $g^{-k} = (g^k)^{-1} = 1$. Thus we can assume that $k \geq 1$, then by the well-ordering principle, there exists the "smallest" positive integer n such that $g^n = 1$.

Definition 2.8: Order

Let G be a group and $g \in G$. If n is the smallest positive integer such that $g^n = 1$, then we say that n is the **order** of g. We denote this as

$$o(g) = n$$

If no such n can be found, then we say the element has **infinite order**, and we write $o(g) = \infty$.

Proposition 2.4

Let G be a group and $g \in G$ satisfying $o(g) = n \in \mathbb{N}$. For $k \in \mathbb{Z}$, we have

1. $g^k = 1$ if and only if $n \mid k$;
2. $g^k = g^m$ if and only if $k \equiv m \pmod{n}$;
3. $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ where $1, g, \ldots, g^{n-1}$ are all distinct. In particular, $|\langle g \rangle| = o(g)$.

Lecture 6 - Monday, September 16

Proof. 1. If $n|k$, then $k = nq$ for some $q \in \mathbb{Z}$, thus

$$g^k = g^{nq} = (g^n)^q = 1^q = 1$$

By the division algorithm, we may write $k = nq + r$ for $q, r \in \mathbb{Z}$ with $0 \leq r < n$. Since $g^k = 1$ and $g^n = 1$, we have

$$g^r = g^{k-nq} = g^k \cdot (g^n)^{-q} = 1 \cdot 1^{-q} = 1$$

Since $0 \leq r < n$, and $o(g) = n$, it follows that $r = 0$ and hence $n = nq$ yields us $n|k$.

2. Note that $g^k = g^n$ if and only if $g^{k-m} = 1$, we have $n \mid (k - m)$, i.e., $k \equiv m \pmod{n}$.

3. If follows from (2) that $1, g, \ldots, g^{n-1}$ are all disticnt. Clearly, we have $\{1, g, \ldots, g^{n-1}\} \subseteq \langle g \rangle$. To prove the other direction of inclusion, let $x = g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. Write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$, then

$$x = g^k = g^{nq} \cdot g^r = q^1 \cdot g^r = g^r \in \{1, g, \ldots, g^{n-1}\}$$

□

Proposition 2.5

Let G be a group and $g \in G$ with $o(g) = \infty$, given $k \in \mathbb{Z}$, then we have

1. $g^k = 1$ if and only if $k = 0$;
2. $g^k = g^m$ if and only if $k = m$;
3. $\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}$ are all distinct.

Proof. It is easy to see that (2) and (3) follow directly from (1). If $g^k = 1$ for some $k \neq 0$, then $g^{-k} = (g^k)^{-1} = 1$, thus we may assume without loss of generality that $k \geq 1$. However, it implies that $o(g)$ is finite, which contradicts the infinitude of the order of g, thus $k = 0$. Conversely, we simply have $g^0 = 1$. □

Proposition 2.6

Let G be a group and $g \in G$ with $o(g) = n \in \mathbb{N}$. If $g \in \mathbb{N}$, then

$$o(g^d) = \frac{n}{\gcd(n, d)}$$

Proof. For simplicity, we introduce

$$n_1 := \frac{n}{\gcd(n, d)} \qquad \text{and} \qquad d_1 := \frac{d}{\gcd(n, d)}$$

It is easy to observe that $\gcd(n_1, d_1) = 1$. Note that

$$(g^d)^{n_1} = (g^n)^{d_1} = 1$$

Thus it suffices to show that n_1 is the smallest such positive integer. Suppose $(g^d)^r = 1$ for some $r \in \mathbb{N}$, then $g^{dr} = 1$. Thus there exists $q \in \mathbb{Z}$ such that $dr = nq$. Dividing both sides by $\gcd(n, d)$, we get

$$d_1 r = \frac{d}{\gcd(n, d)} r = \frac{n}{\gcd(n, d)} q = n_1 q$$

Since $n_1 \mid d_1 r$ and $\gcd(n_1, d_1) = 1$, we get $n_1 \mid r$, i.e., $n_1 = r\ell$ for some $\ell \in \mathbb{Z}$. Since $n_1, r \in \mathbb{N}$, it follows that $\ell \in \mathbb{N}$. Since $\ell \geq 1$, we get $r \geq n_1$. □

2.3 Cyclic Groups

We recall that for a group G, if $G = \langle g \rangle$ for some $g \in G$, then G is called a cyclic group. For $a, b \in G$, we have $a = g^m$ and g^n for some $m, n \in \mathbb{Z}$. Hence

$$ab = g^m \cdot g^n = g^{m+n} = g^n \cdot g^m = ba$$

Proposition 2.7: Every cyclic group is abelian

Every cyclic group is abelian.

Discovery 2.2

The converse of the above proposition does not hold, as an counterexample, consider the Klein 4-group. $K_4 \cong C_2 \times C_2$ is abelian, but it is indeed not cyclic because all the elements has order of either 1 or 2.

Proposition 2.8

Every subgroup of a cyclic group is cyclic.

Lecture 7 - Wednesday, September 18

Proof. Let $G = \langle g \rangle$ be cyclic and H be a subgroup of G. If $H = \{1\}$, then $H = \langle 1 \rangle$ is cyclic. If $H \neq \{1\}$, then there exists $g^k \in H$ with $k \in \mathbb{Z}$ and $k \neq 0$. Since H is a group, we have $g^{-k} \in H$. Thus we can assume that $k \in \mathbb{N}$. Let m be the smallest positive integer such that $g^m \in H$.
`Claim:` $H = \langle g^m \rangle$. It is easy to observe that $\langle g^m \rangle \subseteq H$. To prove the other inclusion, note that for any $h \in H \subseteq G = \langle g \rangle$, we can write $h = g^k$ for $k \in \mathbb{Z}$. By division algorithm, we have $k = qm + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Thus we may write $g^r = g^{k-mq} = g^k(g^m)^{-q} \in H$. If $r \neq 0$, this contradicts the minimality of m, thus we must have $r = 0$, or $m \mid k$ and we have $g^k \in \langle g^m \rangle$. If follows that $H = \langle g^m \rangle$. □

Proposition 2.9

Let $G = \langle g \rangle$ be cyclic with $o(g) = n \in \mathbb{N}$, then $G = \langle g^k \rangle$ if and only if $\gcd(k, n) = 1$.

Proof. Recall that we have

$$o(g^k) = \frac{n}{\gcd(n, k)}$$

which completes the proof. □

Theorem 2.3: Fundamental Theorem of Finite Cyclic Group

Let $G = \langle g \rangle$ be a cyclic group with $o(g) = n \in \mathbb{N}$, then

1. If H is a subgroup of G, then $H = \langle g^d \rangle$ for some $d \mid n$. If follows that $|H| \mid |G|$.
2. Conversely, if $k \mid n$, then $\langle g^{n/k} \rangle$ is the unique subgroup of G of order k.

Proof. We know that H is cyclic from the above proposition, say $H = \langle g^m \rangle$ for some $m \in \mathbb{N} \cup \{0\}$. Let $d = \gcd(n, m)$.
`Claim:` $H = \langle g^d \rangle$. Since $d \mid m$, we may write $m = dk$ for some $k \in \mathbb{Z}$. Then $g^m = g^{dk} = (g^d)^k \in \langle g^d \rangle$. Thus $H = \langle g^m \rangle \subseteq \langle g^d \rangle$. On the other hand, since $d = \gcd(m, n)$, so there exists $x, y \in \mathbb{Z}$ such that $d = mx + ny$, it follows that $g^d = g^{mx+ny} = (g^m)^x(g^n)^y = (g^m)^x 1 \in \langle g^m \rangle$. Therefore, we also have $\langle g^d \rangle \subseteq \langle g^m \rangle$. Now we may conclude that $H = \langle g^m \rangle = \langle g^d \rangle$. Note that since $d = \gcd(m, n)$, thus $d \mid n$. Also, recall that we have

$$|H| = o(g^d) = \frac{n}{\gcd(d, n)} = \frac{n}{d} \quad \Rightarrow \quad |H| \mid |G|$$

For the second statement, we know that the cyclic group $\langle g^{n/k} \rangle$ is of order

$$\frac{n}{\gcd(n, n/k)} = k$$

To show uniqueness, let K be a subgroup of G which is of order k with $k \mid n$. By (1), let $K = \langle g^d \rangle$ with $d \mid n$. Then

$$k = |K| = \frac{n}{\gcd(n, d)} = \frac{n}{d}$$

It follows that $d = n/k$ and thus $K = \langle g^{n/k} \rangle$. □

Discovery 2.3

The above theorem shows that there is a one to one correspondance between the set of positive divisors of n and all subgroups of a cyclic group of order n.

2.4 Non-Cyclic Groups

Definition 2.9:

Let X be a non-empty subset of a group G and let $\langle X \rangle$ be defined as

$$\langle X \rangle = \{x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} : x_i \in X, k_i \in \mathbb{Z}, m \geq 1\}$$

which denotes the set of all products of powers of (not necessarily) distinct elements of X.

Discovery 2.4: Subgroup of G generated by X

Note that if $x_1^{k_1} \cdots x_m^{k_m} \in \langle X \rangle$ and $\tilde{x_1}^{r_1} \cdots \tilde{x_n}^{r_n} \in \langle X \rangle$, then

$$x_1^{k_1} \cdots x_m^{k_m} \tilde{x_1}^{r_1} \cdots \tilde{x_n}^{r_n} \in \langle X \rangle$$

Also ${x_1}^0 \in \langle X \rangle$ and $(x_1^{k_1} \cdots x_m^{k_m})^{-1} = x_m^{-k_m} \cdots x_1^{-k_1} \in \langle X \rangle$. Hence $\langle X \rangle$ is a subgroup of G, containing X, called the **subgroup of G generated by X**.

Example 2.7

The Klein 4 group $K_4 = \{1, a, b, c\}$ where $a^2 = b^2 = c^2 = 1$ and $ab = c$ (or $ac = b$ or $bc = a$). Thus

$$K_4 = \langle a, b : a^2 = 1 = b^2 \text{ and } ab = ba \rangle$$

We can also replace a, b by a, c or b, c.

Example 2.8

The symmetric group of degree 3. $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ where $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau = \tau\sigma^2$ (one can take $\sigma = (123)$ and $\tau = (12)$). Thus

$$S_3 = \langle \sigma, \tau : \sigma^3 = \varepsilon = \tau^2 \text{ and } \sigma\tau = \tau\sigma^2 \rangle$$

We can also replace σ, τ by $\sigma, \tau\sigma$ or $\sigma, \tau\sigma^2$ and etc.

Definition 2.10: Dihedral Group

For $n \geq 2$, the **dihedral group of order** $2n$ is defined by

$$D_{2n} = \{1, a, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\}$$

where $a^n = 1 = b^2$ and $aba = b$. Thus

$$D_{2n} = \langle a, b : a^n = 1 = b^2 \text{ and } aba = b \rangle$$

Discovery 2.5

Note that when $n = 2$ or 3, we have

$$D_4 \cong K_4 \qquad \text{and} \qquad D_6 = S_3$$

Exercise: For $n \geq 3$, consider a regular n-group and its group of symmetries. How does it relate to D_{2n}?
Hint: consider all possible rotations and reflections.

3 Normal Subgroups

3.1 Homomorphisms and Isomorphisms

Definition 3.1: Homomorphism

Let G and H be groups. A mapping $\alpha : G \to H$ is called a **homomorphism** if

$$\alpha(a *_G b) = \alpha(a) *_H \alpha(b) \qquad \forall\, a, b \in G$$

To simplify notation, we often write

$$\alpha(ab) = \alpha(a)\alpha(b)$$

Example 3.1

Consider the determinant map

$$\det : (GL_n(\mathbb{R}), \cdot) \to \mathbb{R}^* \qquad \text{given by} \qquad A \mapsto \det(A)$$

Since $\det(AB) = \det(A)\det(B)$, the mapping is a group homomorphism.

Proposition 3.1

Let $\alpha : G \to H$ be a group homomorphism, then

1. $\alpha(1_G) = 1_H$;
2. $\alpha(g^{-1}) = \alpha(g)^{-1}$, for all $g \in G$;
3. $\alpha(g^k) = \alpha(g)^k$, for all $g \in G$;

Proof. **Exercise**. □

Definition 3.2: Isomorphism

Let G and H be groups. Consider a mapping $\alpha : G \to H$. If α is a homomorphism and is bijective, then we say α is an **isomorphism**. In this case, we say G and H are **isomorphic** and denoted as $G \cong H$.

Proposition 3.2

We have the following:

1. The identity map $G \to G$ is an isomorphism;
2. If $\sigma : G \to H$ is an isomorphism, then the inverse $\sigma^{-1} : H \to G$ is also an isomorphism;

3. If $\sigma : G \to H$ and $\tau : H \to K$ are isomorphisms, then the composite map $\tau \circ \sigma : G \to K$ is also an isomorphism.

Proof. **Exercise**. □

Discovery 3.1

We see that $\cong$ is an equivalence relation.

Example 3.2

Let $\mathbb{R}^+ = \{r \in \mathbb{R} : r > 0\}$. Our claim is that

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$$

Proof. Define

$$\sigma : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot) \quad \text{by } \sigma(r) = e^r$$

where e is the exponential function. Note that the exponential map from $\mathbb{R}$ to $\mathbb{R}^+$ is bijective. Also, for $r, s \in \mathbb{R}$, we have

$$\sigma(r + s) = e^{r+s} = e^r \cdot e^s = \sigma(r)\sigma(s)$$

It is clear to see that σ is a homomorphism, and it follows that σ is an isomorphism as desired. □

Example 3.3

We have $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}^*, \cdot)$.

Proof. Suppose that $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ is an isomorphism. Then τ is onto. Thus there exists $q \in \mathbb{Q}$ such that $\tau(q) = 2$. Write $\tau(q/2) = a \in \mathbb{Q}^*$, thus we have

$$a^2 = \tau(q/2)\tau(q/2) = \tau(q/2 + q/2) = \tau(q) = 2$$

which yields a contradiction (a is in fact irrational). □

3.2 Cosets and Lagrange Theorem

Definition 3.3: Coset

Let H be a subgroup of a group G. If $a \in G$, we define

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

to be the **right coset of H genereted by** a. Similarly, define the **left coset of H genereted by** a:

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

Discovery 3.2

Since $1 \in H$, so we have $H1 = H = 1H$ and $a \in Ha$ and $a \in aH$. Note that in general, Ha and aH are not subgroups of G and $Ha \neq aH$. However, if G is abelian, then $Ha \cong aH$.

Example 3.4

Let $K_4 = \{1, a, b, ab\}$ with $a^2 = 1 = b^2$ and $ab = ba$. Let $H = \{1, a\}$ which is a subgroup of K_4. Note that since K_4 is abelian, we have

$$gH = Hg$$

for any $g \in K_4$. Then the right (or left) cosets of H are

$$H1 = \{1, a\} = Ha \qquad \text{and} \qquad Hb = \{b, ab\} = Hab$$

Thus, there are exactly two cosets of H in K_4.

Example 3.5

Let $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ with $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau = \tau\sigma^2$. Let $H = \{\varepsilon, \tau\}$ be the subgroup of S_3. Since $\sigma\tau = \tau\sigma^2$, the right coset of H are

$$H\varepsilon = \{\varepsilon, \tau\} = H\tau \qquad H\sigma = \{\sigma, \tau\sigma\} = H\tau\sigma \qquad H\sigma^2 = \{\sigma^2, \tau\sigma^2\} = H\tau\sigma^2$$

Also, the left cosets of H are

$$\varepsilon H = \{\varepsilon, \tau\} = \tau H \qquad \sigma H = \{\sigma, \tau\sigma^2\} = \tau\sigma^2 H \qquad \sigma^2 H = \{\sigma^2, \tau\sigma\} = \tau\sigma H$$

Note that $H\sigma \neq \sigma H$ and $H\sigma^2 \neq \sigma^2 H$.

Proposition 3.3

Let H be a subgroup of a group G and let $a, b \in G$,

1. $Ha = Hb$ if and only if $ab^{-1} \in H$. In particular, we have $Ha = H$ if and only if $a \in H$ (taking $b = 1$);
2. If $a \in Hb$, then $Ha = Hb$;
3. Either $Ha = Hb$ or $Ha \cap Hb = \varnothing$. Thus, the distinct right cosets of H forms partition of G.

Proof. 1. If $Ha = Hb$, then $a = 1a \in Ha = Hb$. Thus $a = hb$ for some $h \in H$ and we have $ab^{-1} = h \in H$;
Conversely, suppose $ab^{-1} \in H$, then for all $h \in H$,

$$ha = ha(b^{-1}b) = h(ab^{-1})b \in Hb$$

Thus $Ha \subseteq Hb$. Note that if $ab^{-1} \in H$, since H is a subgroup, then $(ab^{-1})^{-1} = ba^{-1} \in H$. Then for all $h \in H$,

$$hb = hba^{-1}a = h(ba^{-1})a \in Ha$$

Thus $Hb \subseteq Ha$. It follows that $Ha = Hb$.

2. If $a \in Hb$, then $ab^{-1} \in H$, thus by (1), $Ha = Hb$.

3. If $Ha \cap Hb = \varnothing$, then we are done. Otherwise, if $Ha \cap Hb \neq \varnothing$, then there exists $x \in Ha \cap Hb$. Since $x \in Ha$, by (2), we have $Ha = Hx$. Since $x \in Hb$, by (2), we have $Hb = Hx$. Thus we must have $Ha = Hb$.

□

Lecture 9 - Monday, September 23

Discovery 3.3

The analogous of the above proposition also hold for left cosets for (1), in particular, we have $aH = bH$ if and only if $b^{-1}a \in H$.

Exercise: Let G be a group and H a subset of G. For $a, b \in G$, do we still have "$Ha = Hb$ or $Ha \cap Hb = \varnothing$".

Definition 3.4: Index

Following the above proposition, we see that G can be written as a disjoint union of right cosets of H, we define the **index** $[G : H]$ to be the number of right (or left) cosets of H in G.

3.3 Lagrange Theorem

Theorem 3.1: Lagrange Theorem

Let H be a subgroup of a finite group G, we have $|H| \mid |G|$, and

$$[G : H] = \frac{|G|}{|H|}$$

Proof. Write $k = [G : H]$ and let $Ha_1, Ha_2, \ldots, Ha_k$ be the distinct right cosets of H in G. Therefore have

$$G = Ha_1 \sqcup Ha_2 \sqcup \cdots \sqcup Ha_k$$

Since $|Ha_i| = |H|$ for each i, we have

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_k| = k|H|$$

It follows that $|H| \mid |G|$ and $[G : H] = k = |G|/|H|$. □

Corollary 3.1

1. If G is a finite group and $g \in G$, then $o(g) \mid |G|$;
2. If G is a finite group with $|G| = n$, then for all $g \in G$, we have $g^n = 1$.

Proof. [1] Take $H = \langle g \rangle$, then we have $|H| = o(g)$.
[2] Let $o(g) = m$, then by [1], we have $m \mid n$. Thus $g^n = (g^m)^{n/m} = 1^{n/m} = 1$. □

3.4 Euler's Theorem and Fermat's Little Theorem

Example 3.6

For $n \in \mathbb{N}$ with $n \geq 2$, let $\mathbb{Z}_n^*$ be the set of (multiplicative) invertible elements in $\mathbb{Z}_n$. Let the **Euler φ-function**, $\varphi(n)$, denote the order of $\mathbb{Z}_n^*$. i.e.,

$$\varphi(n) = \left| \{[k] \in \mathbb{Z}_n : k \in \{0, \ldots, n-1\} \wedge \gcd(k, n) = 1\} \right|$$

As a direct consequence of the Corollary, we see that if $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. This is **Euler's theorem**. If $n = p$ for some prime number p, then Euler's Theorem implies that $a^{p-1} \equiv 1 \pmod{p}$, which is known as the **Fermat's Little Theorem**.

We recall by constructing their Cayler Table, we show that $G \cong C_2$ if $|G| = 2$ and $G \cong C_3$ if $|G| = 3$.

Corollary 3.2

If G is a group with $|G| = p$ where p is prime, then $G \cong C_p$, the cyclic group of order p.

Proof. Let $g \in G$ with $g \neq 1$, then we have $o(g) \mid p$. Since $g \neq 1$ and p is a prime, so $o(g) = p$. Therefore we have

$$|\langle g \rangle| = o(g) = p \quad \Rightarrow \quad G = \langle g \rangle \cong C_p$$

□

Corollary 3.3

Let H and K be finite subgroups of a group G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

Proof. We know that $H \cap K$ is a subgroup of H and K. By Lagrange Theorem, we have $|H \cap K| \mid H$ and $|H \cap K| \mid |K|$. It follows that $|H \cap K| = 1$, thus $H \cap K = \{1\}$. □

3.5 Normal Subgroups

Let H be a subgroup of a group G and $g \in G$. In general, $gH \neq Hg$.

Definition 3.5: Normal Subgroups

Let H be a subgroup of a group G, if $gH = Hg$ for all $g \in G$, then we say H is **normal** in G, denoted as

$$H \lhd G$$

Example 3.7

Certainly, we have $\{1\} \lhd G$ and $G \lhd G$.

Example 3.8

The centre $Z(G)$ of G, $Z(G) = \{z \in G : zg = gz \quad \forall\ g \in G\}$ is an abelian subgroup of G. By its definition, we have $Z(G) \lhd G$, thus every subgroup of $Z(G)$ is normal in G.

Example 3.9

If G is an abelian group, then every subgroup of G is normal in G. However, the converse if not true. See more on quaternion group Q_8 in A3.

3.5.1 Normality Test

Proposition 3.4: Normality Test

Let H be a subgroup of a group G, TFAE:

1. $H \lhd G$;
2. $gHg^{-1} \subseteq H$ for all $g \in G$;
3. $gHg^{-1} = H$ for all $g \in G$.

Proof. `(1)` $\Rightarrow$ `(2)`: Let $x \in gHg^{-1}$, say $x = ghg^{-1}$ for some $h \in H$. Then by (1), $gh \in gH = Hg$, say $gh = h_1 g$ for some $h_1 \in H$. Then

$$x = ghg^{-1} = h_1 gg^{-1} = h_1 \in H$$

Thus $gHg^{-1} \subseteq H$.
`(2)` $\Rightarrow$ `(3)`: If $g \in G$, then by (2), we have $gHg^{-1} \subseteq H$. Taking g^{-1} in place of g in (2), we get

$$g^{-1}Hg \subseteq H \quad \Rightarrow \quad H \subseteq gHg^{-1} \quad \Rightarrow \quad gHg^{-1} = H$$

`(3)` $\Rightarrow$ `(1)`: If $gHg^{-1} = H$, we simply have $gH = Hg$. □

Lecture 10 - Wednesday, September 25

Example 3.10

Let $G = GL_n(\mathbb{R})$ and $H = SL_n(\mathbb{R})$. For $A \in G$ and $B \in H$, we have

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A)\det(B)\frac{1}{\det(A)} = 1$$

Thus $ABA^{-1} \in H$ and it follows that $AHA^{-1} \subseteq H$ for all $A \in G$. By Normality Test, we have $H \lhd G$. i.e.,

$$SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$$

Proposition 3.5

If H is a subgroup of a group G and $[G : H] = 2$, then $H \lhd G$.

Proof. Let $g \in G$, if $g \in H$, then $Hg = H = gH$. If $g \notin H$, since $[G : H] = 2$, then $G = H \cup Hg$, a disjoint union. Thus $Hg = G\backslash H$. Similarly, if $g \notin H$, we also have $gH = G\backslash H$. Therefore, $Hg = gH$ for all $g \in G$. i.e., $H \lhd G$. □

Example 3.11

Let A_n be the alternating group contained in S_n. Since $[S_n : A_n] = 2$, thus by the above proposition, we have $A_n \lhd S_n$.

Example 3.12

Let $D_{2n} = \langle a, b : a^n = 1 = b^2 \text{ and } aba = b\rangle$ be the dihedral group of order $2n$. Since $[D_{2n} : \langle a\rangle] = 2$, we have $\langle a\rangle \lhd D_{2n}$.

Let H and K be subgroups of group G, the intersection $H \cap K$ is the "largest" subgroup of G contained in H and K. One may consider the "smallest" subgroup containing both H and K. Notice that $H \cup K$ is the "smallest subset" containing H and K. However, we see in HW2 that $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$. A more useful construction tuens out to be the **product** H and K defined as

$$HK = \{hk : h \in H, k \in K\}$$

Still, HK is *not always* a group.

Exercise: Find an example such that HK is not a subgroup.

Lemma 3.1

Let H and K be subgroups of group G, TFAE:

1. HK is a subgroup of G;
2. $HK = KH$;

3. KH is a subgroup of G.

Proof. STP (1) if and only if (2).
`[2]` $\Rightarrow$ `[1]`: We have $1 = 1 \cdot 1 \in HK$. Also, if $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Thus we wish to show closure. For $hk, h_1k_1 \in HK$, we have $kh_1 = h_2k_2$, so

$$hkh_1k_1 = h(kh_1)k_1 = hh_2k_2k_1 \in HK$$

By the subgroup test, we have HK is a subgroup of G.
`[1]` $\Rightarrow$ `[2]`: Let $kh \in KH$ with $k \in K$ and $h \in H$, since H and K are subgroups of G, we have $h^{-1} \in H$ and $k^{-1} \in K$. Since HK is also a subgroup of G, we have

$$kh = (h^{-1}k^{-1})^{-1} \in HK \quad \Rightarrow \quad KH \subseteq HK$$

On the other hand, if $hk \in HK$, since HK is a subgroup of G, we have

$$k^{-1}h^{-1} = (hk)^{-1} \in HK$$

say $k^{-1}h^{-1} = h_1k_1$, thus $hk = k_1^{-1}h_1^{-1} \in KH$, so $HK \subseteq KH$. It follows that $KH = HK$. □

Proposition 3.6

Let H and K be subgroups of a group G,

1. If $H \lhd G$ or $K \lhd G$, then $HK = KH$ is a subgroup of G;
2. If $H \lhd G$ and $K \lhd G$, then $HK \lhd G$

Proof. `[1]`: Suppose $H \lhd G$, then

$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH$$

Thus it follows that $HK = KH$ is a subgroup of G by the above lemma.
`[2]`: If $g \in G$ and $hk \in HK$, since $H \lhd G$ and $K \lhd G$, we have

$$g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK$$

Thus $HK \lhd G$. □

Exercise: Find an example that $HK = KH$ is a subgroup of G, but H and K are not normal in G.

Definition 3.6: Normalizer

Let H be a subgroup of a group G, the **normalizer** of H, denoted by $N_G(H)$, is defined to be

$$N_G(H) = \{g \in G : gH = Hg\}$$

Discovery 3.4

Notice that $H \lhd G$ if and only if $N_G(H) = G$. Also note that in the proof of the above proposition, we do not need the full assumption that $H \lhd G$, we only need $kH = Hk$ of all $k \in K$, i.e., $k \in N_G(H)$.

Corollary 3.4

Let H and K be subgroups of a group G. If $K \subseteq N_G(H)$ (or $H \subseteq N_G(K)$), then $HK = KH$ is a subgroup of G.

Proof. See the above discovery. □

Theorem 3.2

If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $HK = H \times K$.

Lecture 11 - Friday, September 27

Proof. `Claim 1:` If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $hk = kh$ for all $h \in H$ and $k \in K$.
`Proof of claim 1:` Consider

$$x = hk(kh)^{-1} = hkh^{-1}k^{-1}$$

Note that $kh^{-1}k^{-1} \in H$, thus $x = h(kh^{-1}k^{-1}) \in H$. Similarly, since $hkh^{-1} \in K$, we have $x = (hkh^{-1})k^{-1} \in K$. Since $x \in H \cap K = \{1\}$, we have $hkh^{-1}k^{-1} = 1$, which implies that $hk = kh$ as desired.
Since $H \lhd G$, by above proposition, HK is a subgroup of G. Define

$$\sigma : H \times K \to HK$$

by $\sigma((h, k)) = hk$ for all $h \in H$ and $k \in K$.
`Claim 2:` σ is an isomorphism.
`Proof of claim 2:` Let $(h, k), (h_1, k_1) \in H \times K$. By claim 1, we have $h_1k = kh_1$. Thus

$$\begin{aligned}\sigma((h, k) \cdot (h_1, k_1)) = \sigma((hh_1, kk_1)) &= hh_1kk_1 \\ &= hkh_1k_1 \\ &= \sigma((h, k))\sigma((h_1, k_1))\end{aligned}$$

so σ is a homomorphism. Note that by the definition of HK, σ is onto. Also, if $\sigma((h, k)) = \sigma((h_1, k_1))$, we have $hk = h_1k_1$. Thus $h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}$. Thus $h_1^{-1}h = 1 = k_1k^{-1}$, i.e., $h = h_1$ and $k = k_1$. Thus σ is one-to-one and claim 2 holds.
It follows that $HK \cong H \times K$. □

Result 3.1

As a direct consequence of the above theorem, we have:

Corollary 3.5

Let G be a finite group and let $H \lhd G$, $K \lhd G$ with $H \cap K = \{1\}$ and $|H||K| = |G|$, then

$$G \cong H \times K$$

Example 3.13

Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, and let G be a cyclic group of order mn. Write $G = \langle a \rangle$ with $o(a) = mn$. Let $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$. Then $|H| = o(a^n) = m$ and $|K| = o(a^m) = n$. It follows that $|H||K| = |G|$, since $\gcd(m, n) = 1$, we have $H \cap K = \{1\}$. Also, since G is cyclic and thus abelian, we have $H \lhd G$ and $K \lhd G$, so we have

$$G \cong H \times K \qquad \text{i.e. } C_{mn} \cong C_m \times C_n$$

Result 3.2

To consider finite cyclic groups, it suffices to consider cyclic groups with order of prime powers.

4 Isomorphism Theorems

4.1 Quotient Groups

Let G be a group and K be a subgroup of G. It is natural to ask if we could make the set of right cosets of K, $\{Ka : a \in G\}$, into a group. A natural way to define multiplication on this set is:

$$Ka \cdot Kb = Kab \qquad \forall\, a, b \in G \tag{$*$}$$

Note that we could have $Ka = Ka_1$ and $Kb = Kb_1$ with $a \neq a_1$ and $b \neq b_1$. Thus, in order for $(*)$ to make sense, a necessary condition is

$$Ka = Ka_1 \wedge Kb = Kb_1 \quad \Rightarrow \quad Kab = Ka_1b_1$$

In this case, we say that the multiplication $KaKb = Kab$ is well-defined.

Lemma 4.1

Let K be a subgroup of a group G, TFAE:

1. $K \lhd G$;
2. For $a, b \in G$, the multiplication $KaKb = Kab$ is well-defined.

Proof. `[1]` $\Rightarrow$ `[2]`: Let $Ka = Ka_1$ and $Kb = Kb_1$, so $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$. To get $Kab = Ka_1b_1$, it suffices to show that $ab(a_1b_1)^{-1} \in K$. Note that $K \lhd G$, we have $aKa^{-1} \subseteq K$. Thus

$$ab(a_1b_1)^{-1} = ab(b_1^{-1}a_1^{-1}) = a(bb_1^{-1})a_1^{-1} = (a(bb_1^{-1})a^{-1})(aa_1^{-1}) \in K$$

It follows that $Kab = Ka_1b_1$.
`[2]` $\Rightarrow$ `[1]`: If $a \in G$, to show $K \lhd G$, it suffices to show that $aka^{-1} \in K$ for all $k \in K$. Since $Ka = Ka$ and $Kk = K1$, by (2), we have

$$Kak = Ka1$$

It follows that $aka^{-1} \in K$ as desired. □

Proposition 4.1

Let $K \lhd G$ and write $G/K = \{Ka : a \in G\}$. For this set of all cosets of K,

1. G/K is a group under the operation $KaKb = Kab$;
2. The mapping $\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is an onto homomorphism;
3. If $[G : K]$ is finite, then $|G/K| = [G : K]$. In particular, $|G/K| = |G|/|K|$.

Proof.

(1) By the above lemma, we know that the operation is well-defined and G/K is closed under the operation. The identity of G/K is K, which is the same as $K1$. Also, $Ka \cdot Ka^{-1} = K = Ka^{-1}Ka$. Finally, G/K attains associativity because of the associativity of G, thus G/K is a group.

(2) φ is clearly onto. For $a, b \in G$, we have

$$\varphi(a)\varphi(b) = (Ka)(Kb) = K(ab) = \varphi(ab)$$

(3) If $[G : K]$ is finite, by the definition of the index, we have $[G : K] = |G/K|$. Also, if G is finite, by Lagrange theorem,

$$|G/K| = [G : K] = |G|/|K|$$

□

Lecture 12 - Monday, September 30

Definition 4.1: Quotient Group

Let $K \lhd G$, the group G/K of all cosets of K in G is called the **quotient group of G by K**. Also, the map

$$\varphi : G \to G/K$$

is given by $\varphi(a) = Ka$ is called the **coset map**.

Exercise: Let $D_{10} = \langle a, b : a^5 = 1 = b^2 \text{ and } aba = b \rangle$ be the dihedral group of order 10. List all normal subgroups K of D_{10} and all quotient groups D_{10}/K.

4.2 Isomorphism Theorems

Definition 4.2: Kernel & Image

Let $\alpha : G \to H$ be a group homomorphism. The **kernel** of α is defined by

$$\ker \alpha = \{g \in G : \alpha(g) = 1_H\} \subseteq G$$

and the **image** of α is defined by

$$\text{im } \alpha = \{\alpha(g) : g \in G\} \subseteq H$$

Proposition 4.2

Let $\alpha : G \to H$ be a group homomorphism

1. $\text{im } \alpha$ is a subgroup of H;
2. $\ker \alpha$ is a normal subgroup of G.

Proof. [1] definition check.
[2] definition check it is a subgroup, it is normal because

$$\alpha(g \ker \alpha g^{-1}) = \alpha(g)1_H\alpha(g^{-1}) = 1 \in \ker \alpha$$

Thus we have $g \ker \alpha g^{-1} \subseteq \ker \alpha$, wanted in teh Normality Test. □

Example 4.1

Consider the determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ defined by $A \mapsto \det(A)$. Thus we have $\ker(\det) = SL_n(\mathbb{R})$, the special linear group of order n. Thus $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

Example 4.2

Define the **sign** of a permutation $\sigma \in S_n$ by

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

Then the sign mapping $\operatorname{sgn} : S_n \to \{1, -1\}$ defined by $\sigma \mapsto \operatorname{sgn}(\sigma)$ is a homomorphism. We know that the kernel of the set is A_n, the alternating group, thus we have $A_n \lhd S_n$.

4.2.1 First Isomorphism Theorem

Theorem 4.1: First Isomorphism Theorem

Let $\alpha : G \to H$ be a group homomorphism. We have

$$G/\ker\alpha \cong \operatorname{im}\alpha$$

Proof. Let $K = \ker\alpha$. Since $K \lhd G$, G/K is a group. Define the group map

$$\overline{\alpha} : G/K \to \operatorname{im}\alpha$$

by $\overline{\alpha}(Kg) = \alpha(g)$ for all $Kg \in G/K$. Note that

$$Kg = Kg_1 \iff gg_1^{-1} \in K \iff \alpha(gg_1^{-1}) = 1 \iff \alpha(g) = \alpha(g_1)$$

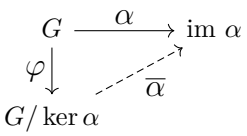
so the map is well-defined (one-to-one). The map is also clearly onto. It remains to show that $\overline{\alpha}$ is a group homomorphism. For $g, h \in G$,

$$\overline{\alpha}(KgKh) = \overline{\alpha}(Kgh) = \alpha(gh) = \alpha(g)\alpha(h) = \overline{\alpha}(Kg)\overline{\alpha}(Kh)$$

Thus $\overline{\alpha}$ is a group isomorphism as desired. □

Result 4.1

Let $\alpha : G \to H$ be a group homomorphism and $K = \ker\alpha$. Let $\varphi : G \to G/K$ be the coset map and let $\overline{\alpha}$ be defined as in the proof of the First Isomorphism Theorem. We have the following diagram:



Note that for $g \in G$, we have

$$\overline{\alpha}\varphi(g) = \overline{\alpha}(Kg) = \alpha(g)$$

thus $\alpha = \overline{\alpha}\varphi$. On the other hand, if we have $\alpha = \overline{\alpha}\varphi$, then the action of $\overline{\alpha}$ is determined by α and φ as

$$\overline{\alpha}(Kg) = \overline{\alpha}(\varphi(g)) = \overline{\alpha}\varphi(g) = \alpha(g)$$

Proposition 4.3

Let $\alpha : G \to H$ be a group homomorphism and $K = \ker \alpha$. Then α factors uniquely as $\alpha = \overline{\alpha}\varphi$ where $\varphi : G \to G/K$ is the coset and $\overline{\alpha} : G/K \to H$ is defined by $\overline{\alpha}(Kg) = \alpha(g)$. Note that φ is onto and $\overline{\alpha}$ is one-to-one.

Example 4.3

We have seen that $\mathbb{Z} = \langle \pm 1 \rangle$ and $\mathbb{Z}_n = \langle [1] \rangle$ for some $n \in \mathbb{N}$.
Let G be a cyclic group. Consider the map $\alpha : (\mathbb{Z}, +) \to G$ defined by $\alpha(k) = g^k$ for all $k \in \mathbb{Z}$, which is a group homomorphism. By the definition of $\langle g \rangle$, α is onto. Note that

$$\ker \alpha = \{k \in \mathbb{Z} : g^k = 1\}$$

Here we have two cases:

1. If $o(g) = \infty$, then $\ker \alpha = \{0\}$. By the First Isomorphism Theorem, we have

$$G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$$

2. If $o(g) = n \in \mathbb{N}$, then we have $\ker \alpha = n\mathbb{Z}$, again by the First Isomorphism Theorem, we have

$$G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

Result 4.2

If G is cyclic, then

$$G \cong \mathbb{Z} \qquad \text{or} \qquad G \cong \mathbb{Z}_n$$

Lecture 13 - Wednesday, October 02

4.2.2 Second Isomorphism Theorem

Theorem 4.2: Second Isomorphism Theorem

Let H and K be subgroups of a group G with $K \lhd G$. Then HK is a subgroup of G, $K \lhd HK$, $H \cap K \lhd H$, and

$$HK/K \cong H/(H \cap K)$$

Proof. Since $K \lhd G$, we know that $HK = KH$ is a subgroup of G, and so we have $K \lhd HK$. Consider the map

$$\alpha : H \to HK/K$$

defined by $\alpha(h) = Kh$. Then α is a homomorphism (**exercise**). If $x \in HK = KH$, say $x = kh$, then

$$Kx = K(kh) = Kh = \alpha(h)$$

Thus α is onto. Finally, we know

$$\ker \alpha = \{h \in H : Kh = K\} = \{h \in H : h \in K\} = H \cap K$$

By the First Isomorphism Theorem, we have

$$H/H \cap K \cong HK/K$$

as desired. □

4.2.3 Third Isomorphism Theorem

Theorem 4.3: Third Isomorphism Theorem

Let $K \subseteq H \subseteq G$ be groups with $K \lhd G$ and $H \lhd G$, then $H/K \lhd G/K$, and

$$(G/K)/(H/K) \cong G/H$$

Proof. Define $\alpha : G/K \to G/H$ by $\alpha(Kg) = Hg$ for all $g \in G$. Note that if we have $Kg = Kg_1$, then $gg^{-1} \in K \subseteq H$, thus $Hg = Hg_1$, and so α is well-defined. Clearly, α is onto. Also note that

$$\ker \alpha = \{Kg : Hg = H\} = \{Kg : g \in H\} = H/K$$

By the First Isomorphism Theorem, we have

$$(G/K)/(H/K) \cong G/H$$

as desired. □

5 Group Actions

5.1 Cayley's Theorem

Theorem 5.1: Cayley's Theorem

If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Comment 5.1

Idea of proof: Define

$$\begin{aligned} \sigma : G &\to S_G \\ a &\mapsto \mu_a \end{aligned}$$

where $\mu_a : G \to G$ is defined as $g \mapsto ag$.

Proof. Let $G = \{g_1, \ldots, g_n\}$ and let S_G be the permutation group of G, By identifying g_i with i $(1 \leq i \leq n)$, we see that

$$S_G \cong S_n$$

Thus it suffices to find a one-to-one homomorphism $\sigma : G \to S_G$. For $a \in G$, define $\mu_a : G \to G$ by $\mu_a(g) = ag$ for all $g \in G$. Note that $ag = ag_1$ implies then $g = g_1$ by cancellation, and $\mu_a(a^{-1}g) = g$, thus μ_a is a bijection and thus $\mu_a \in S_G$. Define $\sigma : G \to S_G$ by $\sigma(a) = \mu_a$. For $a, b \in G$, we have $\mu_{ab} = \mu_a\mu_b$ and thus σ is a homomorphism. Also, if $\mu_a = \mu_b$, then $a = \mu_a(1) = \mu_b(1) = b$. Thus σ is a one-to-one homomorphism, which implies that the kernel is the identity. By First Isomorphism Theorem, we have $G \cong \operatorname{im} \sigma$, a subgroup of $S_G \cong S_n$. □

Example 5.1

Let H be a subgroup of a group G with $[G : H] = m \ll \infty$. Let $X = \{g_1H, g_2H, \ldots, g_mH\}$ be the set of all distinct left cosets of H in G. For $a \in G$, define $\lambda_a : X \to X$ by

$$\lambda_a(gH) = agH \qquad \text{for all } gH \in X$$

Note that $agH = ag_1H$ implies that $gh = g_1H$ and $\lambda_a(a^{-1}gH) = gH$, hence λ_a is a bijection and $\lambda_a \in S_X$, the permutation group of X. Consider the map $\tau : G \to S_X$ defined by

$$\tau(a) = \lambda_a$$

For $a, b \in G$, we have $\lambda_{ab} = \lambda_a\lambda_b$ and thus τ is a homomorphism. Note that if $a \in \ker \tau$, then λ_a is the identity permutation. In particular, $aH = \lambda_a(H) = H$, which implies that $a \in H$, thus $\ker \tau \subseteq H$.

Theorem 5.2: Extended Cayley's Theorem

Let H be a subgroup of a group G with $[G : H] = m \ll \infty$. If G has no normal subgroup contained in H except $\{1\}$, then G is isomorphic to a subgroup of S_m.

Comment 5.2

Idea of proof: Let $X = \{g_1H, \ldots, g_mH\}$ be the set of all left cosets of H in G. Define

$$\begin{aligned} \tau : G &\to S_X \\ a &\mapsto \lambda_a \end{aligned}$$

where $\lambda_a : X \to X$ is defined as $gH \mapsto agH$.

Proof. Let X be the set of all distinct left cosets of H in G. We have $|X| = m$ and $S_X \cong S_m$. We have seen from the above example that there exists a group homomorphism $\tau : G \to S_X$ with $K = \ker \tau \subseteq H$. By the First Isomorphism Theorem, we have

$$G/K \cong \operatorname{im} \tau$$

Since $K \subseteq H$ and $K \lhd G$, by the assumption, we have $K = \{1\}$, and it follows that $G \cong \operatorname{im} \tau$, a subgroup of $S_X \cong S_m$. □

Lecture 14 - Friday, October 04

Corollary 5.1

Let G be a finite group and p the smallest prime dividing $|G|$. If H is a subgroup of G with $[G : H] = p$, then $H \lhd G$.

Discovery 5.1

This is a generalization of the proposition (3.5).

Proof. Let X be the set of all distinct left cosets of H in G, we have $|X| = p$ and $S_X \cong S_p$. Let $\tau : G \to S_X \cong S_p$ be the group homomorphism defined in the proof of Extended Cayley Theorem with $K = \ker \tau \subseteq H$. By the First Isomorphism Theorem, we have

$$G/K \cong \operatorname{im} \tau \subseteq S_p$$

Thus G/K is isomorphic to a subgroup of S_p. By Lagrange Theorem, we have $|G/K| \mid p!$. Also, since $K \subseteq H$, if $[H : K] = k$, then

$$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = pk$$

Thus $p \mid p!$ and $k \mid (p-1)!$. Since k divides $|H|$ which divides $|G|$ and p is the smallest prime dividing $|G|$, we see that every prime divisor of k must be $\geq p$ unless $k = 1$. Combining this with $k \mid (p-1)!$, this forces $k = 1$, which implies that $K = H$, thus $H \lhd G$. □

5.2 Group Actions

Definition 5.1: Group Action

Let G be a group and X a non-empty set. A **group action** of G on X is a mapping $G \times X \to X$ denoted by $(a, x) \mapsto a \cdot x$ such that

1. $1 \cdot x = x$ for all $x \in X$;
2. $a \cdot (b \cdot x) = (a \cdot b) \cdot x$ for all $a, b \in G$ and $x \in X$.

In this case, we say G **acts** on X.

Discovery 5.2

Let G be a group acting on a set $X \neq \varnothing$. For $a, b \in G$ and $x, y \in X$, by (1) and (2) we have

$$a \cdot x = b \cdot y \iff (b^{-1}a)x = y$$

In particular, $a \cdot x = a \cdot y$ if and only if $x = y$.

Example 5.2: Action by Conjugation

If G is a group, let G act on itself, i.e., $X = G$ by $a \cdot x = axa^{-1}$. Note that

- $1 \cdot x = 1x1^{-1} = x$;
- $a \cdot (b \cdot x) = a \cdot (bxb^{-1}) = a(bxb^{-1}) = (ab)x$.

In this case, we say G acts on itself by conjugation.

Discovery 5.3

For $a \in G$, define $\sigma_a : X \to X$ by $\sigma_a(x) = a \cdot x$ for all $x \in X$. Then one can show (see hw5) that

1. $\sigma_a \in S_X$, the permutation group of X;
2. The function $\theta : G \to S_X$ given by $\theta(a) = \sigma_a$ is a group homomorphism with $\ker\theta = \{a \in G : a \cdot x = x \ \ \forall\, x \in X\}$.

Notice that the group homomorphism $\theta : G \to S_X$ gives an equivalent definition of group action of G on X.
If $X = G$ and $|G| = n$ and $\ker\theta = \{1\}$ (faithful action), the map $\theta : G \to S_n$ shows that G is isomorphic to a subgroup of S_n, which is Cayley's Theorem.

Definition 5.2: Orbit and Stablizer

Let G be a group acting on a set $X \neq \varnothing$ and $x \in X$. We denote by

$$G \cdot x = \{g \cdot x : g \in G\} \subseteq X$$

the **orbit of** x and

$$S(x) = \{g \in G : g \cdot x = x\}$$

the **stablizer of** x.

5.2.1 Orbit Stablizer Theorem

Proposition 5.1: Orbit Stablizer Theorem

Let G be a group acting on a set $X \neq \varnothing$ and $x \in X$. Let $G \cdot x$ and $S(x)$ be the orbit and stablizer of x respectively, then

1. $S(x)$ is a subgroup of G;
2. there exists a bijection from $G \cdot x$ to $\{g \cdot S(x) : g \in G\}$ and thus $|G \cdot x| = [G : S(x)]$.

Proof. [1]: Since $1 \cdot x = x$, so we have $1 \in S(x)$. Also, if $g, h \in S(x)$, then $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, which implies that $gh \in S(x)$. Moreover, $g^{-1} \cdot x = (g^{-1}g) \cdot x = x$, hence by the subgroup test, we have $S(x)$ is a subgroup of G.

Lecture 15 - Monday, October 07

[2]: Consider the map $\varphi : G \cdot x \to \{gS(x) : g \in G\}$ defined by $\varphi(g \cdot x) = gS(x)$. Note that

$$g \cdot x = h \cdot x \iff h^{-1}g \in S(x) \iff gS(x) = hS(x)$$

Thus φ is well-defined and one-to-one. Since φ is clearly onto, φ is a bijection. It follows that

$$|G \cdot x| = |\{gS(x) : g \in G\}| = [G : S(x)]$$

□

5.2.2 Orbit Decomposition Theorem

Theorem 5.3: Orbit Decomposition Theorem

Let G be a group acting on a finite set $X \neq \varnothing$, let

$$X_f = \{x \in X : a \cdot x = x \ \ \forall a \in G\}$$

Note that $x \in X_f$ if and only if $|G \cdot x| = 1$. Let $G \cdot x_1, G \cdot x_2, \ldots, G \cdot x_n$ denote the distinct non-singleton

orbits (i.e., $|G \cdot x| > 1$). Then

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$$

Proof. The idea of the proof is to show that all $G \cdot x_1, G \cdot x_2, \ldots, G \cdot x_n$ are pairwise disjoint.
Note that for $a, b \in G$, $x, y \in X$,

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y \iff y \in G \cdot x \iff G \cdot x = G \cdot y$$

Thus two orbits are either disjoint or the same, it follows that the orbits are from a disjoint union of X. Since $x \in X_f$ if and only if $|G \cdot x| = 1$, the set $X \backslash X_f$ contains all non-singleton orbits, which are disjoint. Thus by previous proposition, we have

$$|X| = |X_f| + \sum_{i=1}^{n} |G \cdot x_i| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$$

wwwww. □

Example 5.3

Let G be a group acting on itself by conjugation, i.e., $g \cdot x = gxg^{-1}$. Then

$$\begin{aligned} G_f &= \{x \in G : gxg^{-1} = x \ \ \forall\, g \in G\} \\ &= \{x \in G : gx = xg \ \ \forall\, g \in G\} = Z(G) \end{aligned}$$

Also, for all $x \in G$,

$$S(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

The set is called the **centralizer of** x and is defined by $S(x) = C_G(x)$. Finally, in this case, the orbit

$$G \cdot x = \{gxg^{-1} : g \in G\}$$

is called the **conjugacy class of** x. Then, as a direct consequence of the Orbit Decomposition theorem, we have the following corollary.

Corollary 5.2

Let G be a finite group and $\{gx_1g^{-1} : g \in G\}, \ldots, \{gx_ng^{-1} : g \in G\}$ denote the distinct non-singleton conjugacy classes, then

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)]$$

Lemma 5.1

Let p be a prime and $m \in \mathbb{N}$. Let G be a group of order p^m acting on a finite set $X \neq \varnothing$. Let X_f be defined as in the Orbit Decomposition theorem, then we have

$$|X| = |X_f| \pmod{p}$$

Proof. By Orbit Decomposition theorem, we have

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$$

with $[G : S(x_i)] > 1$ for all $1 \leq i \leq n$. Since $[G : S(x_i)]$ divides $|G| = p^m$, we have $p \mid [G : S(x_i)]$. □

5.2.3 Cauchy

Theorem 5.4: Cauchy

Let p be a prime and G a fintie group, if $p \mid |G|$, then G contains an element of order p.

Proof. (by J Mckay) Define

$$X = \{(a_1, \ldots, a_p) : a_i \in G \text{ and } a_1 a_1 \cdots a_p = 1\}$$

Since a_p is uniquely determined by $a_1, \ldots, a_{p-1}$, if $|G| = n$, we have $|X| = n^{p-1}$. Since $p \mid n$, we have $|X| \equiv 0 \pmod{p}$. Let the group $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ acts on X by "cycling", i.e., for $k \in \mathbb{Z}_p$,

$$k \cdot (a_1, \ldots, a_p) = (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$$

One can verify that this action is well-defined. Let X_f be defined as in Orbit Decomposition theorem, then

$$(a_1, \ldots, a_p) \in X_f \iff a_1 = \cdots = a_p$$

Clearly, $(1, \ldots, 1) \in X_f$ and $|X_f| \geq 1$. Since $|\mathbb{Z}_p| = p$, we have

$$|X_f| \equiv |X| \equiv 0 \pmod{p}$$

It follows that $|X_f| \geq p$, which implies that there exists some $G \ni a \neq 1$ such that $(a, \ldots, a) \in X_f$, thus $a^p = 1$. Since p is prime and a is not units, we have $o(a) = p$. □

Quiz 5.1

Let G be a finite group acting on a non-empty set X. For $x \in X$, let $S(x)$ and $G \cdot x$ denote the stablizer and orbit of x respectively. Determine if the following statements are true or false.

(F) $G \cdot x$ is a subgroup of G;

(T) $|G \cdot x| = [G : S(x)]$.

Quiz 5.2

Determine wheather the following statement is true or false: the map $(\mathbb{Z}_4, +) \times \mathbb{Z}_7 \to \mathbb{Z}_7$, $(n, x) \mapsto n \cdot x := x^n$, is a group action.

Proof. The statement is false, because $(2 + 2) \cdot x = 0 \cdot x = 1$, but

$$2 \cdot (2 \cdot x) = 2 \cdot (x^2) = x^4 \neq 1$$

for $x = 2$ as an example. □

Quiz 5.3

Determine whether the following statement is true or false: the map $\mathbb{Z} \times \mathbb{R} \to \mathbb{R}$, $(n, x) \mapsto n \cdot x := x + n$, is a group action.

Proof. True. □

Quiz 5.4

Let G be a finite group acting on a non-empty set X. For each $x \in X$, define X_f as:

$$X_f = \{x \in X : a \cdot x = x \text{ for all } a \in G\}.$$

Determine if the following statements are true or false.

1. If q is a positive integer with $q \mid |G|$, then G contains an element of order q.
2. If $x \in X_f$, then $|G \cdot x| = 1$.
3. Let p be prime and $m \in \mathbb{N}$. If $|G| = p^m$ and $|X_f| \geq 1$, then $|X_f| \geq p$.

Proof. [1] is false, it is true if q is a prime. [2] is true. [3] is false, we know that

$$|X| \equiv |X_f| \pmod{p}$$

but we don't have information of how many elements are there in X_f. □

Quiz 5.5

et G be a finite group and H be a subgroup of G. Determine if the following statements are true or false.

1. If $|G| = n$, then G is isomorphic to a subgroup of S_{n+1}.
2. If $|G : H| = m$, then G is isomorphic to a subgroup of S_m.
3. If p is the smallest prime with $p \mid |G|$ and $|G : H| = p$, then $H \triangleleft G$.

Proof. [1] is true, we know that G is isomorphic to a subgroup of S_n by Cayley's Theorem, and we know that S_n is a subgroup of S_{n+1}. [2] is false, we also require that there is no normal subgroup of G contained in H. [3] is true. □

Lecture 16 - Wednesday, October 09

6 Sylow Theorems

6.1 p-Groups

Definition 6.1: p-Group

Let p be a prime, a group in which every element has order of a non-negative power of p is called a **p-group**.

As a direct corollary of the Cauchy Theorem:

Corollary 6.1

A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. [$\Longrightarrow$]
SFAC that $|G|$ is not a power of p, then there exists another prime q such that $q \mid |G|$. By Cacuhy, we know that there exists element of order q, contradicting the fact that G is a p-group.
[$\Longleftarrow$]
Since G is a power of p, we know that all elements in G have order of power of p as a result of Lagrange Theorem. □

Lemma 6.1

The center $Z(G)$ of a non-trivial finite p-group G contains more than one element.

Proof. Recall that we have

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

where $[G : C_G(x_i)] > 1$. Since G is a p-group, by the above corollary, we know that $p \mid |G|$, hence we have

$$|Z(G)| \equiv |G| \equiv 0 \pmod{p}$$

It follows that $p \mid |Z(G)|$. Since $1 \in Z(G)$ and $|Z(G)| \geq 1$, we know that $|Z(G)|$ has at least p elements. □

Lemma 6.2

If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}$$

Proof. We recall

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

is the **normalizer** of H in G. Let X be the set of all left cosets of H in G, hence $|X| = [G : H]$. Let H act on X by left multiplication. Then for $x \in G$,

$$\begin{aligned} xH \in X_f &\iff hxH = xH \qquad \forall\, h \in H \\ &\iff x^{-1}hxH = H \qquad \forall\, h \in H \\ &\iff x^{-1}Hx = H \\ &\iff x \in N_G(H) \end{aligned}$$

Thus $|X_f|$ is the number of cosets xH with $x \in N_G(H)$ and hence $|X_f| = [N_G(H) : H]$. □

Corollary 6.2

Let H be a p-subgroup of a fintie group G. If $p \mid [G : H]$, then $p \mid [N_G(H) : H]$ and $N_G(H) \neq H$.

Proof. By the above lemma, we have

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$$

Since $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq 1$, we must have $[N_G(H) : H] \geq p$, thus $N_G(H) \neq H$. □

Lecture 17 - Friday, October 11

6.2 Sylow's Three Theorems

6.2.1 First Sylow Theorem

Theorem 6.1: First Sylow Theorem

Let G be a group of order $p^n m$ where p is a prime, $n \geq 1$ and $\gcd(p, m) = 1$, then G contains a subgroup of order p^i for all $1 \leq i \leq n$. Moreover, every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.

Discovery 6.1

The theorem can be viewed as a generalization of Cauchy Theorem (the case of $i = 1$).

Proof. We prove this theorem by induction on i. For $i = 1$, by Cauchy Theorem, G contains an element a of order p, in other words, $|\langle a \rangle| = p$. Suppose that the statement hold for $1 \leq i < n$, say H is a subgroup of G of order p^i. Then $p \mid [G : H]$. By the above corollary, $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq p$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p, such a group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$, we have $H \lhd H_1$. Finally,

$$|H_1| = |H||H_1/H| = p^i \cdot p = p^{i+1}$$

as desired. □

Definition 6.2: Sylow p-group

A subgroup P of a group G is said to be a **Sylow p-group of** G if P is a maximal p-group of G, i.e., $P \subseteq H \subseteq G$ with H is a p-group, then $P = H$.

Corollary 6.3

Let G be a group of order $p^n m$ where p is a prime, $n \geq \lceil 0.69 \rceil$ and $\gcd(p, m) = 1$. Let H be a p-subgroup of G,

1. H is a Sylow p-subgroup if and only if $|H| = p^n$;
2. Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup;
3. If there is ony one Sylow p-subgroup, denoted as P, then P is a normal subgroup of G.

6.2.2 Second Sylow Theorem

Theorem 6.2: Second Sylow Theorem

If H is a p-subgroup of a finite group G and P is any p-subgroup of G, then there exists $g \in G$ such that $H = gPg^{-1}$. In particular, any two Sylow p-subgroup of G are conjugate.

Proof. Let X be the set of all left cosets of P in G and let H acts on X by left multiplication. By Lemma 5.1, we have

$$|X_f| \equiv |X| = [G : P] \pmod{p}$$

Since $p \nmid [G : P]$, we have $|X_f| \neq 0$. Thus there exists $gP \in X_f$ for some $g \in G$. Note that

$$\begin{aligned} gP \in X_f &\iff hgP = gP \qquad \forall\, h \in H \\ &\iff g^{-1}hgP = P \qquad \forall\, h \in H \\ &\iff gHg^{-1} \subseteq P \\ &\iff H \subseteq g^{-1}Pg \end{aligned}$$

If H is a Sylow p-subgroup, then $|H| = |P| = |gPg^{-1}|$, then $H = gPg^{-1}$. □

6.2.3 Third Sylow Theorem

Theorem 6.3: Third Sylow Theorem

If G is a finite group and there is a prime p such that $p \mid |G|$, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$.

Proof. By Second Sylow Theorem, the number of Sylow p-subgroup of G is the number of conjugates of any one of them, say P. This number is $[G : N_G(P)]$, which is a divisor of $|G|$.
Let X be the set of all Sylow p-subgroups of G and let P act on X by conjugation. Then $Q \in X_f$ if and only

if $gQg^{-1} = Q$ for all $g \in P$, where the latter condition holds if and only if $P \subseteq N_G(Q)$. Both P and Q are Sylow p-subgroups of G and hence of $N_G(Q)$. Thus by the above corollary, they are conjugate in $N_G(Q)$. Because $Q \lhd N_G(Q)$, this can only occur if $Q = P$ and $X_f = \{P\}$. By Lemma 5.1,

$$|X_f| \equiv |X| \equiv 1 \pmod{p}$$

Thus $|X| = kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$ as desired. □

Discovery 6.2

Suppose G is a group with $|G| = p^n m$ with $\gcd(p, m) = 1$. Let n_p be the number of Sylow p-subgroups of G. By the third Sylow Theorem, we see that $n_p \mid p^n m$ and $n_p \equiv 1 \pmod{p}$. Since $p \neq n_p$, we have $n_p \mid m$.

Example 6.1

`Claim:` every group of order 15 is cyclic.

Proof. Let G be a group of order $15 = 3 \cdot 5$, let n_p be the number of Sylow p-subgroups of G. By the third Sylow Theorem, we have $n_3 \mid 5$ and $n_3 \equiv 1 \pmod{3}$. Thus $n_3 = 1$, and similarly, we also have $n_5 = 1$. It follows that there is only one Sylow 3-subgroup and one Sylow 5-subgroup of G, denoted as P_3 and P_5 respectively. Thus $P_3 \lhd G$ and $P_5 \lhd G$. Consider $|P_3 \cap P_5|$, which divides both 3 and 5, so

$$|P_3 \cap P_5| = 1 \quad \Rightarrow \quad P_3 \cap P_5 = \{1\}$$

Also $|P_3 P_5| = 15 = |G|$, it follows that

$$G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$$

as desired. □

Exercise: Construct a cyclic group of order greater than 100.

Proof. $7 \cdot 17 = 119 > 100$. □

Lecture 18 - Monday, October 21

Example 6.2

There are two isomorphic classes of groups of order 21.

Proof. Let G be a group with $|G| = 21$. Let n_p be the number of Sylow p-subgroup of G. By the third Sylow Theorem, we have

$$n_3 \mid 7 \qquad \text{and} \qquad n_3 \equiv 1 \pmod{3}$$

Thus $n_3 = 1$ or 7. Also, we have

$$n_7 \mid 3 \qquad \text{and} \qquad n_7 \equiv 1 \pmod{7}$$

so we have $n_7 = 1$. It follows that G has a unique Sylow 7-subgroup, say P_7. Note that $P_7 \lhd G$ and is cyclic, say $P_7 = \langle x \rangle$ with $x^7 = 1$. Let H be a Sylow 3-subgroup, since $H = 3$, H is cyclic and so $H = \langle y \rangle$ with $y^3 = 1$. Since $P_7 \lhd G$, we have $yxy^{-1} = x^i$ for some $1 \leq i \leq 6$, hence

$$x = y^3xy^{-3} = y^2(yxy^{-1})y^{-2} = y^2x^iy^{-2} = x^{i^3}$$

Recall that $x^7 = 1$, so we have

$$i^3 - 1 \equiv 0 \pmod 7$$

Since $1 \leq i \leq 6$, we have $i = 1, 2$, or 4.

1. If $i = 1$, then $yxy^{-1} = x$, i.e., $yx = xy$. Thus G is an abelian group and $G \cong Z_{21}$.
2. If $i = 2$, then $yxy^{-1} = x^2$, thus

$$G = \{x^iy^j : 0 \leq i \leq 6, 0 \leq j \leq 2, yxy^{-1} = x^2\}$$

3. If $i = 4$, then $yxy^{-1} = x^4$. Note that

$$y^2xy^{-2} = y(yxy^{-1})y^{-1} = x^{16} = x^2$$

Observe that y^2 could also be the generator of H, then by replacing y with y^2, we have case 2 $\equiv$ case 3. As a result, we conclude that there are two isomorphic classes of group of order 21. □

Exercise: Prove that there is no simple group of order 72.

Proof. We know that $n_3 \mid 2^3$ and $n_3 \equiv 1 \pmod 3$, so $n_3 = 1$ or 4. If $n_3 = 1$, the group is not simple, so we may assume that $n_3 = 4$. Let G acts on those subgroups by conjugation, so we get a homomorphism $G \to S_4$, which has a size of $4! = 24 < 72$. This implies that the kernel of the homomorphism cannot be trivial, proving that the group G isn't simple. □

Quiz 6.1

Let G be a group of order $p^n \cdot m$ with $\gcd(p, m) = 1$. Let S be the set of all Sylow p-subgroups of G. Determine if the following statements are true or false.

(T) If $P \in S$, then $|P| = p^n$.

(F) If $P \in S$, then $P \lhd G$.

(T) $|S| \equiv 1 \pmod p$.

(T) $|S| \mid m$.

Quiz 6.2

Let p be a prime and H a non-trivial p-subgroup of a finite group G. Let $N_G(H)$ be the normalizer of H in G. Determine if the following statements are true or false.

(T) $|H| = p^n$ for some $n \in \mathbb{N}$.

(F) The center $Z(H)$ of H has only one element.

(T) $H \leq N_G(H)$.

(F) $N_G(H) \neq H$.

Quiz 6.3

Is a group of order 69 always abelian?

Proof. We may show that the number of Sylow 3-subgroup and Sylow 23-subgroup are both 1, thus for G with $|G| = 69$, we have

$$G \cong C_3 \times C_{23} \cong C_{69}$$

which is in fact cyclic. □

Quiz 6.4

Is a group of order 55 always abelian?

Proof. Nope. See this link for counter example. □

7 Finite Abelian Groups

7.1 Primary Decomposition

Definition 7.1: Power of Group

Let G be a group and $m \in \mathbb{Z}$, we define

$$G^{(m)} = \{g \in G : g^m = 1\}$$

Proposition 7.1

Let G be an abelian group, then $G^{(m)}$ is a subgroup of G.

Proof. We have $1^m = 1 \in G^{(m)}$. If $g, h \in G^{(m)}$, we have

$$(gh)^m = gh \cdots gh = g^m h^m = 1$$

Finally, we have $(g^{-1})^m = (g^m)^{-1} = 1$. □

Proposition 7.2

Let G be a finite abelian group with $|G| = mk$ with $\gcd(m, k) = 1$. Then

1. $G \cong G^{(m)} \times G^{(k)}$;
2. $|G^{(m)}| = m$ and $|G^{(k)}| = k$.

Proof. Since G is abelian, we have

$$G^{(m)} \lhd G \qquad \text{and} \qquad G^{(k)} \lhd G$$

Also, since $\gcd(m, k) = 1$, there exists $x, y \in \mathbb{Z}$ such that $mx + ky = 1$.
`Claim 1:` $G^{(m)} \cap G^{(k)} = \{1\}$
For $g \in G^{(m)} \cap G^{(k)}$, we simply have

$$g = g^{mx+ky} = g^{mx} g^{ky} = 1$$

`Claim 2:` $G = G^{(m)} G^{(k)}$
If $g \in G$, then

$$1 = g^{mk} = (g^k)^m = (g^m)^k$$

If follows that $g^k \in G^{(m)}$ and $g^m = G^{(k)}$. Thus

$$g = g^{mx+ky} = (g^k)^y (g^m)^x \in G^{(m)} G^{(k)}$$

Combining the above two claims, we have $G \cong G^{(m)} \times G^{(k)}$ by Theorem (3.2) as desired. Now, write $|G^{(m)}| = m$ and $|G^{(k)}| = k'$, hence $mk = |G| = m'k'$.

`Claim 3:` $\gcd(m, k') = 1$

Suppose that $\gcd(m, k') \neq 1$, then there exists a prime p such that $p \mid m$ and $p \mid k'$. By Cauchy Theorem, there exists $g \in G^{(k)}$ with $o(g) = p$. Since $p \mid m$, we also have

$$g^m = (g^p)^{m/p} = 1 \qquad \text{i.e., } g \in G^{(m)}$$

Thus we must have $g = 1$, which gives a contradiction since $o(g) = p$. Thus, we have $\gcd(m, k') = 1$. Note that since $m \mid m'k'$ and $\gcd(m, k') = 1$, we have $m \mid m'$. Similarly, we have $k \mid k'$. Since $mk = m'k'$, we have $m = m'$ and $k = k'$. □

Lecture 19 - Wednesday, October 23

As a direct consequence of the above proposition, we have

7.1.1 Primary Decomposition Theorem

Theorem 7.1: Primary Decomposition Theorem

Let G be a finite abelian group with $|G| = {p_1}^{n_1} \cdots {p_k}^{n_k}$ where $p_1, \ldots, p_k$ are distinct primes and $n_1, \ldots, n_k \in \mathbb{N}$, then we have

(1)
$$G \cong G^{({p_1}^{n_1})} \times \cdots \times G^{({p_k}^{n_k})}$$

(2)
$$\left|G^{({p_i}^{n_i})}\right| = {p_i}^{n_i} \qquad 1 \leq i \leq k$$

Example 7.1

Let $G = \mathbb{Z}_{13}^*$, then $|G| = 12 = 2^2 \cdot 3$. Note that

$$G^{(4)} = \{a \in \mathbb{Z}_{13}^* : a^4 = 1\} = \{1, 5, 8, 12\}$$

and

$$G^{(3)} = \{a \in \mathbb{Z}_{13}^* : a^3 = 1\} = \{1, 3, 9\}$$

so by the above theorem, we have

$$\mathbb{Z}_{13}^* \cong \{1, 5, 8, 12\} \times \{1, 3, 9\}$$

7.2 Structure Theorem of Finite Abelian Groups

Comment 7.1

By the Primary Decomposition Theorem, to understand finite abelian groups, it suffices to consider finite abelian groups of prime order. We recall that if $|G| = p$ for p is a prime, then $G \cong \mathbb{Z}_p$. If $|G| = p^2$, then we have $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. We wonder how about other powers of p.

Proposition 7.3

If G is a fintie abelian p-group that contains only one subgroup of order p, then G is cyclic.

Discovery 7.1

Contrapositively, if a finite abelian group is not cyclic, it has at least two subgroups of order p.

Proof. Let $y \in G$ be of maximal order, i.e., $o(y) \geq o(x)$ for all $x \in G$.
`Claim :` $G = \langle y \rangle$
Suppose for a contradiction that $G \neq \langle y \rangle$, then the quotient group

$$G/\langle y \rangle \neq \{1\}$$

is a non-trivial p-group, which by Cauchy Theorem contains an element of order p, say $z \neq 1$. Now consider the coset map $\pi : G \to G/\langle y \rangle$. Let $x \in G$ such that $\pi(x) = z$. Since

$$\pi(x^p) = \pi(x)^p = z^p = 1$$

we see that $x^p \in \langle y \rangle$. Thus $x^p = y^m$ for some $m \in \mathbb{Z}$. Here comes two cases:

1. If $p \nmid m$, since $o(y) = p^r$ for some $r \in \mathbb{N}$, then

$$o(y^m) = \frac{p^r}{\gcd(m, p^r)} = p^r$$

   Since y is of max order, we have

$$o(x^p) < o(x) \leq o(y) = o(y^m) = o(x^p)$$

   which yields us a contradiction.

2. If $p \mid m$, then $m = pk$ for some $k \in \mathbb{Z}$. Thus we have $x^p = y^m = y^{pk}$. Since G is abelian, we have

$$(xy^{-k})^p = 1$$

   Thus xy^{-k} belongs to the one and only one subgroup of order p, say H. On the other hand, the cyclic group $\langle y \rangle$ contains a subgroup of order p, which must be H. Thus $xy^{-k} \in \langle y \rangle$, which implies that $x \in \langle y \rangle$. It follows that $z = \pi(x) = 1$, a contradiction.

Combining two cases, we see that $G = \langle y \rangle$. □

Proposition 7.4

Let $G \neq \{1\}$ be a finite abelien p-group. Let C be a cyclic subgroup of max order. Then G contains a subgroup B such that

$$G = CB \qquad \text{and} \qquad C \cap B = \{1\}$$

Thus by Theorem (3.2), we have $G \cong C \times B$.

Proof. Proof is introduced later. □

Theorem 7.2

Let $G \neq \{1\}$ be a finite abelian p-group, then G is isomorphic to a direct product of cyclic groups

Proof. By the above proposition, there exist a cyclic group C_1 and a subgroup B_1 of G such that $G \cong C_1 \times B_1$. Since $|B_1|$ divides $|G|$ by Lagrange's Theorem, the group B_1 is also a p-group itself. Thus if $B \neq \{1\}$, by above proposition, there exist a cyclic group C_2 and a subgroup B_2 such that $B_1 \cong C_2 \times B_2$. Continue in this way to get cyclic groups until we obtain $B_k = \{1\}$ for some $k \in \mathbb{N}$, then

$$G \cong C_1 \times \cdots \times C_k$$

as desired. □

Comment 7.2

One can show that the decomposition of a finite abelian p-group into a direct product of cyclic groups is unique up to their order. Moreover, one can show the following exercise:

Exercise: If G is a fintie abelian p-group, and

$$G \cong C_1 \times \cdots C_k \cong D_1 \times \cdots \times D_\ell$$

are two decompositions of G is products of cyclic groups C_i and D_j of order p^{n_i} and p^{m_j} respectively. Then $k = \ell$, and after suitable rearrangements,

$$n_1 = m_1,\ n_2 = m_2, \ldots, n_k = m_\ell$$

Lecture 20 - Friday, October 25

Comment 7.3

Test 1 day.

Lecture 21 - Monday, October 28

Proof. This is the proof for proposition (7.4).
We prove this result by induction. If $|G| = p$, we take $C = G$ and $B = \{1\}$ and the result follows. Suppose that the result holds for all abelian groups of order p^{n-1} with $n \in \mathbb{N}$ and $n \geq 2$. Consider $|G| = p^n$, so we have two cases:
`Case 1:` $G = C$. By taking $B = \{1\}$, the result follows.
`Case 2:` $G \neq C$. This means that G is not cyclic, so by proposition (7.3), there exist at least two subgroups of order p. Since C is cyclic, it contains exactly one subgroup of order p by theorem (2.3). Thus there exists

a subgroup D of G with $|D| = p$ and $D \not\subseteq C$. Hence we have $C \cap D = \{1\}$. Consider the coset map $\pi : G \to G/D$. If we consider $\pi|_C$, the restriction of π on C, then

$$\ker \pi|_C = C \cap D = \{1\}$$

By First Isomorphism Theorem, we have $\pi(C) \cong C$. Let y be the generator of the cyclic group C, i.e., $C = \langle y \rangle$. Since $\pi(C) \cong C$, $\pi(C) = \langle \pi(y) \rangle$. By the assumption on C, $\pi(C)$ is a cyclic subgroup of G/D of maximal order. Since $|G/D| = p^{n-1}$, by the inductive hypothesis, G/D has a subgroup E such that

$$\pi(C)E = G/D \qquad \text{and} \qquad \pi(C) \cap E = \{1\}$$

Let $B = \pi^{-1}(E)$, i.e. $\pi(B) = E$.
`Claim 1:` $G = CB$
Note that since E is a subgroup containing $\{1\}$, we have

$$\pi^{-1}(\{1\}) = D \subseteq B$$

If $x \in G$, since $\pi(C)\pi(B) = \pi(C)E = G/D$, there exists $u \in G$ and $v \in B$ such that $\pi(x) = \pi(u)\pi(v)$. Since $\pi(xu^{-1}v^{-1}) = 1$, we have

$$xu^{-1}v^{-1} \in D \subseteq B$$

Since $v \in B$, we have $xu^{-1} \in B$. Since G is abelian, we have $x = uxu^{-1} \in CB$.
`Claim 2:` $C \cap B = \{1\}$
Let $x \in C \cap B$. Then

$$\pi(x) = \pi(C) \cap \pi(B) = \cap(C) \cap E = 1$$

Since $\pi(x) = 1$ in G/D, we have $x \in D$. Therefore we have $x \in C \cap D = \{1\}$. The result follows by combining claim 1 and claim 2. □

7.2.1 Structure Theorem of Finite Abelian Group

Theorem 7.3: Structure Theorem of Finite Abelian Group

If G is a finite abelian group, then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

where $\mathbb{Z}_{p_i^{n_i}} = (\mathbb{Z}_{p_i^{n_i}}, +) \cong C_{p_i^{n_i}}$ are cyclic groups of order $p_i^{n_i}$ for all $1 \leq i \leq k$. Note that p_i are not necessarily distinct. The numbers $p_i^{n_i}$ are uniquely determined up to their order.

Comment 7.4

Note that if p_1, p_2 are distinct primes, then

$$C_{p_1^{n_1}} \times C_{p_2^{n_2}} \cong C_{p_1^{n_1} \cdot p_2^{n_2}}$$

Theorem 7.4: Invariant Factor Decomposition of Finite Abelian Group

Let G be a finite abelian group, then

$$G \cong \mathbb{Z}_r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$$

where $r \geq 0$ and $n_i \in \mathbb{N}$ for $1 \leq i \leq r$, $n_1 > 1$ and $n_1 \mid n_2 \mid \cdots \mid n_r$.

Example 7.2

Let G be an abelian group of order $48 = 2^4 \cdot 3$. Hence we have

$$G \cong H \times Z_3$$

where H is an abelian group of order 2^4. The options for H are

- $\mathbb{Z}_{2^4}$
- $\mathbb{Z}_{2^3} \times \mathbb{Z}_2$
- $\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}$
- $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Quiz 7.1

Let p be a prime and G a finite group. Determine if the following statements are true or false.

(T) If G is a p-group, then $|G| = p^n$ for some $n \in \mathbb{N} \cup \{0\}$.

(T) If G is not a p-group, then $|G| \neq p^n$ for all $n \in \mathbb{N} \cup \{0\}$.

(F) If G is an abelian p-group, then G is cyclic.

Proof. I think the third is false, consider $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

Quiz 7.2

Let G be a finite abelian group with $|G| = 35$. For $m \in \mathbb{Z}$, let $G^{(m)} = \{g \in G \mid g^m = 1\}$. Determine if the following statements are true or false.

(T) $G \cong G^{(5)} \times G^{(7)}$.

(F) $|G^{(5)}| = 7$.

(T) $G^{(5)} \cap G^{(7)} = \{1\}$.

(F) If $g \in G$, then $g^7 \in G^{(7)}$.

Quiz 7.3

Let p be a prime and G a finite abelian group. Determine if the following statements are true or false.

(T) If G is a p-group, then G is isomorphic to a direct product of cyclic groups.

(T) $G \cong C_{p_1}^{n_1} \times \cdots \times C_{p_k}^{n_k}$ for some primes p_i and non-negative integers n_i (where $1 \leq i \leq k$), where C_{p^n} denotes the cyclic group of order p^n.

(T) $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ with $n_i \in \mathbb{N}$ and $n_1 \mid n_2 \mid \cdots \mid n_r$.

Lecture 22 - Wednesday, October 30

8 Rings

8.1 Rings

Definition 8.1: Rings

A set R is a **(unital) ring** if it has two operations, addition $+$ and multiplication $\cdot$, such that $(R, +)$ is an abelian group and $(R, \cdot)$ satisfies the closure, associativity, and identity properties of a group. More precisely, if R is a ring, then for all $a, b, c \in R$,

- $a + b \in R$;
- $a + (b + c) = (a + b) + c$;
- $\exists\ 0 \in R$ such that $a + 0 = a = 0 + a$ for all $a \in R$ (0 is called the **zero** in R);
- $\exists\ -a \in R$ such that $a + (-a) = 0 = (-a) + a$ ($-a$ is called the **inverse of** a in R);
- $a + b = b + a$;
- $ab := a \cdot b \in R$;
- $a(bc) = (ab)c$;
- $\exists\ 1 \in R$ such that $a1 = a = 1a$ (1 is called the **unity** in R).
- $a(b + c) = ab + ac$ and $(b+c)a = ba+ca$ (*distributivity law*).

Comment 8.1

A ring is said to be a **commutative ring** if $ab = ba$.

Example 8.1

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings with the zero being 0 and the unity being 1.

Example 8.2

For $n \in \mathbb{N}$ with $n \geq 2$, $\mathbb{Z}_n$ is a commutative ring with the zero being $[0]$ and the unity being $[1]$.

Example 8.3

For $n \in \mathbb{N}$ with $n \geq 2$, the set $M_n(\mathbb{R})$ is a ring using matrix addition and matrix multiplication with the zero being the zero matrix and the unity being the identity matrix. However, it is not a commutative ring.

Discovery 8.1

Note that since $(R, \cdot)$ is not a group, there is no left or right cancellation. For instance, in $\mathbb{Z}$,

$$0 \cdot x = 0 = 0 \cdot y$$

does not imply $x = y$.

Definition 8.2:

Given a ring R, we wish to distinguish the difference between multiples in addition and in multiplication. For $n \in \mathbb{N}$ and $a \in R$, we write

$$na = a + a + \cdots + a \qquad (n\text{-times addition})$$

and

$$a^n = a \cdot a \cdots a \qquad (n\text{-times multiplication})$$

In terms of addition, we have

$$0a = 0 \qquad 1a = a \qquad -(-a) = a$$

For $n \in \mathbb{N}$, we also define

$$(-n)a = (-a) + (-a) + \cdots + (-a) \qquad (n \text{ times addition})$$

Also, we define $a^0 = 1$. If the multiplicative inverse of a exists, say a^{-1}, i.e., $a^{-1}a = 1 = aa^{-1}$, we define

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

For $n, m \in \mathbb{N}$, we indeed have

$$(na) + (ma) = (n+m)a; \qquad n(ma) = (nm)a; \qquad n(a+b) = na + nb$$

Proposition 8.1

Let R be a ring and $r, s \in R$,

(a) If 0 is the zero of R, then $0r = 0 = r0$;

(b) $(-r)s = r(-s) = -rs$;

(c) $(-r)(-s) = rs$;

(d) For any $m, n \in \mathbb{Z}$, $(mr)(ns) = (mn)(rs)$.

8.1.1 Trivial Ring

Definition 8.3: Trivial Ring

A **trivial ring** is a ring of only one element. In this case, we have $1 = 0$.

Comment 8.2

If R is a ring with $R \neq \{0\}$, since $r = r \cdot 1$ for all $r \in R$, we have $1 \neq 0$. (Otherwise we have

$r = r1 = r0 = 0$).

Example 8.4: Component-wise Operations

Let $R_1, \ldots, R_n$ be rings. We define **component-wise operations** on the product $R_1 \times \cdots R_n$ as follows:

$$(r_1, \ldots, r_n) + (s_1, \ldots, s_n) = (r_1 + s_1, \ldots, r_n + s_n)$$
$$(r_1, \ldots, r_n) \cdot (s_1, \ldots, s_n) = (r_1 \cdot s_1, \ldots, r_n \cdot s_n)$$

One can check that $R_1, \ldots, R_n$ is a ring. This set is called the **direct product** of $R_1, \ldots, R_n$.

8.1.2 Characteristic

Definition 8.4: Characteristic

If R is a ring, we define the **characteristic** of R, denoted by $\mathrm{ch}(R)$, in terms of the order of 1_R in the additive group $(R, +)$:

$$\mathrm{ch}(R) = \begin{cases} n & \text{if } o(1_R) = n \in \mathbb{N} \text{ in } (R, +) \\ 0 & \text{if } o(1_R) = \infty \text{ in } (R, +) \end{cases}$$

Discovery 8.2

For $k \in \mathbb{Z}$, we write $kR = 0$ to mean that $kr = 0$ for all $r \in R$. Since we have

$$kr = k(1_R r) = (k1_R)r$$

so $kR = 0$ if and only if $k1_R = 0$. Now we have the following proposition:

Proposition 8.2

Let R be a ring and $k \in \mathbb{Z}$,

1. If $\mathrm{ch}(R) = n$, then $kR = 0$ if and only if $n \mid k$;
2. If $\mathrm{ch}(R) = 0$, then $kR = 0$ if and only if $k = 0$.

Example 8.5

Each of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ has characteristic 0.

Example 8.6

For $n \in \mathbb{N}$ with $n \geq 2$, the ring $\mathbb{Z}_n$ has characteristic n.

8.2 Subrings

Lecture 23 - Friday, November 01

Definition 8.5: Subring

A subset S of a ring R is a **subring** if S is a ring itself with $1_S = 1_R$ with the same addition and multiplication.

Comment 8.3

Note that properties (2), (3), (7), and (9) are automatically satisfied. Thus, in order to show that S is a subring, we introduce the "Subring Test".

8.2.1 Subring Test

Proposition 8.3: Subring Test

1. $1_R \in S$;
2. If $s, t \in S$, then $st \in S$ and $s - t \in S$.

Comment 8.4

Note that if (2) holds, then $0 = s - s \in S$ and $-t = 0 - t \in S$.

Example 8.7: The chain of subrings

We have a chain of commutative rings:

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Example 8.8: The centre of a ring is a subring

If R is a ring, the **centre** $Z(R)$ of R is defined to be

$$Z(R) = \{z \in R : zr = rz \quad \forall\, r \in R\}$$

Note that $1_R \in Z(R)$, and if $s, t \in Z(R)$, then for all $r \in R$

$$(st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st)$$
$$(s - t)r = sr - tr = rs - rt = r(s - t)$$

By the subring test, $Z(R)$ is a subring of R.

Example 8.9: Gaussian integers

Let

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$$

Then one can show $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, called the ring of **Gaussian integers**.

8.3 Ideals

Let R be a ring and A an additive subgroup of R. Since $(R, +)$ is abelian, we have $A \lhd R$. Thus we have the additive quotient group

$$R/A = \{r + A : r \in R\}$$

with $r + A = \{r + a : a \in A\}$. Using the known properties of the cosets and quotient groups, we have the following proposition:

Proposition 8.4

Let R be a ring and A an additive subgroup of R, for $r, s \in R$, we have

1. $r + A = s + A$ if and only if $(r - s) \in A$;
2. $(r + A) + (s + A) = (r + s) + A$;
3. $0 + A = A$ is the additive identity of R/A;
4. $-(r + A) = (-r) + A$ is the additive inverse of $r + A$;
5. $k(r + A) = kr + A$ for all $k \in \mathbb{Z}$.

Since R is a ring, it is natural to ask if we could make R/A to be a ring. A natural way to define multiplication in R/A is that

$$(r + A)(s + A) = rs + A \qquad \forall\, r, s \in R \tag{*}$$

Note that we could have $r + A = r_1 + A$ and $s + A = s_1 + A$ with $r \neq r_1$ and $s \neq s_1$. Hence in order to make $(*)$ make sense, a necessary condition is

$$r + A = r_1 + A \text{ and } s + A = s_1 + A \;\Rightarrow\; rs + A = r_1 s_1 + A$$

In this case, we say the multiplication $(r + A)(s + A)$ is well-defined.

Proposition 8.5

Let A be an additive subgroup of a ring R. For $a \in A$, we define

$$Ra = \{ra : r \in R\} \quad \text{and} \quad aR = \{ar : r \in R\}$$

TFAE:

1. $Ra \subseteq A$ and $aR \subseteq A$ for every $a \in A$;

2. For $r, s \in R$, $(r + A)(s + A) = rs + A$ is well-defined in R/A.

Proof. `(1)` $\Rightarrow$ `(2)`
If $r + A = r_1 + A$ and $s + A = s_1 + A$, we wish to show that $rs + A = r_1 s_1 + A$. Since $(r - r_1) \in A$ and $(s - s_1) \in A$, by (1), we have

$$\begin{aligned} rs - r_1 s_1 &= rs - r_1 s + r_1 s - r_1 s_1 \\ &= (r - r_1)s + r_1(s - s_1) \\ &\in (r - r_1)R + R(s - s_1) \subseteq A \end{aligned}$$

Hence we have $rs + A = r_1 s_1 + A$.
`(2)` $\Rightarrow$ `(1)`
Let $r \in R$ and $a \in A$, thus we have

$$ra + A = (r + A)(a + A) = (r + A)(0 + A) = r0 + A = A$$

Thus $ra \in A$ and we have $Ra \subseteq A$. Similarly, we have $aR \subseteq A$. □

Definition 8.6: Ideal

An additive subgroup A of a ring R is an **ideal** of R if $RA \subseteq A$ and $AR \subseteq A$.
Thus a subseteq A of R is an ideal if $0 \in A$ and for $a, b \in A$ and $r \in R$, we have $a - b \in A$ and $ra, ar \in A$.

Example 8.10

If R is a ring, then $\{0\}$ and R are ideals of R.

Example 8.11

Let R be a commutative ring and $a_1, \ldots, a_n \in R$. Consider the set I generated by $a_1, \ldots, a_n$, i.e.,

$$I = \langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\}$$

Exercise: Then one can show that I is an ideal.

Lecture 24 - Monday, November 04

8.3.1 Ideal Test

Proposition 8.6: Ideal Test

1. $0_R \in A$;
2. For $a, b \in A$ and $r \in R$. $a - b \in A$ and $ar, ra \in A$.

Proposition 8.7

Let A be an ideal of a ring R. If $1_R \in A$, then $A = R$.

Proof. For every $r \in R$, since A is an ideal and $1_R \in A$, we have $r = r1_R \in A$. It follows that $R \subseteq A \subseteq R$ and hence $R = A$. □

Comment 8.5

By the above proposition, we see that an ideal is not necessarily a (sub)ring since it may not contain the unity 1_R.

Proposition 8.8

Let A be an ideal of a ring R. Then the additive quotient group R/A is a ring with the multiplication $(r + A)(s + A) = rs + A$. The unity of R/A is $(1 + A)$.

Definition 8.7: Quotient Ring

Let A be an ideal for a ring R, the ring R/A is called **quotient ring** of R by A.

Definition 8.8: Principle Ideal

Let R be a commutative ring and A an ideal of R. If $A = aR = \{ar : r \in R\} = Ra$ for some $a \in A$, we say that A is a principle ideal generated by A and denote it by $A = \langle a \rangle$.

Example 8.12

If $n \in \mathbb{Z}$, then $\langle n \rangle = n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proposition 8.9

All ideals of $\mathbb{Z}$ are of the form $\langle n \rangle$ for some $n \in \mathbb{Z}$. If $\langle n \rangle \neq \{0\}$ and $n \in \mathbb{N}$, then the generator is uniquely determined.

Proof. Let A be an ideal of $\mathbb{Z}$, if $A = \{0\}$, then $A = \langle 0 \rangle$. Otherwise, choose $a \in A$ with $a \neq 0$ such that $|a|$ is minimum. Clearly, $\langle a \rangle \subseteq A$. To prove the other inclusion, let $b \in A$ be arbitrary. By the division algorithm, we have $b = qa + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < a$. Since A is an ideal and $a, b \in A$, we have $r = b - qa \in A$ with $|r| < |a|$, which implies that $r = 0$ and $b = qa$. Thus $b \in \langle a \rangle$. It follows that $A \subseteq \langle a \rangle$ and so $A = \langle a \rangle$. □

8.4 Isomorphism Theorems

Definition 8.9: Ring Homomorphism

Let R and S be rings. A mapping $\theta : R \to S$ is a **ring homomorphism** if for all $a, b \in R$,

1. $\theta(a+b) = \theta(a) + \theta(b)$;
2. $\theta(ab) = \theta(a)\theta(b)$;
3. $\theta(1_R) = 1_S$.

Comment 8.6

In group homomorphism, we may derive (3) from (2). However, in ring homomorphisms, condition (2) does not imply (3) since we no longer have cancellation [$\theta(1_R) \in S$ does not necessarily have a multiplicative inverse].

Example 8.13

Consider mapping $k \to [k]$ from $\mathbb{Z}$ to $\mathbb{Z}_n$. This is clearly an onto ring homomorphism.

Example 8.14

If R_1 and R_2 are rings, the projection $\pi_1 : R_1 \times R_2 \to R_1$ defined by $\pi_1(r_1, r_2) = r_1$ is an onto homomorphism. Similarly, $\pi_2 : R_1 \times R_2 \to R_1$ defined by $\pi_2(r_1, r_2) = r_2$ is also an onto homomorphism.

Proposition 8.10

Let $\theta : R \to S$ be a ring homomorphism and $r \in R$:

1. $\theta(0_R) = 0_S$;
2. $\theta(-r) = -\theta(r)$;
3. $\theta(kr) = k\theta(r)$ for all $k \in \mathbb{Z}$;
4. $\theta(r^n) = \theta(r)^n$ for all $n \in \mathbb{N} \cup \{0\}$;
5. If $u \in \mathbb{R}^*$ (u is called a **unit** of R), thus $\theta(u^k) = \theta(u)^k$ for all $k \in \mathbb{Z}$.

Proof. **Exercise:**

□

Definition 8.10: Ring Isomorphism

A mapping of rings $\theta : R \to S$ is a **ring isomorphism** if θ is a ring homomorphism and a bijection. In this case, we say R and S are isomorphic and denote it as

$$R \cong S$$

Exercise: Let $\theta : R \to S$ be a bijection of rings with $\theta(rr') = \theta(r)\theta(r')$ for all $r, r' \in R$. Write $\theta(1_R) = e$, prove that $se = es$ for all $s \in S$, hence condition (3) in ring homomorphism can be omitted in this case.

Lecture 25 - Wednesday, November 06

Definition 8.11: Kernel and Image

Let $\theta : R \to S$ be a ring homomorphism, the **kernel** of θ is defined by

$$\ker \theta = \{r \in R : \theta(r) = 0\} \subseteq R$$

and the **image** of θ is defined by

$$\text{im } \theta = \theta(R) = \{\theta(r) : r \in R\} \subseteq S$$

We have learnt from group theory that $\ker \theta$ and $\text{im } \theta$ are additive subgroups of R ans S respectively.

Proposition 8.11

Let $\theta : R \to S$ be a ring homomorphism, then

1. $\text{im } \theta$ is a subring of S;
2. $\ker \theta$ is a ideal of R.

Proof. [Part 1]: Since $\text{im } \theta = \theta(R)$ is an additive subgroup of S, it suffices to show that $\theta(S)$ is closed under multiplication and $1_S \in \theta(R)$. We have $1_S = \theta(1_R) \in \theta(R)$. Additionally, if $s_1 = \theta(r_1)$ and $s_2 = \theta(r_2)$, then

$$s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) \in \theta(R)$$

By the subring test, $\theta(R)$ is a subring of S.
[Part 2]: Since $\ker \theta$ is an additive subgroup of R, it suffices to show $ra, ar \in \ker \theta$ for all $r \in R$ and $a \in \ker \theta$. If $r \in R$, and $a \in \ker \theta$, then

$$\theta(ra) = \theta(r)\theta(a) = \theta(r) \cdot 0 = 0$$

Thus $ra \in \ker \theta$. Similarly, $ar \in \ker \theta$, thus $\ker \theta$ is an ideal of R. □

8.4.1 First Isomorphism Theorem

Theorem 8.1: First Isomorphism Theorem

Let $\theta : R \to S$ be a ring homomorphism, we have

$$R/\ker \theta \cong \text{im } \theta$$

Proof. Let $A = \ker \theta$, since A is an ideal, R/A is a ring. Define the ring map

$$\bar{\theta} : R/A \to \text{im } \theta$$

by $\bar{\theta}(r+A) = \theta(r)$ for all $r + A \in R/A$. Note that

$$r + A = s + A \iff r - s \in A \iff \theta(r-s) = 0 \iff \theta(r) = \theta(s)$$

Thus $\bar{\theta}$ is well-defined and one-to-one. Also, $\bar{\theta}$ is clearly onto. We leave the proof for $\bar{\theta}$ is a ring homomorphism as an exercise. It follows that $\bar{\theta}$ is a ring isomorphism and we are done. □

Discovery 8.3

Let A and B be two subsets of a ring R, if both A and B are subrings, then $A \cap B$ is the largest subring contained in both A and B. To consider, the smallest subring of R containing both A and B (A and B are not necessarily subrings), we define the *sum* of $A + B$ to be

$$A + B = \{a + b : a \in A, b \in B\}$$

and then one can show the following proposition:

Proposition 8.12

If R is a ring, we have

1. If A and B are two subrings of R, then $A \cap B$ is a subring of R;
2. If A is a subring and B is an ideal of R, then $A + B$ is a subring of R;
3. If A and B are ideals of R, then $A + B$ is an ideal of R.

Proof. **Exercise.** □

8.4.2 Second Isomorphism Theorem

Theorem 8.2: Second Isomorphism Theorem

Let A be a subring and B an ideal of a ring R. Then $A + B$ is a subring of R, B is an ideal of $A + B$, $A \cap B$ is an ideal of A and

$$(A + B)/B \cong A/A \cap B$$

Proof. See A8. □

8.4.3 Third Isomorphism Theorem

Theorem 8.3: Third Isomorphism Theorem

Let A and B be ideals of a ring R with $A \subseteq B$, then B/A is an ideal in R/A and

$$(R/A)/(B/A) \cong R/B$$

Proof. See A8. □

8.4.4 Fourth Isomorphism Theorem (Correspondence Theorem)

Theorem 8.4: Fourth Isomorphism Theorem

Let R be a ring and A an ideal. There exists a bijection between the set of ideals B of R that contains A and the set of ideals of R/A.

Proof. **This was left as an exercise.**
Denote the set of ideals B of R containing A to be C and the set of ideals of R/A to be D. We also establish the map $\varphi : C \to D$ defined by

$$\varphi(B) = \{b + A : b \in B\} \subset R/A$$

Also establish the map $\pi : D \to C$ defined by

$$\pi(S) = \{s : s + A \in S\} \subset R$$

1. If $S \in D$, then

$$(\varphi \circ \pi)(S) = \{b + A : b \in \pi(S)\} \tag{1}$$
$$= \{b + A : b + A \in S\} = S \tag{2}$$

2. If $B \in C$, then

$$\begin{aligned}(\pi \circ \varphi)(B) &= \{s : s + A \in \varphi(B)\} \\ &= \{s : s + A = b + A \text{ for some } b \in B\} \\ &= \{s : s \in b + A \text{ for some } b \in B\} \supset B\end{aligned}$$

   Morover, we also know that

$$s \in b + A \quad \Rightarrow \quad s - b \in A \subseteq B \quad \Rightarrow \quad s \in B$$

   which implies that $(\pi \circ \varphi)(B) = B$.

We have now shown that φ and π establish a bijection. See more at this Math Stackexchange Post. □

8.5 Chinese Remainder Theorem

Theorem 8.5

Let A and B be ideals of R, then

1. If $A + B = R$, then $R/(A \cap B) \cong R/A \times R/B$;
2. If $A + B = R$ and $A \cap B = \{0\}$, then $R \cong R/A \times R/B$.

Proof. Notice that 2 is a direct consequence of 1, so it STP 1. Define the map $\theta : R \to R/A \times R/B$ by

$$\theta(r) = (r + A, r + B)$$

Then θ is a ring homomorphism (exercise). Also, $\ker\theta = A \cap B$. To show that θ is onto, let $(s+A, t+B) \in R/A \times R/B$ with $s, t \in R$. Since $A+B = R$, there exist $a \in A$ and $b \in B$ such that $a+b = 1$. Let $r = sb+ta$, then

$$s - r = s - sb - ta = s(1-b) - ta = sa - ta = (s-t)a \in A$$

Thus $s + A = r + A$. Similarly, we have $t + B = r + B$, thus

$$\theta(r) = (r + A, r + B) = (s + A, t + B)$$

Now by the first Isomorphism, we have our desired result. □

Example 8.15

Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. By Euclid's Lemma, we have

$$1 = mr + ns \qquad \text{for } r, s \in \mathbb{Z}$$

Then $1 \in m\mathbb{Z} + n\mathbb{Z}$ and hence $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Also, since $\gcd(m, n) = 1$, we have $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$. Hence by the Chinese Remainder Theorem, we have the following corollary:

Corollary 8.1

1. If $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, then

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

2. If $m, n \in \mathbb{Z}$ with $m, n \geq 2$ and $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$, where $\varphi(m) = |\mathbb{Z}_m^*|$ is the Euler φ-function.

Proof. Proof for 1 is simple, from 1, we have

$$\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$$

□

Comment 8.7

By the above corollary, for $[a] \in \mathbb{Z}_m$ and $[b] \in \mathbb{Z}_n$, there exists a unique $[c] \in \mathbb{Z}_{mn}$ such that $[c] = [a] \in \mathbb{Z}_m$ and $[c] = [b] \in \mathbb{Z}_n$. i.e., it is equivalent to say $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ has a unique solution $x \equiv c \pmod{mn}$.

Lecture 26 - Friday, November 08

Exercise: Combining the Third Isomorphism Theorem and the fact that all ideals of $\mathbb{Z}$ are principle, prove that all ideals of $\mathbb{Z}_n$ are principle.

Let p be a prime, we recall that one consequence of the Lagrange Theorem is that every group of order p is cyclic, i.e.,

$$G \cong C_p \cong \mathbb{Z}_p$$

We have an analogous result for rings as well:

Proposition 8.13

If R is a ring with $|R| = p$, where p is a prime, then $R \cong \mathbb{Z}_p$.

Proof. Define $\theta : \mathbb{Z}_p \to R$ by

$$\theta([k]) = k1_R$$

Note that R is an additive group and $|R| = p$, so by Lagrange's Theorem, $o(1_R) = 1$ or p. Since $1_R \neq 0$, we have $o(1_R) = p$. Thus

$$[k] = [m] \iff p \mid (k-m) \iff (k-m)1_R = 0 \iff k1_R = m1_R$$

Thus θ is well-defined and one-to-one. Also θ is a ring homomorphism (exercise). Since $|\mathbb{Z}_p| = p = |R|$, we know that θ is onto. It follows that θ is a ring isomorphism and hence $R \cong \mathbb{Z}_p$. □

Exercise: `[Hard]` What are the possible rings, say R, with $|R| = p^2$ for p is a prime.

Quiz 8.1

Let $\theta : R \to S$ be a ring homomorphism. Determine if the following statements are true or false.

(T) The image of θ is a subring of S.

(F) The kernel of θ is an ideal of S.

(T) $R/\ker\theta \cong \operatorname{im}\theta$.

Quiz 8.2

Let I be an ideal of a ring R. Determine if the following statements are true or false.

(T) If $r \in R$ then $rI \subseteq I$.

(F) For any $r \in R$, we have $rI = Ir$.

(F) If $0 \in I$, then $I = R$.

Quiz 8.3

Determine if the following statements are true or false.

(T) Let A be a subring and B an ideal of a ring R. Then $A \cap B$ is an ideal of A.

(T) Let A and B be ideals of a ring R. If $A \subseteq B$, then $(R/A)/(B/A) \cong R/B$.

9 Commutative Rings

9.1 Integral Domains and Fields

Definition 9.1: Unit

Let R be a ring, we say $u \in R$ is a **unit** if u has a multiplicative inverse in R, denoted by u^{-1}. We have

$$uu^{-1} = 1 = u^{-1}u$$

Discovery 9.1

Note that if u is a unit in R and $r, s \in R$, we have

$$ur = us \implies r = s \qquad \text{and} \qquad ru = su \implies r = s$$

Comment 9.1

Let R^* denote the set of all units in R, one can show that $(R^*, \cdot)$ is a group, the **group of units of** R.

Example 9.1

Note that 2 is a unit in $\mathbb{Q}$, but it is not a unit in $\mathbb{Z}$. We have $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ and $\mathbb{Z}^* = \{\pm 1\}$.

Exercise: Consider the ring of Gaussian integers (see 8.9).

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\} \subseteq \mathbb{C}$$

One can show that $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.
Hint: Define the norm

$$N(x + yi) = x^2 + y^2$$

Prove that $N(ab) = N(a)N(b)$ and $N(a) = 1$ if and only if a is a unit.

Definition 9.2: Division Ring

A ring $R \neq \{0\}$ is a **division ring** if $R^* = R\backslash\{0\}$, i.e., every non-zero element in R is a unit in R.

Definition 9.3: Field

A commutative division ring is a **field**.

Example 9.2

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields, but not $\mathbb{Z}$.

Example 9.3: $\mathbb{Z}_n$ is a field if and only if n is a prime

We recall that the equation

$$[a][x] = [1] \pmod{n}$$

has a solution if and only if $\gcd a, n = 1$. Thus if n is a prime, then

$$\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$$

and thus $\mathbb{Z}_p$ is a field. On the other hand, if n is composite, say $n = ab$ for $1 < a, b < n$, then the non-zero congruence class $[a], [b]$ are not units in $\mathbb{Z}_n$ as there is no solution to

$$[a][x] = [1] \qquad \text{or} \qquad [b][x] = [1]$$

and hence $\mathbb{Z}_n^* \neq \mathbb{Z}_n \backslash \{0\}$. Therefore, $\mathbb{Z}_n$ is a field if and only if n is a prime.

Discovery 9.2

If R is a field, then its only ideals are $\{0\}$ and R since if $A \neq 0$ is an ideal of R, then $0 \neq a \in A$ implies that $1 = aa^{-1} \in A$. As a consequence, if we have a ring homomorphism π from a field F to a ring S, then $\ker \pi = \{0\}$ or F because $\ker \pi$ is an ideal. Hence π is either injective, or a zero map.

Exercise: [Wedderburn's little theorem]
Every finite division ring is a field.

Lecture 27 - Monday, November 11

Note that to solve $x^2 - x - 6 = 0$, we wriet $(x-3)(x+2) = 0$, which yields us the results: $x = 3$ or $x = -2$. However, in $\mathbb{Z}_6$, we have $[2][3] = [0]$, which means that if we have $[x-3][x-2] = [0]$, it does not necessarily mean that $[x] = [3]$ or $[-2]$.

Definition 9.4: Zero Divisor

Let $R \neq \{0\}$ be a ring. For $0 \neq a \in R$, we say a is a **zero divisor** if there exists $b \in \mathbb{R}$ such that $ab = 0$.

Example 9.4

In $\mathbb{Z}_6$, [2], [3], [4] are zero divisors since

$$[2][3] = [0] = [4][3]$$

Example 9.5

The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{R})$ because

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Proposition 9.1

Given a ring R, TFAE:

1. If $ab = 0 \in R$, then $a = 0$ or $b = 0$;
2. If $ab = ac \in R$ and $a \neq 0$, then $b = c$;
3. If $ba = ca \in R$ and $a \neq 0$, then $b = c$.

Proof. It suffices to prove (1) $\iff$ (2).
`[Forward direction:]` Let $ab = ac$ with $a \neq 0$, then $a(b - c) = 0$ and thus we must have $b - c = 0$, which further implies that $b = c$.
`[Backward direction:]` Let $ab = 0 \in R$, here we have two cases:

1. *Case 1*: if $a = 0$, then we are done;
2. *Case 2*: if $a \neq 0$, then we have $ab = 0 = a0$, thus by cancellation we have $b = 0$.

□

Definition 9.5: Integral Domain

A *commutative ring* $R \neq \{0\}$ is an **integral domain** if it has no zero divisor, i.e., if $ab = 0$ in R, then $a = 0$ or $b = 0$.

Example 9.6

$\mathbb{Z}$ is an integral domain.

Example 9.7

If p is a prime, then $p \mid ab$ implies that $p \mid a$ or $p \mid b$, i.e., $[a][b] = [0] \in \mathbb{Z}_p$ implies $[a] = 0$ or $[b] = [0]$. However, if $n = ab$ with $1 < a, b < n$, then $[a][b] = [0]$ with $[a] \neq [0]$ and $[b] \neq [0]$. Thus $\mathbb{Z}_n$ is an integral domain for if and only if n is a prime.

Proposition 9.2

Every field is an integral domain.

Proof. Let $ab = 0$ in a field R, we wish to show that $a = 0$ or $b = 0$. Here we have two cases:

1. *Case 1*: If $a = 0$, we are done;
2. *Case 2*: If $a \neq 0$, then a has an inverse a^{-1} in R, thus we have $b = a^{-1}ab = a^{-1}0 = 0$.

thus we have done our proof. □

Comment 9.2

Using the same proof, one can show that every subring of a field is an integral domain.

Comment 9.3

Integral domains are not necessarily fields. For instance, $\mathbb{Z}$ is an integral domain but fails to be a field.

Example 9.8

The Gaussian Ring $\mathbb{Z}[i]$ is an integral domain (**exercise**), but since $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$, it is not a field.

Proposition 9.3

Every finite integral domain is a field.

Proof. Let R be a finite integral domain and $a \in R$ with $a \neq 0$. Consider the map $\theta : R \to R$ defined by $\theta(r) = ar$. Since R is an integral domain, $ar = as$ with $a \neq 0$ implies $r = s$. Hence θ is injective, so it is surjective (by the finiteness of R). This tells us that there exists $b \in R$ such that $ab = 1$, hence R is a field (R is commutative because it is an integral domain). □

Proposition 9.4

The characteristic of any integral domain is either 0 or a prime p.

Proof. Let R be an integral domain,

1. *Case 1*: If $\mathrm{ch}(R) = 0$ we are done.;
2. *Case 2*: If $\mathrm{ch}(R) = n \in \mathbb{N}$. Note that since $R \neq \{0\}$, we have $n \neq 1$, so $\mathrm{ch}(R) = n \in \mathbb{N}\backslash\{1\}$. Suppose n is not a prime, say $n = ab$ for $1 < a, b < n$. If 1 is the unity of R, then we have

$$(a \cdot 1)(b \cdot 1) = (a \cdot b)(1 \cdot 1) = n \cdot 1 = 0$$

Since R is an integral domain, we must have $a \cdot 1 = 0$ or $b \cdot 1 = 0$, which is a contradiction.

Therefore n is either 0 or a prime p. □

Lecture 28 - Wednesday, November 13

Discovery 9.3

Let R be an integral domain with $\text{ch}(R) = p$ where p is a prime. For $a, b \in R$, we have

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + \binom{p}{p}b^p$$

Since p is a prime, we have $p \mid \binom{p}{i}$ for all $1 \leq i \leq (p-1)$. Since $\text{ch}(R) = p$, we have

$$(a+b)^p = a^p + b^p$$

9.2 Prime Ideals and Maximal Ideals

Let p be a prime and $a, b \in \mathbb{Z}$. We see in Math 135/ 145 that if $p \mid ab$, then $p \mid a$ or $p \mid b$. In other words, if $ab \in p\mathbb{Z}$, then $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Definition 9.6: Prime Ideal

Let R be a commutative ring, and ideal $P \neq R$ of R is a **prime ideal** if whenever $r, s \in R$ satisfy $rs \in P$, then $r \in P$ or $s \in P$.

Example 9.9

$\{0\}$ is a prime ideal of $\mathbb{Z}$.

Example 9.10

For $n \in \mathbb{N}$ with $n \geq 2$, $n\mathbb{Z}$ is a prime ideal if and only if n is a prime.

9.2.1 If R is a commutative ring, then an ideal P of R is a prime ideal if and only if R/P is an integral domain.

Proposition 9.5

If R is a commutative ring, then an ideal P of R is a prime ideal if and only if R/P is an integral domain.

Proof. Since R is a commutative ring, so is R/P. Note that

$$R/P \neq \{0\} \iff 0+P \neq 1+P \iff 1 \notin P \iff P \neq R$$

For $r, s \in R$, we have

$$\begin{aligned} P \text{ is a prime ideal} &\iff rs \in P \text{ implies } r \in P \text{ or } s \in P \\ &\iff (r+P)(s+P) = 0+P \text{ implies } r+P = 0+P \text{ or } s+P = 0+P \\ &\iff R/P \text{ is an integral domain} \end{aligned}$$

□

Definition 9.7: Maximal Ideal

Let R be a commutative ring. An ideal $M \neq R$ of R is a **maximal ideal** if whenever A is an ideal such that $M \subseteq A \subseteq R$, then $A = M$ or $A = R$.

Comment 9.4

Let M be a max ideal of R and $r \notin M$. Then $\langle r \rangle + M$ is an ideal (**exercise**) of R and $\langle r \rangle + M = R$.

9.2.2 If R is a commutative ring, then an ideal M of R is a maximal ideal if and only if R/M is a field.

Proposition 9.6

If R is a commutative ring, then an ideal M of R is a maximal ideal if and only if R/M is a field.

Proof. Since R is a commutative ring, so is R/M. Note that

$$R/M \neq \{0\} \iff 0 + M \neq 1 + M \iff 1 \notin M \iff M \neq R$$

In addition, for $r \in R$, note that $r \notin M$ if and only if $r + M \neq 0 + M$. Hence we have

$$\begin{aligned} M \text{ is a maximal ideal} &\iff \langle r \rangle + M = R \text{ for any } r \notin M \\ &\iff 1 \in \langle r \rangle + M \text{ for any } r \notin M \\ &\iff \text{for any } r \notin M, \exists\, s \in R \text{ s.t. } 1 + M = rs + M \\ &\iff \text{for any } r + M \neq 0 + M, \exists\, s + M \in R/M \text{ s.t. } (r + M)(s + M) = 1 + M \\ &\iff R/M \text{ is a field} \end{aligned}$$

□

Corollary 9.1

Every maximal ideal of a commutative ring is a prime ideal.

Comment 9.5

The converse of the above corollary isn't true. For instance, consider $\mathbb{Z}$, we know that $\{0\}$ is a prime ideal but fails to be a max ideal.

Example 9.11

Consider the ideal $\langle x^2+1\rangle$ in the ring $\mathbb{Z}[x]$. The map $\theta : \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined by

$$\theta(f(x)) = f(i)$$

is surjective since $\theta(a+bx) = a+bi$. One can also check that the kernel of the map is $\langle x^2+1\rangle$. By the First Isomorphism Theorem, we have

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

Recall that $\mathbb{Z}[i]$ is an integral domain but not a field, we conclude that the ideal $\langle x^2+1\rangle$ is prime, but not maximal.

9.3 Fields of Fractions

We have seen that every subring of a field is an integral domain. In fact, the converse also holds. That is, every integral domain is isomorphic to a subring of a field.

Lecture 29 - Friday, November 15

Given an integral domain R, we want to construct a field F of all "fractions" r/s from R.
Let R be an integral domain and let $D = R \setminus \{0\}$. Consider the set

$$X = R \times D = \{(r,s) : r \in R, s \in S\}$$

We say $(r,s) \equiv (r_1,s_1)$ if and only if $rs_1 = r_1 s$. One can show that this $\equiv$ is an equivalent relation (**exercise**). In particular,

1. $(r,s) \equiv (r,s)$;
2. $(r,s) \equiv (r_1,s_1)$ if and only if $(r_1,s_1) \equiv (r,s)$;
3. If $(r,s) \equiv (r_1,s_1)$ and $(r_1,s_1) \equiv (r_2,s_2)$, then $(r,s) \equiv (r_2,s_2)$.

Motivated by the case $R = \mathbb{Z}$, we now define the *fraction*, r/s, to be the equivalence class $[(r,s)]$ of the pair (r,s) on X. Let F denote the set of all these fractions, i.e.,

$$F = \left\{\frac{r}{s} : r \in R, s \in D\right\} = \left\{\frac{r}{s} : r,s \in R, s \neq 0\right\}$$

The addition and multiplication of F are defined by

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1} \qquad \text{and}$$
$$\frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

where ss_1, $rs_1 + r_1 s$, and rr_1 are all elements of R.

Comment 9.6

Note that $ss_1 \neq 0$ since R is an integral domain and $s, s_1 \neq 0$, so these operators are well-defined.

Then one can show with the above defined addition and multiplication that F becomes a field with the zero being $0/1$, the unity being $1/1$, the negative of r/s is $-r/s$. Moreover, if $r/s \neq 0$ in F, then $r \neq 0$ and thus $s/r \in F$ and we have

$$\frac{r}{s}\frac{s}{r} = \frac{rs}{sr} = \frac{rs}{rs} = \frac{1}{1} = 1$$

In addition, we have $R \cong R'$ where

$$R' = \left\{\frac{r}{1} : r \in R\right\} \subseteq F$$

Therefore we have the following theorem:

9.3.1 Field of Fractions (& Ring of Fractions)

Theorem 9.1: Field of Fractions

Let R be an integral domain, then there exists a field F consisting of fractions r/s with $r, s \in R$ and $s \neq 0$. By identifying $r = r/1$ for all $r \in R$, we can view R as a subring of F. Such F is called the **field of fractions** of R.

Discovery 9.4: Ring of Fractions

Given an integral domain R, one can generalize the above set $D = R \setminus \{0\}$ to any subset $D \subseteq R$ satisfying

1. $0 \notin D$;
2. $1 \in D$;
3. If $a, b \in D$, then $ab \in D$.

Then one can show that the corresponding set of fractions F is an integral domain containing R. Such F is called the **ring of fractions** of R over D and is denoted by $D^{-1}R$.

9.3.2 Localization

Discovery 9.5

If R is an integral domain and P is a prime ideal, take $D = R \setminus P$. Then D satisfies conditions (1)-(3) in the above discovery (**exercise**). The resulting $D^{-1}R$ is called the **localization** of R at the prime ideal P.

Quiz 9.1

Let R be a commutative ring and P an ideal of R. Determine if the following statements are true or false.

(F) P is a maximal ideal if it satisfies that for an ideal A of R with $P \subseteq A \subseteq R$, then $A = P$ or $A = R$.

(T) If R/P is an integral domain, then P is a prime ideal.

(T) If R/P is a field, then P is a maximal ideal.

(T) Every maximal ideal of R is a prime ideal.

Quiz 9.2

Let R be a ring. Determine if the following statements are true or false.

(F) If every nonzero element of R is a unit, then R is a field.

(T) If R is a field, then R is an integral domain.

(T) If R is a finite integral domain, then R is a field.

(T) $\mathbb{Z}_{11}$ is a field.

Quiz 9.3

Let R be a ring and $u \in R$ a unit. Determine if the following statements are true or false.

(T) If $r, s \in R$ satisfy $ru = su$, then $r = s$.

(F) If $R = \mathbb{Q}$, then $u \in \{\pm 1\}$.

10 Polynomial Rings

10.1 Polynomials

Definition 10.1: Polynomial

Let R be a ring and x a variable, let

$$R[x] = \left\{ f(x) = a_0 + a_1 x + \cdots + a_m x^m : m \in \mathbb{N} \cup \{0\} \text{ and } a_i \in R (0 \leq i \leq m) \right\}$$

Such $f(x)$ is called a **polynomial in x over R**. If $a_m \neq 0$, we say $f(x)$ has degree m, denoted by $\deg f = m$. We say a_m is the **leading coefficient** of $f(x)$.

Definition 10.2: Monic

If a_m, the leading coefficient, is 1, then we say $f(x)$ is **monic**.

Definition 10.3: Constant Polynomial

If $\deg f = 0$, then $f(x) = a_0 \in R \setminus \{0\}$. In this case, we say $f(x)$ is a **constant polynomial**. Note that

$$f(x) = 0 \iff a_0 = a_1 = \cdots = a_m = 0$$

We define $\deg 0 = -\infty$.

Comment 10.1

Note that $f(x) = 0$ is also a constant polynomial.

Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $g(x) = b_0 + b_1 x + \cdots + b_n b^n$ in $R[x]$ with $m \leq n$. We write $a_i = 0$ for $m + 1 \leq i \leq n$, then we can define addition and multiplication on $R[x]$ as follows:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \qquad \text{and}$$
$$f(x)g(x) = c_0 + c_1 x + \cdots + c_{m+1} x^{m+1}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$. Then one can show that under these operations,

Proposition 10.1

Let R be a ring and x a variable, then

1. $R[x]$ is a ring;
2. R is a subring of $R[x]$;
3. $Z(R[x]) = Z(R)[x]$.

Proof. [1]. **exercise**.
[2]. R is the same as the set of constant polynomials;

Lecture 30 - Monday, November 18

[3]. Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in Z(R)[x]$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n \in R[x]$, then we have

$$f(x)g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}$$

with $c_i = a_0b_i + \cdots + a_ib_0$. Since $a_i \in Z(R)$, we have $a_ib_j = b_ja_i$ for all i, j, which implies that $f(x)g(x) = g(x)f(x)$ for all $g(x) \in R(x)$. Hence we proved

$$Z(R)[x] \subseteq Z(R[x])$$

Now we wish to show the other inclusion. If $f(x) = a_0 + a_1x + \cdots + a_mx^m \in Z(R[x])$, then $bf(x) = f(x)b$ for all $b \in R \subseteq R[x]$. It follows that $a_ib = ba_i$ for all $b \in R$. Therefore we must have $a_i \in Z(R)$ and so

$$Z(R[x]) \subseteq Z(R)[x]$$

Combining both direction of inclusions we have our result. □

Discovery 10.1

Although $f(x) \in R[x]$ can be used to define a function from R to R, the polynomial is not the same as the function it defines.

Example 10.1

For instance, there are only 4 functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$, but there are infinitely many irreducible polynomials in $\mathbb{Z}_2[x]$.

Proposition 10.2

Let R be an integral domain, then

1. $R[x]$ is an integral domain;
2. If $f \neq 0$ and $g \neq 0$ in $R[x]$, then $\deg(fg) = \deg(f) + \deg(g)$ (called the **product formula**) ;
3. The units in $R[x]$ are R^*, the units in R.

Proof. Suppose $f(x) \neq 0$ and $g(x) \neq 0$ are polynomials in $R[x]$, say $f(x) = a_0 + a_1x + \cdots + a_mx^m \in Z[x]$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n \in R[x]$ with $a_m \neq 0$ and $b_n \neq 0$. Then

$$f(x)g(x) = (a_m + b_n)x^{m+n} + \cdots + a_0b_0$$

Since R is an integral domain, we have $a_m b_n \neq 0$ and thus $f(x)g(x) \neq 0$. It follows that $R[x]$ is an Integral domain. Moreover, we see

$$\deg(fg) = m + n = \deg(f) + \deg(g)$$

Thus (1) and (2) follow. For statement (3), let $u(x) \in R[x]$ be a unit with the inverse $v(x)$. Since $u(x)v(x) = 1$ by (2), we have

$$\deg(u) + \deg(v) = \deg(1) = 0$$

and we have $u(x) \neq 0$ and $v(x) \neq 0$. Hence we must have $\deg(u) = \deg(v) = 0$, which implies that u and v are units in R and hence

$$R[x]^* \subseteq R^*$$

Since we must have $R^* \subseteq R[x]^*$ as a consequence of $R \subseteq R[x]$, we conclude that $R[x]^* = R^*$. □

Example 10.2

Note that in $\mathbb{Z}_4[x]$, we have $2x \cdot 2x = 4x^2 = 0$. Thus

$$\deg(2x) + \deg(2x) \neq \deg(2x \cdot 2x)$$

Hence the product formula only applies to integral domain.

Result 10.1

To extend the product formula to 0, we define $\deg(0) = -\infty$.

10.2 Polynomials over a Field

In this section, we will consider $F[x]$ with F being a field and explore its analogies with the set of integers $\mathbb{Z}$.

Definition 10.4: Divide

Let F be a field and $f(x), g(x) \in F[x]$, we say $f(x)$ **divides** $g(x)$, denoted by $f(x) \mid g(x)$, if there exists $h(x) \in F[x]$ such that $g(x) = f(x)h(x)$.

Proposition 10.3

Let F be a field and $f(x), g(x), h(x) \in F[x]$.

1. If $f(x) \mid g(x)$ and $g(x) \mid h(x)$, then $f(x) \mid h(x)$;
2. If $f(x) \mid g(x)$ and $f(x) \mid h(x)$, then $f(x) \mid (g(x)u(x) + h(x)v(x))$ for any $u(x), v(x) \in F[x]$.

Proof. **exercise**. □

Discovery 10.2

For $a, b \in \mathbb{Z}$, we know that we have $a = \pm b$. If we have $a, b \geq 0$ then we could conclude that $a = b$. Similarly, if $f(x), g(x) \in F[x]$ with $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then we know $f(x) = sg(x)$ for some $s \in F^*$. In order to be able to conclude $f(x) = g(x)$, we need both of them to be monic. Therefore, we have the following proposition:

Proposition 10.4

Let F be a field and $f(x), g(x) \in F[x]$ are monic polynomials. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.

Lecture 31 - Wednesday, November 20

Proof. Since $f(x) \mid g(x)$ and $g(x) \mid f(x)$, we have $g(x) = r(x)f(x)$ and $f(x) = s(x)g(x)$ for some $r(x), s(x) \in F[x]$. Then

$$f(x) = s(x)r(x)f(x)$$

Therefore, by proposition (10.2), we have

$$\deg(f) = \deg(s) + \deg(r) + \deg(f)$$

which implies that $\deg(r) + \deg(s) = 0$. Thus $f(x) = sg(x)$ for some $r \in F$. Since both f and g are monic, we must have $s = 1$ and hence $f(x) = g(x)$. □

10.2.1 Division Algorithm

Proposition 10.5: Division Algorithm

Let F be a field and $f(x), g(x) \in F[x]$ with $f(x) \neq 0$. Then there exists a unique $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x)f(x) + r(x)$$

with $\deg(r) < \deg(f)$.

Comment 10.2

Note that for the case $r(x) = 0$, we have

$$\deg(r) = -\infty < \deg(f) \neq 0$$

Proof. We first prove by induction that such $q(x)$ and $r(x)$ exist. Write $m = \deg(f)$ and $n = \deg(g)$. If $n < m$, then $g(x) = 0f(x) + g(x)$. Suppose that $n \geq m$ and the result holds for all $g(x) \in F[x]$ with $\deg(g) < n$. Write

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$

with $a_m \neq 0$ and

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n$$

Since F is a field, a_m^{-1} exists. Consider

$$\begin{aligned} g_1(x) &= g(x) - b_n a_m^{-1} x^{n-m} f(x) \\ &= 0 \cdot x^n + (b_{n-1} - b_n a_m^{-1} a_{m-1} x^{n-1} + \cdots) \end{aligned}$$

Since $\deg g_1 < n$, by induction hypothesis, there exists $q_1(x), r_1(x) \in F[x]$ such that

$$g_1(x) = q_1(x) f(x) + r_1(x)$$

with $\deg(r_1) < \deg(f)$. It follows that

$$\begin{aligned} g(x) &= g_1(x) + b_n a_m^{-1} x^{n-m} f(x) \\ &= (q_1(x) + b_n a_m^{-1} x^{n-m}) f(x) + r_1(x) \end{aligned}$$

To prove uniqueness, suppose that we also have $g(x) = q'(x) f(x) + r'(x)$ with $\deg(r') < \deg(f)$. Then

$$r(x) - r'(x) = (q'(x) - q(x)) f(x)$$

If $q'(x) - q(x) \neq 0$, we get

$$\deg(r - r') = \deg(q' - q) + \deg(f) \geq \deg(f)$$

which leads to a contradiction since $\deg(r - r') < \deg(f)$. Thus we must have $q(x) = q'(x)$ and $r(x) = r'(x)$. □

Proposition 10.6

Let F be a field and $f(x), g(x) \in F[x]$ and $f(x), g(x) \neq 0$, then there exists $d(x) \in F[x]$ which satisfies the following conditions:

1. $d(x)$ is monic;
2. $d(x) \mid f(x)$ and $d(x) \mid g(x)$.
3. If $e(x) \mid f(x)$ and $e(x) \mid g(x)$, then $e(x) \mid d(x)$;
4. $d(x) = u(x) f(x) + v(x) g(x)$ for some $u(x), v(x) \in F[x]$.

Proof. Consider the set

$$X = \{u(x) f(x) + v(x) g(x) : u(x), v(x) \in F[x]\}$$

Since $f(x) \in X$, the set X contains non-zero polynomials and thus contains monic polynomials. Among all monic polynomials in X, choose $d(x) = u(x) f(x) + v(x) g(x)$ of minimal degree. Thus (1) and (4) are immediately satisfied. For (3), since $d(x) = u(x) f(x) + v(x) g(x)$, a linear combination of $f(x)$ and $g(x)$, then if $e(x) \mid f(x)$ and $e(x) \mid g(x)$, we must also have $e(x) \mid d(x)$. It remains to prove (2), by the division

algorithm, we write $f(x) = q(x)d(x) + r(x)$ with $\deg r < \deg d$, then

$$\begin{aligned} r(x) &= f(x) - q(x)d(x) \\ &= f(x) - q(x)(u(x)f(x) + v(x)g(x)) \\ &= (1 - q(x)u(x))f(x) - (q(x)v(x))g(x) \end{aligned}$$

Note that if $r(x) \neq 0$, write $c \neq 0$ to be the leading coefficient of $r(x)$. Since F is a field, the above expression of $r(x)$ shows that $c^{-1}r(x)$ is a monic polynomial of X with

$$\deg(c^{-1}r) = \deg r < \deg d$$

which contradicts the choice of $d(x)$. Thus $r(x) = 0$ and we have $d(x) \mid f(x)$. Similarly, we may also show that $d(x) \mid g(x)$ and thus (2) holds. □

Discovery 10.3

Notice that if both $d(x)$ and $d_1(x)$ satisfy the above conditions, then $d(x) \mid d_1(x)$ and $d_1(x) \mid d(x)$. Since both of them are harmonic, we have $d(x) = d_1(x)$.

Lecture 32 - Friday, November 22

Definition 10.5: GCD

We call the abvoe $d(x)$ the **greatest common divisor** of $f(x)$ and $g(x)$, denoted by

$$d(x) = \gcd(f(x), g(x))$$

We recall that $p \in \mathbb{Z}$ is a prime if $p \geq 2$ and whenever $p = ab$ with $a, b \in \mathbb{Z}$, then $a = \pm 1$ or $b = \pm 1$.

Comment 10.3

Note that ± 1 are the unites of $\mathbb{Z}$.

Definition 10.6: Irreducible

If F is a field, a polynomial $\ell(x) \neq 0$ is **irreducible** if $\deg \ell \geq 1$ and whenever $\ell(x) = \ell_1(x)\ell_2(x)$ in $F[x]$, we have

$$\deg \ell_1 = 0 \quad \text{or} \quad \deg \ell_2 = 0$$

Definition 10.7: Reducible

Polynomials that are not irreducible are **reducible**.

Example 10.3

If $\ell(x) \in F[x]$ satisfies $\deg \ell = 1$, then $\ell(x)$ is irreducible.

Example 10.4

One can show that if $\deg f = 2$ or 3, then f is irreducible if and only if $f(d) \neq 0$ for any $d \in F$.

Proof. See HW10. □

Example 10.5

Let $\ell(x), f(x) \in F[x]$. If $\ell(x)$ is irreducible and $\ell(x) \nmid f(x)$, then $\gcd(\ell(x), f(x)) = 1$.

Proposition 10.7

Let F be a field and $f(x), g(x) \in F[x]$, if $\ell(x) \in F[x]$ is irreducible and $\ell(x) \mid f(x)g(x)$, then $\ell(x) \mid f(x)$ or $\ell(x) \mid g(x)$.

Proof. Suppose we have $\ell \mid f(x)g(x)$. If $\ell(x) \mid f(x)$, we are done. Otherwise if $\ell(x) \nmid f(x)$, then

$$d(x) := \gcd(\ell(x), f(x)) = 1$$

Hence we have

$$1 = \ell(x)u(x) + f(x)v(x)$$

for some $u(x), v(x) \in F[x]$. Then

$$g(x) = g(x)\ell(x)u(x) + g(x)f(x)v(x)$$

which implies that $\ell(x) \mid g(x)$. □

Discovery 10.4

Let $f_1(x), \ldots, f_n(x) \in F[x]$ and let $\ell(x) \in F[x]$ be irreducible. If

$$\ell(x) \mid f_1(x)f_2(x)\cdots f_n(x)$$

Then we know by the above proposition that $\ell(x) \mid f_i(x)$ for some $i \in [n]$.

10.2.2 Unique Factorization Theorem

Theorem 10.1: Unique Factorization Theorem

Let F be a field and $f(x) \in F[x]$ with $\deg f \geq 1$, then we can write

$$f(x) = c\ell_1(x)\ell_2(x)\cdots\ell_m(x)$$

where $c \in F^*$ and $\ell_i(x)$ are monic irreducible polynomials. This factorization is unique up to the order of ℓ_i.

Exercise: Use the above theorem to prove that there are infinitely many polynomials in $F[x]$ (See Chapter 11 Exercise 11.21).

Comment 10.4

Recall that in $\mathbb{Z}$, all ideals are of the form $\langle n \rangle = n\mathbb{Z}$. If $n \in \mathbb{N}$, then n is unique.

Lecture 33 - Monday, November 25

Proposition 10.8

Let F be a field. Then all ideals of $F[x]$ are of the form

$$\langle h(x) \rangle = h(x)F[x]$$

for some $h(x) \in F[x]$. If $h(x) \neq 0$ and is monic, then the generator is uniquely determined.

Proof. Let A be an ideal of $F[x]$. If $A = \{0\}$, then $A = \langle 0 \rangle$. Else if $A \neq \{0\}$, then it contains a monic polynomial (since F is a field, if $f \in A$ with leading coefficient a, then $a^{-1}f \in A$ is monic). Among all the monic polynomials in A, we choose $h(x) \in A$ with the minimal degree. Then

$$\langle h(x) \rangle \subseteq A$$

On the other hand, let $f(x) \in A$. By the division algorithm, we have

$$f(x) = q(x)h(x) + r(x)$$

with $q(x), r(x) \in F[x]$ and $\deg r < \deg h$. If $r(x) \neq 0$, let $u \neq 0$ be its leading coefficient. Since A is an ideal and $f(x), h(x) \in A$, we have

$$u^{-1}r(x) = u^{-1}(f(x) - q(x)h(x)) = u^{-1}f(x) - u^{-1}q(x)h(x) \in A$$

which is a monic polynomial in A with $\deg(u^{-1}r) < \deg h$, contradicting our choice for h. Thus we must have $r(x) = 0$, and $f(x) = q(x)h(x)$. It follows that $f(x) \in \langle h(x) \rangle$ and hence $A = \langle h(x) \rangle$. □

Comment 10.5

In $\mathbb{Z}$, when we divide an integer by n, the remainder is $0 \leq r < n$. i.e., $r \in [n-1]$. Then we have

$$\begin{aligned}\mathbb{Z}_n &= \mathbb{Z}/\langle n\rangle = \{[0],[1],\ldots,[n-1]\}\\ &= \{0+\langle n\rangle, 1+\langle n\rangle, \ldots, (n-1)+\langle n\rangle\}\end{aligned}$$

Similarly, in $F[x]$, when we divide a polynomial by $h(x)$ of degree n, then the remainder $r(x)$ satisfy $\deg r < \deg h$. i.e.,

$$r(x) = a_0 + a_1 x + \cdots a_{m-1} r^{m-1} \in F[x]$$

Then we have

$$\begin{aligned}F[x]/\langle h(x)\rangle &= \{a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + \langle h(x)\rangle : a_i \in F\}\\ &= \{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} : a_i \in F \text{ and } h(t) = 0\}\end{aligned}$$

Result 10.2

Let $A \neq \{0\}$ be an ideal of $F[x]$, by the above proposition, we can write $A = \langle h(x)\rangle$ for a unique monic polynomial $h(x) \in F[x]$. Suppose that $\deg h = m \geq 1$. Consider the quotient ring

$$R = F[x]/A$$

and thus

$$R = \{\overline{f}(x) = f(x) + A : f(x) \in F[x]\}$$

Write $t = \overline{x} = x + A$. Then by the division algorithm, one can show that

$$R = \overline{a_0} + \overline{a_1}t + \cdots + \overline{a_{m-1}}t^{m-1} : \overline{a_i} \in F$$

Consider the map $\theta : F \to R$ given by $\theta(a) = \overline{a}$. Since θ is not the zero map and $\ker\theta$ is an ideal of F, we have $\ker(\theta) = \{0\}$. Thus θ is a one-to-one ring homomorphism. Since $F \cong \theta(F)$, by identifying F with $\theta(F)$, we can write

$$R = a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} : a_i \in F, \quad \text{where } h(t) = 0$$

Note that in R, we have **exercise**

$$a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} = b_0 + b_1 t + \cdots + b_{m-1}t^{m-1} \iff a_i = b_i \ \forall\, i$$

Theorem 10.2

Let F be a field and let $h(x) \in F[x]$ be monic with $\deg h = m \geq 1$, then the quotient ring $R = F[x]/\langle h(x)\rangle$ is given by

$$a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} : a_i \in F, \quad \text{where } h(t) = 0$$

in which an element of R can be uniquely represented in the above form.

Example 10.6

Consider the ring $\mathbb{R}[x]$. Let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. By above proposition, we have

$$\begin{aligned} R[x]/\langle x^2+1\rangle &= \{a + bt : a, b \in \mathbb{R} \text{ and } t^2 + 1 = 0\} \\ &\cong \{a + bi : a, b \in \mathbb{R} \text{ and } i^2 = -1\} \end{aligned}$$

We recall that $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ is a field if and only if n is a prime.

Proposition 10.9

Let F be a field and $h(x) \in F[x]$ with $\deg h \geq 1$, TFAE:

1. $F[x]/\langle h(x)\rangle$ is a field;
2. $F[x]/\langle h(x)\rangle$ is an integral domain;
3. $h(x)$ is irreducible in $F[x]$.

Example 10.7

Since $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$ which is a field, the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$.

Example 10.8

Consider $x^3 + x + 1$ in $\mathbb{Z}_2$. We note that it has no root in $\mathbb{Z}_2$, hence is irreducible. Thus

$$\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle = \{a + bt + ct^2 : a, b, c \in \mathbb{Z}_2 \text{ and } t^3 + t + 1 = 0\}$$

is a field of 8 elements, denoted as $\mathbb{F}_8$.

Comment 10.6

$\mathbb{F}_8$ is not the same as $\mathbb{Z}_8$ since $\mathbb{Z}_8$ is not a field.

Lecture 34 - Wednesday, November 27

Proof. This is the proof for proposition (10.9).
Write $A = \langle h(x)\rangle$.

1. `[1]` $\Rightarrow$ `[2]`:
   A field is an integral domain.

2. [2] $\Rightarrow$ [3]:
If $h(x) = f(x)g(x)$ with $f(x), g(x) \in F[x]$, then

$$(f(x) + A)(g(x) + A) = f(x)g(x) + A = h(x) + A = 0 + A \in F[x]/A$$

By (2), we know that either $f(x) + A = 0 + A$ or $g(x) + A = 0 + A$. i.e., either $f(x) \in A$ or $g(x) \in A$. If $f(x) \in A = \langle h(x) \rangle$, then $f(x) = q(x)h(x)$ for some $q(x) \in F[x]$. Then $h(x) = f(x)g(x) = q(x)h(x)g(x)$. Since $F[x]$ is an integral domain, this implies that $q(x)g(x) = 1$, which gives $\deg g = 0$. Similarly, if $g(x) \in A$, then $\deg f = 0$. Thus $h(x)$ is irreducible in $F[x]$.

3. [3] $\Rightarrow$ [1]:
Note that $F[x]/A$ is a commutative ring. Thus to show it is a field, STP that every non-zero element of $F[x]/A$ has an inverse. Let $f(x) + A \neq 0 + A$ with $f(x) \in F[x]$. Then $f(x) \in A$ and hence $h(x) \nmid f(x)$. Since $h(x)$ is irreducible, we have $\gcd(f(x), h(x)) = 1$. By proposition (10.6), we know that there exists $u(x), v(x) \in F[x]$ such that $1 = u(x)f(x) + v(x)h(x)$. Thus

$$(u(x) + A)(f(x) + A) = 1 - v(x)h(x) + A = 1 + A$$

It follows that $f(x) + A$ has an inverse in $F[x]/A$ and hence $F[x]/A$ is a field.

□

10.3 Analogies between $\mathbb{Z}$ and $\mathbb{F}[x]$

	$\mathbb{Z}$	$F[x]$
Elements	m	$f(x)$
Size	$\lvert m \rvert$ = absolute value	$\deg f$
Units	$\{\pm 1\}$	$F^* = F \setminus \{0\}$
	$\mathbb{Z} \setminus \{0\} = \pm\mathbb{N}$	$F \setminus \{0\} = F^*$ $\{h :$ monic $\}$
Unique factorization	$m = \pm 1 \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, p_i prime	$f(x) = c\ell_1^{\beta_1} \cdots \ell_s^{\beta_s}$, ℓ_i monic irreducible
Ideals	$\langle n \rangle$, unique if $n \in \mathbb{N}$ $\mathbb{Z}/\langle n \rangle$ is a field iff n prime	$\langle h(x) \rangle$, unique if h monic $F[x]/\langle h(x) \rangle$ is a field iff h irreducible

Quiz 10.1

Let R be a ring and x a variable. Let $R[x]$ denote all polynomials in x over R. Determine if the following statements are true or false.

(T) R is a subring of $R[x]$.

(T) If R is an integral domain, then $R[x]$ is an integral domain.

(F) The units of $R[x]$ are the same as the units of R.

(T) Let $R = \mathbb{R}$, the set of real numbers. If $f, g \in R[x] \setminus \{0\}$, then $\deg(fg) = \deg(f) + \deg(g)$.

Quiz 10.2

Let F be a field and x a variable. Let $F[x]$ denote all polynomials in x over F. Determine if the following statements are true or false.

(T) If $f(x), g(x) \in F[x]$ are monic, and $f(x) \mid g(x) = g(x) \mid f(x)$ then $f(x) = g(x)$.

(T) If $f(x) \in F[x]$ is a unit, then $\deg(f) = 0$.

(T) All ideals of $F[x]$ are of the form $\langle h(x) \rangle$. If $h(x)$ is monic, then $h(x)$ is uniquely determined.

(T) If $l(x) \neq 0$ in $F[x]$ is irreducible, then $F[x]/\langle l(x) \rangle$ is an integral domain.

Comment 10.7

Examinable contents end here.

---

11 Not Examinable Fun Stuff

11.1 Fermat's Last Theorem in $F[x]$

We recall Fermat's Last Theorem, which states that for $n \geq 3$, the equation

$$x^n + y^n = z^n$$

has no non-trial solution in $\mathbb{Z}$.

Let F be a field and $n \in \mathbb{N}$ with $n \geq 3$. Consider the equation

$$f(x)^n + g(x)^n = h(x)^n$$

with $f(x), g(x), h(x) \in F[x]$. We say (f, g, h) is *non-trivial* if $\deg(f), \deg g, \deg h \geq 1$. Also, we say a solution (f, g, h) is **coprime** if

$$\gcd(f, g) = \gcd(f, h) = \gcd(g, h) = 1$$

Proposition 11.1

Let F be a field with $\mathrm{ch}(F) = 0$ and $n \in \mathbb{N}$ with $n \geq 3$. There is no non-trivial coprime solution for the equation

$$f(x)^n + g(x)^n = h(x)^n$$

with $f(x), g(x), h(x) \in F[x]$.

Proof. SFAC we have a non-trivial solution. WLOG suppose

$$\deg f = \deg h \geq \max\{\deg g, 1\}$$

Write $f'(x) = df/dx$. Since we have $f^n + g^n = h^n$, by taking the derivatives, we have

$$nf^{n-1}f' + ng^{n-1}g' = nh^{n-1}h'$$

Since $\mathrm{ch}(F) = 0$, we have $n \neq 0$. By cancelling n and multiplying both sides by h, we have

$$f^{n-1}f'h + g^{n-1}g'h = h^n h' = (f^n + g^n)h'$$

It follows that

$$f^{n-1}(f'h - fh') = g^{n-1}(gh' - g'h)$$

Since $\gcd(f, g) = 1$, we have $f^{n-1} \mid (gh' - g'h)$. Thus

$$(n-1) \cdot \deg f \leq \deg g + (\deg h - 1)$$

Since $\deg f = \deg h \geq \deg g$, we have

$$(n-2) \cdot \deg f \leq \deg g - 1$$

which gives a contradiction if $n \geq 3$. Thus there is no non-trivial coprime solution of $f^n + g^n = h^n$ in

$F[x]$. □

Lecture 35 - Friday, November 29

11.2 Prime Number Theorem and Riemann Hypothesis

Definition 11.1: $\pi(x)$

Define $\pi(x)$ to be the number of prime numbers smaller or equal to x.

11.2.1 Conjecture of Gauss

We have

$$\pi(x) \sim \mathrm{li}(x) \int_2^x \frac{dt}{\log t}$$

The probability that a number is a prime is $\dfrac{1}{\log x}$.

Example 11.1

For example, for $n \in \mathbb{N}$ with $1 \leq n \leq e^{100}$, about 1% of them are primes.

Definition 11.2: Riemann Zeta Function

For $s \in \mathbb{C}$, the **Riemann zeta function** is defined to be

$$\begin{aligned}\zeta(s) = \sum_{n\in\mathbb{N}} \frac{1}{n^s} &= \prod_{p:\text{prime}} \left(1 - \frac{1}{p^2}\right)^{-1} \\ &= \prod_{p:\text{prime}} \left(1 + \frac{1}{p^2} + \frac{1}{p^{2s}} + \cdots\right)\end{aligned}$$

Comment 11.1

- $\zeta(s)$ converges absolutely for $\mathrm{Re}(s) > 1$.
- $\zeta(s)$ can be extended to the whole $\mathbb{C}$.

11.2.2 Riemann Hypothesis

Theorem 11.1

There is no non-trivial zero for $\mathrm{Re}(s) > \dfrac{1}{2}$.

Theorem 11.2: Prime Number Theorem (Hadammard, de la Vallée Poussin)

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

$$\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{(\log x)^n}\right)$$

Comment 11.2

Assuming Riemann Hypothesis, we have

$$\pi(x) = \mathrm{li}(x) + O\left(x^{\frac{1}{2}+\varepsilon}\right)$$

for any $\varepsilon > 0$.

Let's consider the Prime Number Theorem in $\mathbb{Z}_p[x]$ for $f(x) \in \mathbb{Z}_p[x]$, define

$$|f(x)| = p^{\deg f}$$

For $s \in \mathbb{C}$, the zeta function of $\mathbb{Z}_p[x]$ is

$$\zeta_p(s) = \sum_{f:\text{monic}} \frac{1}{|f|^s} = \prod_{\ell:\text{monic, irred}} \left(1 - \frac{1}{|\ell|^s}\right)^{-1}$$

Note that

$$\left|\{f \in \mathbb{Z}_p[x] : \text{monic, } \deg f = d\}\right| = p^d$$

Hence

$$\zeta_p(s) = \sum_{d=0}^{\infty} \frac{p^d}{p^{ds}} = \sum_{d=0}^{\infty} \left(p^{1-s}\right)^d = \frac{1}{1-p^{1-s}}$$

Using this, one can prove that

$$\begin{aligned}\pi_p(x) &= \left|\{\ell : \text{monic, irreducible, } |\ell| \le x\}\right| \\ &= \frac{p}{1-p} \cdot \frac{x}{\log_p x} + O\left(x^{\frac{1}{2}+\varepsilon}\right)\end{aligned}$$

for any $\varepsilon > 0$. This suggests that Riemann Hypothesis also holds in $\mathbb{Z}_p[x]$.

11.3 Taylor Series

For $F(t) \in \mathbb{Z}[t]$ and $a \in \mathbb{Z}$,

$$F(t) = \sum_{i=0}^{\infty} a_i (t-a)^i \qquad \text{with} \qquad a_i = \frac{F^{(i)}(a)}{i!}$$

Let $G_x(t) \in (\mathbb{Z}_p[x])[t]$. For $b \in \mathbb{Z}_p[x]$, one may consider to write

$$G_x(t) = \sum_{i=0}^{\infty} b_i (t-b)^i \qquad \text{with} \qquad b_i = \frac{G_x^{(i)}(b)}{i!}$$

Discovery 11.1

- If $\deg G_x \geq p$, then at least one of the terms $b_i(x-b)^i$ is nonzero for $i \geq p$.
- If $i \geq p$, then
$$i! = 1 \cdot 2 \cdot 3 \cdots p \cdot (p+1) \cdots i = 0$$
which shows that b_i is not well-defined.

Result 11.1

This is a case where we would consider $\mathbb{Z}[x]$ over $F[x]$.

12 Exercises

Exercise 12.1

Let G be a group and let $Z(G)$ denote its centre. Show that if $G/Z(G)$ is cyclic then G is Abelian.

Proof. If $G/Z(G)$ is cyclic, then we know that

$$G/Z(G) = \langle gZ(G)\rangle = \langle g\rangle Z(G)$$

For any $x, y \in G$, we know that $xZ(G) = g^i Z(G)$ and $yZ(G) = g^j Z(G)$ for some i, j. Thus we have $x = g^i z$ and $y = g^j w$ for some $z, w \in Z(G)$. Therefore, we have

$$xy = g^i z g^j w = g^{i+j} zw = g^{i+j} wz = g^j w g^i z = yx$$

as desired. □

Exercise 12.2

Let G be a group and let $Z(G)$ denote its centre. Show that if the group $\mathrm{Aut}(G)$ of automorphisms of G is cyclic, then G is Abelian.

Proof. Recall that $\mathrm{inn}(G) \subset \mathrm{Aut}(G)$ is a subset of the group of automorphisms, so it is cyclic as well. Moreover, by HW4Q1, we know that

$$G/Z(G) \cong \mathrm{inn}(G)$$

thus by previous exercise, we have the desired result. □

Exercise 12.3

The dihedral group D_6, of order 12, acts by rotations and reflections on a regular hexagon. Label the vertices of the hexagon 1,2,3,4,5,6. Let P be the set of ordered pairs of vertices, so the cardinality of P is 36. Then D_6 acts on P in the obvious way: For $\sigma \in D_6$, $1 \le i, j \le 6$, $\sigma \cdot (i, j) = (\sigma(i), \sigma(j))$, where $\sigma(i)$ is the image of the vertex i under the action of σ on the vertices.

(a) Describe the orbits in P under this action of D_6.

(b) For each of the orbits of D_6 in P, fix an element in the orbit and find the order of its stabilizer in D_6.

Proof. [a] Absolute value of the difference of the two indices remain constant.
[b] Easy check. Note that some element have stablizer of size 1 and some of size 2. □

Exercise 12.4

Suppose that G is a (non-trivial) finite group and let p be the smallest prime divisor of the order of G. Show that any normal subgroup of G of order p is contained in the centre of G.

Proof. Let H denote the subgroup of G of order p. Let G act on H by conjugation, that is

$$(g, h) \mapsto ghg^{-1}$$

Note that if $h \neq 1$, then $ghg^{-1} \neq 1$. Hence for all $h \in H$ such that $h \neq 1$, $|G \cdot h|$ is bounded by $p - 1$, or $|G \cdot h| < p$. By Orbit-Stablizer Theorem, we know that

$$|G \cdot h||S(h)| = [G]$$

Recall that p is the smaller prime divide $|G|$, so we must have $|G \cdot h| = 1$. Therefore, for all $h \in H$, we have

$$ghg^{-1} = h \qquad \forall\, g \in G$$

which implies that H is contained in $Z(G)$. □

Exercise 12.5

Suppose that G is a finite *simple* group and p a prime number such that p^2 divides the order of G. Show that any proper subgroup H of G has index $(G : H)$ at least $2p$. (Hint: use a suitable group action.)

Exercise 12.6

Suppose G (finite) acts transitively on a set of n elements, prove $n \mid |G|$

In particular, show C_5, D_5, and A_5 are the only transitive subgroups of A_5 (you may assume A_5 is simple)

Exercise 12.7

Let G be a group of order 24. Assume that no Sylow subgroup of G is normal in G. Show that G is isomorphic to the symmetric group S_4. (TOO HARD FOR SUNO)

Exercise 12.8

Let G, H be groups and G', H' their commmutator subgroups. Does $G' \cong H'$ and $G/G' \cong H/H'$ imply $G \cong H$?

Exercise 12.9

Show that every finite ring contains at least one prime ideal.

Exercise 12.10

Let R be a ring and $\varphi : R \to R$ be a surjective ring homomorphism. Let φ^m denote the composition of φ with itself m times. Suppose that for some m,

$$\ker(\varphi^{m+1}) \subseteq \ker(\varphi^m)$$

prove that φ is injective. (Hint: a homomorphism is injective iff kernel is trivial)

Proof. Since we also know that $\ker(\varphi^m) \subseteq \ker(\varphi^{m+1})$, we know

$$\ker(\varphi^m) = \ker(\varphi^{m+1})$$

Therefore, suppose $\ker(\varphi^m) \neq \{0\}$, take $0 \neq a \in \ker(\varphi^m)$. Since φ is a surjective ring homomorphism, there exists $b \in R$ such that $\varphi^m(b) = a$, this gives us that $\varphi^{m+1}(b) = 0$, so

$$b \in \ker(\varphi^{m+1}) = \ker(\varphi^m)$$

which implies $a = 0$. □

Exercise 12.11

Let R be a commutative ring with a unit. Recall that the Jacobson of R, denoted as $J(R)$, is the intersection of all the maximal ideals of R. Show that $x \in J(R)$ if and only if $xy - 1$ is a unit for all $y \in R$.

Exercise 12.12

Let R be the ring $\mathbb{F}_3[x]/\langle x^2 - 1\rangle$, where $\mathbb{F}_3$ is the field $\mathbb{Z}/3\mathbb{Z}$. Show that R is isomorphic to the ring $\mathbb{F} \oplus \mathbb{F}$.

Exercise 12.13

Prove that there is no simple group of order $2^4 5^6$.

Proof. Let n_5 be the number of Sylow 5-subgroup of G. We know that $n_5 = 1$ or 16. If $n_5 = 1$, we are done, so suppose we have $n_5 = 16$. Then there is a homomorphism from $G \to S_{16}$ given by the fact that G acts on the Sylow 5-subgroups by conjugation. However, observe that

$$\nu_5(16!) = 3 < 6 = \nu_5(2^4 5^6)$$

which implies that the kernel of the homomorphism is not trivial, which is a normal subgroup of G. □

Exercise 12.14

Let G be a group of order $10989 = 3^3 \cdot 11 \cdot 37$. Prove that G contains either a normal Sylow 37-subgroup or a normal Sylow 3-subgroup.

Exercise 12.15

Let G be a group of order pqr, where $p < q < r$ are primes. Prove that G has a normal Sylow subgroup.

Proof. Let n_r be the number of Sylow r-subgroup of G. We know that $n_p \mid pq$ and $n_r \equiv 1 \pmod{r}$. Since we know that $n > p > r$, so it must be the case that $n_r = pq$ since if $n_r = 1$ then we are done. This yields us

$$pq(r-1)$$

elements of order r. Now consider the number of Sylow q-subgroups of G, say n_q. We know that $n_q \mid pr$ and $n_q \equiv 1 \pmod{q}$. Hence $n_q \in \{1, r, pr\}$. If $n_q \geq r$, then this leaves us with at most

$$\begin{aligned} pqr - pq(r-1) - r(q-1) &= pq - rq + r \\ &\leq pr - rq + r \\ &= r(p+1-q) \leq 0 \end{aligned}$$

elements of order p, which is a contradiction. Therefore, if $n_r \neq 1$, we must have $n_q = 1$. This implies that G has a normal Sylow subgroups anyways. s □

Exercise 12.16

Prove that $R[x]$ is an integral domain if and only if R is an integral domain.

Proof. `[Forward:]` We know that $R \subseteq R[x]$.
`[Backward:]` Consider the leading coefficients of $f(x), g(x) \in R[x]$. □

Exercise 12.17

Prove a prime ideal of a finite ring is maximal.

Proof. Denote P to be the prime ideal of the finite ring R, we know that R/P is an finite integral domain, thus is a field. It follows that P is a maximal ideal of R as desired. □

Exercise 12.18

T/F: The set of all nilpotents in a commutative ring is an ideal contained in the intersection of all prime ideals.

Exercise 12.19

Consider the surjective map $\theta : \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined by $\theta(f(x)) = f(i)$. Prove that the kernel $\ker\theta = \langle x^2+1 \rangle$.

Proof. We proceed by proving both directions of inclusion:
`[Backward:]` We know that for $g(x) \in \langle x^2+1 \rangle$, we have $g(i) = 0$, so we have

$$\langle x^2+1 \rangle \subseteq \ker\theta$$

`[Forward:]` Let $f(x) \in \ker\theta$, so $f(i) = 0$. By division algorithm, we know that $f(x) = q(x)(x^2+1) + r(x)$. By some simple case work we can show that $r(x) = 0$. This proves that $f(x) \in \langle x^2+1 \rangle$. Thus we have $\ker\theta \subseteq \langle x^2+1 \rangle$. □

Exercise 12.20

Let $R \neq 0$ be a commutative ring with $\text{char}(R) = p$, where p is a prime. Define $\varphi : R \to R$ by $\varphi(r) = r^p$ for all $r \in R$.

(a) Prove that φ is a ring homomorphism called the *Frobenius endomorphism* .

(b) Prove that if R is a finite field, then φ is an isomorphism, called the *Frobenius automorphism* .

Proof. `[a:]` We know that

1. $\varphi(1) = 1^p = 1$;
2. $\varphi(a + b) = a^p + b^p = \varphi(a) + \varphi(b)$. Recall $\text{ch}(R) = p$ for justification for the second equality;
3. $\varphi(ab) = a^p b^p = (ab)^p = \varphi(ab)$. Recall that we have a commutative ring.

`[b:]` We have $\varphi(r) = 0$ only if $r = 0$ since R is a finite field, thus the kernel is trivial, which implies that the homomorphism is injective, thus surjective, hence is an isomorphism. □

Exercise 12.21

Use Unique Factorization Theorem Theorem (10.1) to prove that there are infinitely many irreducible polynomials in $F[x]$.

Proof. SFAC that there are only finitely many irreducible polynomials, denoted as $\ell_1(x), \ell_2(x), \ldots, \ell_n(x)$. One can show that the polynomial defined as

$$\ell_1(x) \cdot \ell_2(x) \cdots \ell_n(x) + 1$$

is also an irreducible polynomial. □

Exercise 12.22

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

Exercise 12.23

Prove the following three conditions are equivalent (commutative ring):

1. Every ideal is finitely generated
2. If $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ is an increasing chain of ideals of R, then for some $N \in \mathbb{N}$ we have $I_n = I_m$ for all $m, n \geq N$
3. If S is a non-empty set of ideals of R, then S has a maximal element (not neccessarily a maximal ideal in all of R).

Exercise 12.24

Prove the following:

1. If $ab = a$ and $ba = b$ in a ring, show that $a^2 = a$.
2. If $ab + ba = 1$ and $a^3 = a$ in a ring, show that $a^2 = 1$.

Proof. For part 1, we have

$$a^2 = (ab)a = aba = a(ba) = ab = a$$

For part 2, we have

$$a^4 = a^2(ab + ba)a^2 = a^3ba^2 + a^2ba^3 = aba^2 + a^2ba$$

This give us that

$$a(ba + ab)a = a^4$$

which gives us that $1 = ba + ab = a^2$. □

Exercise 12.25

In the ring $\mathbb{Z}[x]$, show that the ideal $\langle x \rangle$ is prime but not maximal.

Proof. Note first that $\langle x \rangle = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$, thus for $fg \in \langle x \rangle$, we have

$$(fg)(0) = 0 \quad \Rightarrow \quad f(0) = 0 \text{ or } g(0) = 0 \quad \Rightarrow \quad f \in \langle x \rangle \text{ or } g \in \langle x \rangle$$

which proves that $\langle x \rangle$ is a prime ideal. However, it is not a maximal ideal because

$$A_n := \{f(x) \in \mathbb{Z}[x] : f(0) \in n\mathbb{Z}\}$$

is an ideal properly contains $\langle x \rangle$. □

Exercise 12.26

Determine the number of irreducible polynomials of degree 2 in $\mathbb{Z}_p[x]$ where p is prime.

Proof. We first count the number of reducible quadratics: There are p of them with repeated factors. In particular, they are in the form of

$$(x - a)^2 \qquad \text{for } a \in \mathbb{Z}_p$$

Moreover, there are $\binom{p}{2}$ of them with distinct factors, namely those in the form of

$$(x - a)(x - b) \qquad \text{for } a, b \in \mathbb{Z}_p$$

In total there are p^2 monic quadratics, thus there are

$$p^2 - p - \binom{p}{2} = p^2 - \frac{p^2 + p}{2}$$

monic irreducible polynomials. We can multiply any of these by a unit, and in $\mathbb{Z}_p$ there are $p-1$ units, so we conclude that there are in total

$$p \cdot \left(p^2 - \frac{p^2+p}{2} \right) = \frac{p(p-1)^2}{2}$$

irreducible quadratics in $\mathbb{Z}_p[x]$. □

Exercise 12.27

Find an irreducible polynomial in $\mathbb{Z}[x]$ which is reducible over $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

Proof. Consider the polynomial: $f(x) := x^2 + 2 \cdot 3 \cdot 5 \cdot 7$. □

Exercise 12.28

For a field F, prove that a finite subgroup of F^* is cyclic.

Proof. By the Structure Theorem of Finite Abelian Groups (7.3), we know that

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

where p_i's are primes not necessarily distinct. Define

$$m := \operatorname{lcm}\left(p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}\right) \leq p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$

we know that for all $g \in G$, we have $g^m = 1$. This implies that all the elements in G are roots for the polynomial $x^m - 1 = 0$. However, G has $p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$ elements, while the polynomial can have at most m roots in F, this implies that

$$m = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$

which further implies that the primes are necessarily distinct. Therefore, G is cyclic. □

Exercise 12.29

Let G be a finite group and let $H \subset G$ be a subgroup of G, with $[G : H] = 2$. Show that H contains all the elements of G of odd order.

Proof. Since $[G : H] = 2$, we know that H is a normal subgroup of G (see proposition (3.5)). Hence G/H is a well-defined quotient group. Let $x \in G$ have odd order n. Then $(xH)^n = x^n H = 1H = H$, and so the order of xH divides n. In particular, the order of xH is odd. But G/H has order $[G : H] = 2$, and since the nontrivial element of G/H has order 2 we must have $xH = H$, which shows that $x \in H$. □

Index