PMATH 347 Groups and Rings

University of Waterloo - Fall 2024

1st December 2024

Instructor: Yu-Ru Liu

LaTeX : Xing Liu

Contents

1 Groups

Lecture 1

1.1 Notations

Definition 1.1 (Notations).

$$\mathbb{N} = \{1, 2, \ldots\}$$

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

$$\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$$

$$\mathbb{R} = \text{ set of real numbers}$$

$$\mathbb{C} = \text{ set of complex numbers} = \left\{a + bi : a, b \in \mathbb{R} \text{ and } i^2 = -1\right\}$$

For $n \in \mathbb{N}$, let $\mathbb{Z}_n$ denote the set of integers modulo n,

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

where the congruence classes:

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

For the set $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$, S consists of two operations: addition and multiplication.

Matrices

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

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \quad \text{with } a_{ij} \in \mathbb{R} \ (1 \leq i, j \leq n).$$

We denote by $M_n(\mathbb{R})$, the set of all $n \times n$ matrices over $\mathbb{R}$. We can perform addition and multiplication for $M_n(\mathbb{R})$ as follows:

For $A = [a_{ij}], B = [b_{ij}] \in M_n(\mathbb{R})$, $A + B = [a_{ij} + b_{ij}]$ and $AB = [c_{ij}]$, where $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

1.2 Groups

Definition 1.2 (**Group**). Let G be a set with $*$, an operation on $G \times G$ ($* : G \times G \to G$). We say that $(G, *)$ is a **group** if it satisfies:

(1) **Closure:** If $a, b \in G$, then $a * b \in G$.

(2) **Associativity:** If $a, b, c \in G$, then $a * (b * c) = (a * b) * c$.

(3) **Identity:** $\exists e \in G$ such that $a * e = a = e * a$ for all $a \in G$. We call e an identity of G.

(4) **Inverse:** $\forall a \in G$, $\exists b \in G$ such that $a * b = e = b * a$. We call b an inverse of a.

Definition 1.3 (**Abelian Group**). A group $(G, *)$ 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 $e * a = a$ in (3) and $b * a = e$ in (4) (e and b need to be on the same side).

Proposition 1.1.

Let G be a group and $a \in G$.

(1) The identity element of G is unique.

(2) The inverse of a is unique.

Proof.

(1) If e_1 and e_2 are both identities, then $e_1 = e_1 * e_2 = e_2$.

(2) If b_1 and b_2 are both inverses of a, then

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

□

Example. The sets $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ 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.

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

For a set S, let S^* denote the subset of S containing all elements with multiplicative inverses. For example, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Then $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ are abelian groups, where the multiplicative identity is 1 and the multiplicative inverse of an element r is $\frac{1}{r}$.

Exercise: What is $\mathbb{Z}_n^*$?

Example. The set $(M_n(\mathbb{R}), +)$ is an abelian group where the additive identity is the zero matrix:

$$O = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} \in M_n(\mathbb{R})$$

and the inverse of $M = [a_{ij}] \in M_n(\mathbb{R})$ is $-M = [-a_{ij}]$.

Example. Consider $(M_n(\mathbb{R}), \cdot)$. The identity matrix is:

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \in M_n(\mathbb{R}).$$

However, since not all $M_n(\mathbb{R})$ matrices have a multiplicative inverse, $(M_n(\mathbb{R}), \cdot)$ is not a group.

Definition 1.4 (**General Linear Group**). Define the set:

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

Lecture 2

Continue from above, $GL_n(\mathbb{R})$. 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 $M_n(\mathbb{R})$.

Also, the identity matrix $I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$ satisfies $\det(I) = 1 \neq 0$ and thus $I \in GL_n(\mathbb{R})$, and $AI = A = IA$ for all $A \in GL_n(\mathbb{R})$.

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

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

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

Exercise: What is $(GL_1(\mathbb{R}), \cdot)$?

Example. Let G and H be groups. Their direct product is the set $G \times H$ with the componentwise operation defined by

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

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 by induction that if $G_1, G_2, \ldots, G_n$ are groups, then $G_1 \times \cdots \times G_n$ is also a group.

Definition 1.5 (**Notation**).
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 $g \in G$ is denoted by g^{-1}.
Also, for $n \in \mathbb{N}$, we define

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

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

Proposition 1.2. Let G be a group and $g, h \in G$. We have
(1) $\left(g^{-1}\right)^{-1} = g$.
(2) $(gh)^{-1} = h^{-1}g^{-1}$.

(3) $g^n g^m = g^{n+m}, \forall n, m \in \mathbb{Z}$.

(4) $(g^n)^m = g^{nm}, \forall n, m \in \mathbb{Z}$.

Proof.

(1) Since $g^{-1}g = 1 = gg^{-1}$, we have $\left(g^{-1}\right)^{-1} = g$.

(2) We have

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

Similarly, $(h^{-1}g^{-1})(gh) = 1$. Thus, $(gh)^{-1} = h^{-1}g^{-1}$.

□

Exercise: Prove (3) and (4) using induction and the definition of g^{-n}.

Remark (**Warning**). In general, it is NOT true that if $g, h \in G$, then $(gh)^n = g^n h^n$. For example, $(gh)^2 = ghgh$ and $g^2h^2 = gghh$.

Thus, to have $(gh)^2 = g^2h^2$, we need $gh = hg$, which is not always true.

Proposition 1.3. Let G be a group and $g, h, f \in G$. Then,

(1) They satisfy the left and the right cancellation. More precisely,

(1 - a) (Left Cancellation) if $gh = gf$, then $h = f$.

(1 - b) (Right Cancellation) if $hg = fg$, then $h = f$.

(2) Given $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$.

Proof.

(1)

(1 - a) By left-multiplying by g^{-1}, we get

$$\begin{aligned} gh = gf &\iff g^{-1}(gh) = g^{-1}(gf) \\ &\iff (g^{-1}g)h = (g^{-1}g)f \\ &\iff 1 \cdot h = 1 \cdot f \\ &\iff h = f. \end{aligned}$$

(1 - b) Similar.

(2) Let $x = a^{-1}b$. Then,

$$ax = a(a^{-1}b) = (aa^{-1})b = 1b = b.$$

If u is another solution, then $au = b = ax$. By (1 - a), we have $u = x$.

Similarly, $y = ba^{-1}$ is the unique solution for $ya = b$.

□

1.3 Symmetric Groups

Definition 1.6 (**One-to-One, Onto, Bijection**).
Let $f : X \to Y$ be a function. We say f is **one-to-one** if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$.
We say f is **onto** if $\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$.
If f is one-to-one and onto, then we say f is a **bijection**.

Definition 1.7 (**Permutation**). Given a non-empty 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.

Note. **Array notation:** $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$, where $\sigma : L \to L$.

Example. Consider the set $L = \{1, 2, 3\}$, which has the following 6 different permutations:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

where

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

indicates the bijection $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ with

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

For $n \in \mathbb{N}$, we denote $S_n = S_{\{1,2,\dots,n\}}$, the set of all permutations of $\{1, 2, \dots, n\}$.

We have seen before that $|S_3|$, the order (size) of S_3, is $6 = 3!$.

To consider the order of general S_n, we note that for a permutation $\sigma \in S_n$, there are n choices for $\sigma(1)$, $(n-1)$ choices for $\sigma(2)$, $\dots$, 1 choice for $\sigma(n)$.

Thus, we have

Proposition 1.4. $|S_n| = n!$.

Lecture 3

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

$$\sigma\tau = \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$$

given by $x \mapsto \sigma(\tau(x))$ $\forall x \in \{1, 2, \dots, n\}$. Both σ, τ are bijections so is $\sigma\tau$, thus $\sigma\tau \in S_n$.

Example. Compute $\sigma\tau$ and $\tau\sigma$ if

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Note that $\sigma\tau(1) = \sigma(\tau(1)) = \sigma(2) = 4$. Also, $\sigma\tau(2) = \sigma(\tau(2)) = \sigma(4) = 2$.
Compute the other numbers in the same way, we have

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

Also, we have

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

We note that $\sigma\tau \neq \tau\sigma$. For any $\sigma, \tau \in S_n$, we have $\sigma\tau, \tau\sigma \in S_n$. We have (exercise)

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

Also, the identity permutation $\epsilon \in S_n$ is defined as

$$\epsilon = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

Then for any $\sigma \in S_n$, we have $\sigma\epsilon = \sigma = \epsilon\sigma$.

Finally, for $\sigma \in S_n$, since it's a bijection, there exists a unique bijection $\sigma^{-1} \in S_n$, called the inverse permutation of σ, such that $\forall x, y \in \{1, 2, \dots, n\}$,

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

It follows that $\sigma(\sigma^{-1}(x)) = \sigma(y) = x$ and $\sigma^{-1}(\sigma(y)) = \sigma^{-1}(x) = y$, i.e., we have

$$\sigma\sigma^{-1} = \epsilon = \sigma^{-1}\sigma.$$

Example. Find the inverse of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$.
Note that $\sigma(1) = 4$. Thus, $\sigma^{-1}(4) = 1$, using the same method, we have

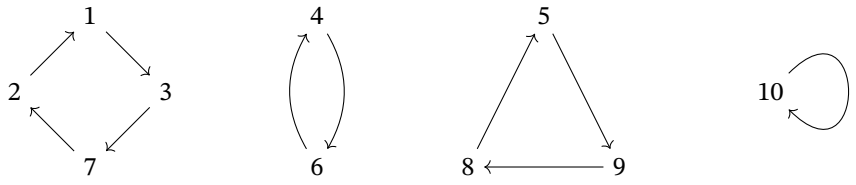
$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}.$$

From the above discussion, we have the following proposition.

Proposition 1.5. S_n is a group, called the **symmetric group of order** n.

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

Consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 9 & 4 & 2 & 5 & 8 & 10 \end{pmatrix} \in S_{10}$. If we represent the action of σ "geometrically", we obtain



Thus, σ can be composed into one 4-cycle (1 3 7 2), one 2-cycle (4 6), one 3-cycle (5 9 8), and one 1-cycle (10).

(We usually do not write 1-cycle.)

Note that these cycles are pairwise disjoint, and we have

$$\sigma = (1\,3\,7\,2)(4\,6)(5\,9\,8).$$

We can also write

$$\sigma = (4\,6)(5\,9\,8)(1\,3\,7\,2),$$

or

$$\sigma = (6\,4)(9\,8\,5)(7\,2\,1\,3).$$

Although the decomposition of cycle rotation is **NOT** unique, the individual cycle is unique. One can prove the following theorem.

Theorem 1.6 (**Cycle Decomposition Theorem**). If $\sigma \in S_n$, write $\sigma \neq \epsilon$, 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 (disjoint cycles are unique, but the order does not matter).

Exercise: Prove this theorem.

Convention: Every permutation in S_n can be regarded as a permutation in S_{n+1} by fixing the number $(n+1)$.

Thus,

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

1.4 Cayley Tables

For a finite group G, defining 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. Such a table is a Cayley Table.

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

Example. Consider the group $(\mathbb{Z}_2, +)$. Its Cayley table is:

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

Example. Consider the group $\mathbb{Z}^* = \{1, -1\}$. Its Cayley table is:

$\mathbb{Z}^*$	1	-1
1	1	-1
-1	-1	1

By $*$, we mean multiplication here.

We note that if we replace 1 by $[0]$ and -1 by $[1]$, the Cayley tables of $\mathbb{Z}^*$ and $\mathbb{Z}_2$ become the same.

In this case, we say $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are isomorphic, denoted by $\mathbb{Z}^* \cong \mathbb{Z}_2$.

Example. For $n \in \mathbb{N}$, the cyclic group of order n is define by

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

with $a^n = 1$ and $1, a, \ldots, a^{n-1}$ are distinct.

We write $C_n = \langle a : a^n = 1 \rangle$ and call a the generator of C_n. The Cayley table of C_n is:

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

Proposition 1.7. Let G be a group. Up to isomorphism, we have

(1) If $|G| = 1$, then $G \cong \{1\}$.

(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 $G \cong K_4 \cong C_2 \times C_2$.

Note. K_4 is the Klein 4-group.

Proof.

(1) If $|G| = 1$, then $G = \{1\}$.

(2) 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 get $g = 1$, a contradiction. Thus, $g^2 = 1$. Hence, the Cayley table of G is

G	1	g
1	1	g
g	g	1

which is isomorphic to C_2.

(3) If $|G| = 3$, then $G = \{1, g, h\}$ with $g, h \neq 1$ and $g \neq h$. Then we have

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

By cancellation, we have $gh \neq g$ and $gh \neq h$. Thus $gh = 1$. Similarly, we have $hg = 1$.

Also, on the row for g, we have $g1 = g$ and $gh = 1$. Since all entries in this row are distinct, we have $g^2 = h$. Similarly, we have $h^2 = g$. Note that

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

and

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

By identifying g with a and h with a^2, we see that $G \cong C_3$.

(4) See A1.

□

Lecture 4

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

2 Subgroups

2.1 Subgroups

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 H is a **subgroup** of G.

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:

Theorem 2.1 (**Subgroup Test**).

(1) If $h_1, h_2 \in H$, then $h_1h_2 \in H$.

(2) There exists an identity element $1_H \in H$ such that $1_Hh = h1_H = h$ for all $h \in H$.

(3) If $h \in H$, then $h^{-1} \in H$.

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

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

Example. We have a chain of subgroups:

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

Example. We recall that $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$. Define

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}.$$

Note that the identity matrix $I \in SL_n(\mathbb{R})$. Let $A, B \in SL_n(\mathbb{R})$.
Then $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$ and $\det\left(A^{-1}\right) = \frac{1}{\det(A)} = \frac{1}{1} = 1$. Thus, AB, $A^{-1} \in SL_n(\mathbb{R})$.
By the Subgroup Test, $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

Definition 2.2 (**Special Linear Group**). We call

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}$$

the **special linear group of order** n **over** $\mathbb{R}$.

Example (**Center of a Group**). Given a group G, we define the center of G to be

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

Note that $Z(G) = G \iff G$ is abelian.

Claim. $Z(G)$ is an abelian subgroup of G.

Proof. Note that $1 \in Z(G)$. Let $y, z \in Z(G)$. Then $\forall g \in G$, we have

$$(yz)g = y(zg) = y(gz) = (yg)z = (gy)z = g(yz).$$

Thus, $yz \in Z(G)$. Also, for $z \in Z(G)$, we have

$$\begin{aligned} zg = gz &\iff z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1} \\ &\iff (z^{-1}z)gz^{-1} = z^{-1}g(zz^{-1}) \\ &\iff gz^{-1} = z^{-1}g. \end{aligned}$$

Thus, $z^{-1} \in Z(G)$. By the Subgroup Test, $Z(G)$ is a subgroup of G. Also, by the definition of $Z(G)$, we see that it is abelian. □

Proposition 2.2. Let H and K be subgroups of a group G. Then their intersection

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

is also a subgroup of G.

Exercise: Prove the above proposition.

Proposition 2.3 (**Finite Subgroup Test**). If H is a finite non-empty subset of a group G, then H is a subgroup of $G \iff H$ is closed under the group operation.

Proof.
($\Rightarrow$) Clear.
($\Leftarrow$) For $H \neq \emptyset$, let $h \in H$. Since H is closed under its operation, we have $h, h^2, h^3, \ldots$ are all in H. Since H is finite, these elements are not all distinct. Thus $h^n = h^{m+n}$ for some $m, n \in \mathbb{N}$. By cancellation from G, we have $h^m = 1$ and thus $1 \in H$. Also, $1 = h^{m-1}h$ implies that $h^{-1} = h^{m-1}$ and thus $h^{-1} \in H$. By the Subgroup Test, H is a subgroup of G. □

2.2 Alternating Groups

We recall that for $\sigma \in S_n$ with $\sigma \neq \epsilon$, 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 $a, b \in \{1, 2, \ldots, n\}$ and $a \neq b$.

Lecture 5

Example. Consider the permutation $(1\,2\,4\,5) \in S_5$. Also, the composition $(1\,2)(2\,4)(4\,5)$ 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 $(1\,2\,4\,5) = (1\,2)(2\,4)(4\,5)$. Also, we can show that:

$$(1\,2\,4\,5) = (2\,3)(1\,2)(2\,5)(1\,3)(2\,4).$$

We see from the example that the factorization into transpositions is **NOT** unique. However, one can prove the following.

Theorem 2.4 (**Parity Theorem**).
If a permutation σ has two factorizations

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

where each γ_i and μ_i is a transposition, then $r \equiv s \pmod 2$.

Note. If a permutation is expressed as a product of transpositions in two different ways, then the number of transpositions used in both factorizations must either both be even or both be odd.

Proof. See Bonus 2. □

Definition 2.4 (**Even, Odd**). A permutation σ is **even** (or **odd**) if it can be written as a product of an **even** (or **odd**) number of transpostions.

Note. By the Parity Theorem, the above definition is well-defined.

Theorem 2.5. For $n \geq 2$, let A_n denote the set of all even permutations in S_n. Then
(1) $\epsilon \in A_n$.
(2) If $\sigma, \tau \in A_n$, then $\sigma\tau \in A_n$ and $\sigma^{-1} \in A_n$.
(3) $|A_n| = \frac{1}{2}n!$.

Proof.

(1) We can write $\epsilon = (1\,2)(1\,2)$. Thus, ϵ is even.

(2) 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, σ_j are transpositions and r, s are even integers. Then $\sigma\tau = \sigma_1 \cdots \sigma_r\tau_1 \cdots \tau_s$ is a product of $(r+s)$ transpositions and thus $\sigma\tau$ is even. Also, we note that since σ_i is a transposition, we have $\sigma_i^2 = \epsilon$ and thus $\sigma_i^{-1} = \sigma_i$. 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.

(3) Let O_n denote the set of odd permutations in S_n. Thus, $S_n = A_n \cup O_n$ and the Parity Theorem implies that $A_n \cap O_n = \varnothing$. Since $|S_n| = n!$, it suffices to show that $|A_n| = |O_n|$.

Let $\gamma = (1\,2)$ and let $f : A_n \to O_n$ 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 $\tau \in O_n$, then $\sigma = \gamma\tau \in A_n$ and $f(\sigma) = \gamma\sigma = \gamma(\gamma\tau) = \gamma^2\tau = \tau$. Thus, f is onto. It follows that f is a bijection. Thusm, $|A_n| = |O_n|$ and thus $|A_n| = \frac{1}{2}n! = |O_n|$.

□

Definition 2.5 (**Alternating Group**). From (1) and (2) of the above theorem, we see that A_n is a subgroup of S_n, called the **alternating group of degree** n.

2.3 Order of Elements

Definition 2.6 (**Notation**).
If G is a group and $g \in G$, we denote $\langle g\rangle = \{g^k : k \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\}$.
Note that $1 = g^0 \in \langle g\rangle$. Also, if $x = g^m$, $y = g^n \in \langle g\rangle$ with $m, n \in \mathbb{Z}$, then

$$xy = g^{m+n} \in \langle g\rangle \quad \text{and} \quad x^{-1} = g^{-m} \in \langle g\rangle.$$

By the Subgroup Test, we have the following.

Proposition 2.6. If G is a group and $g \in G$, then $\langle g\rangle$ is a subgroup of G.

Definition 2.7 (**Cyclic Group, Generator**). If G is a group and $g \in G$, we call $\langle g\rangle$ the **cyclic group 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. Consider $(\mathbb{Z}, +)$. Note that $\forall k \in \mathbb{Z}$, we have $k = k \cdot 1$. Thus, $(\mathbb{Z}, +) = \langle 1\rangle$.
Similarly, $(\mathbb{Z}, +) = \langle -1\rangle$. We observe that for any $n \in \mathbb{Z}$ with $n \neq \pm 1$, $\nexists k \in \mathbb{Z}$ such that $k \cdot n = 1$. Thus, ± 1 are the only generators of $(\mathbb{Z}, +)$.

Note. If we are clear that the group operation is addition, we can write $\underbrace{g + g + \cdots + g}_{k \text{ times}} = kg$.

Let G be a group and $g \in G$. Suppose that $\exists k \in \mathbb{Z}$ with $k \neq 0$ such that $g^k = 1$. Then $g^{-k} = (g^{-1})^k = 1$. 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 the **order** of g is n, denoted by $o(g) = n$.
If no such n exists, then we say g has **infinite order** and write $o(g) = \infty$.

Proposition 2.7. Let G be a group and $g \in G$ satisfying $o(g) = n \in \mathbb{N}$. For $k \in \mathbb{Z}$, we have

(1) $g^k = 1 \iff n \mid k$.

(2) $g^k = g^m \iff k \equiv m \pmod{n}$.

(3) $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ where $1, g, \dots, g^{n-1}$ are all distinct. In particular, $|\langle g \rangle| = o(g)$.

Proof.

(1) ($\Leftarrow$) If $n \mid k$, then $k = nq$ for some $q \in \mathbb{Z}$. Then

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

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

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

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

(2) Note that

$$\begin{aligned} g^k = g^m &\iff g^{k-m} = 1 \\ &\iff n \mid (k - m) \\ &\iff k \equiv m \pmod{n} \end{aligned}$$

which is a result from the previous part.

(3) $\supseteq$: From (2), it follows that $1, g, \dots, g^{n-1}$ are all distinct, and clearly $\{1, g, \dots, g^{n-1}\} \subseteq \langle g \rangle$ by definition.

$\subseteq$: Let$x = g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. Write $k = nq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. Then

$$x = g^k = g^{nq+r} = (g^n)^q (q^r) = g^r \in \{1, g, \dots, g^{n-1}\}.$$

Therefore, $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$.

□

Lecture 6

Proposition 2.8. Let G be a group and $g \in G$ with $o(g) = \infty$. Then for $k \in \mathbb{Z}$, $k \geq 0$, we have

(1) $g^k = 1 \iff k = 0$.

(2) $g^k = g^m \iff k = m$.

(3) $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}$, where all elements are distinct.

Proof.

(1) ($\Leftarrow$) If $k = 0$, then $g^k = g^0 = 1$.

($\Rightarrow$) Assume towards a contradiction that $g^k = 1$ for some $k \in \mathbb{N}$. However, this implies that $o(g) \leq k$ is finite, which contradicts our assumption.

(2) ($\Leftarrow$) If $k = m$, then $g^k = g^m$.

($\Rightarrow$) By contradiction, assume that $g^k = g^m$ for some $k \neq m$. Then, consider $g^{k-m} = (g^k)(g^m)^{-1} = 1$ and moreover, $k - m \neq 0$, which leads to a contradiction by the result from (1).

(3) Immediately follows from (2).

□

Proposition 2.9 (**Order of g^d**). Let G be a group and $g \in G$ with $o(g) = n \in \mathbb{N}$. If $d \in \mathbb{N}$, then

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

In particular, if $d \mid n$, then $\gcd(n, d) = d$ and $o(g^d) = \frac{n}{d}$.

Proof. Let $n_1 = \frac{n}{\gcd(n,d)}, d_1 = \frac{d}{\gcd(n,d)}$. Note that $\gcd(n_1, d_1) = 1$, which is a result from MATH 135 ($\forall a, b \in \mathbb{Z}$, not both 0, we have $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a.b)}) = 1$). Note that

$$(g^d)^{n_1} = (g^d)^{\frac{n}{\gcd(n,d)}} = (g^n)^{\frac{d}{\gcd(n,d)}} = 1.$$

Then, it follows to show that n_1 is indeed the smallest value that satisfies this relation.

Pick some $r \in \mathbb{N}$ such that $(g^d)^r = 1$. Then, $\exists q \in \mathbb{Z}$ such that $dr = nq$ by Proposition 2.7. Dividing both sides by $\gcd(n, d)$, we get $d_1 r = n_1 q \implies n_1 \mid d_1 r$.

Note that n_1, d_1 are coprime, then it must follow that $n_1 \mid r \implies r = n_1 p$ for some $p \in \mathbb{Z}$. Since $r, n_1 > 0$, then $p \in \mathbb{N}$. Thus, $r \geq n_1$ as desired (so n_1 is the smallest). □

2.4 Cyclic Groups

We recall that for a group G, if $G = \langle g \rangle$ for some $g \in G$, then G is a cyclic group.

For $a, b \in G$, we have $a = g^m$, $b = g^n$ for some $m, n \in \mathbb{Z}$. Since

$$ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba,$$

if follows that G must be abelian.

Proposition 2.10. Every cyclic group is abelian.

Note. The converse of this proposition is **NOT** true. One can consider $K_4 \cong C_2 \times C_2$, the Klein 4-group. K_4 is abelian but not cyclic.

Proposition 2.11. Every subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group and let $H \subseteq G$ be a subgroup of G. Set $G = \langle g \rangle$ for some $g \in G$.

If $H = \{1\}$, then $H = \langle 1 \rangle$ is cyclic. If $H \neq \{1\}$, then $\exists g^k \in H$ 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. $H = \langle g^m \rangle$.

Proof. We note that since $g^m \in H$, we have $\langle g^m \rangle \subseteq H$. To prove the other inclusion, note that for any $h \in H \subset G = \langle g \rangle$, we can write $h = g^k$ for some $k \in \mathbb{Z}$. By the division algorithm, we have $k = mq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Then, $g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$. Since $0 \leq r < m$, by the definition of m, we have $r = 0$. Thus, $m \mid k$ and we have $g^k \in \langle g^m \rangle$. It follows that $H \subseteq \langle g^m \rangle$. □

□

Lecture 7

Proposition 2.12.
Let $G = \langle g \rangle$ be a cyclic group with $o(g) = n \in \mathbb{N}$. Then, $G = \langle g^k \rangle \iff \gcd(k, n) = 1$.

Proof. By Proposition 2.9, $o(g^k) = \frac{n}{\gcd(k,n)} = n$. □

Theorem 2.13 (**Fundamental Theorem of Finite Cyclic Group**).
Let $G = \langle g \rangle$ be a cyclic group with $o(g) = n \in \mathbb{N}$.

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

Remark. This theorem shows that there is a 1-1 correspondence between the set of positive divisors of n and all subgroups of a cyclic group of order n.

Proof.

(1) By Proposition 2.11, H is cyclic, say $H = \langle g^m \rangle$ for some $m \in \mathbb{N} \cup \{0\}$. Let $d = \gcd(m, n)$.

Claim. $H = \langle g^d \rangle$.

Proof. Since $d \mid m$, we have $m = dk$ for some $k \in \mathbb{Z}$. Then,

$$g^m = g^{dk} = (g^d)^k \in \langle g^d \rangle .$$

Thus, $H = \langle g^m \rangle \subseteq \langle g^d \rangle$.

To prove the other inclusion, since $d = \gcd(m, n)$, $\exists x, y \in \mathbb{Z}$ such that $d = mx + ny$ (Bezout's Lemma). Then $g^d = g^{mx+ny} = (g^m)^x (g^n)^y = (g^m)^x 1 \in \langle g^m \rangle$. Thusm, $\langle g^d \rangle \subseteq \langle g^m \rangle = H$. It follows that $H = \langle g^d \rangle$. □

Note that since $d = \gcd(m, n)$, we have $d \mid n$. Also, by Proposition 2.7 and 2.9, we have

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

Thus, $|H| \mid |G|$.

(2) By Proposition 2.9, the cyclic group $\left\langle g^{\frac{n}{k}} \right\rangle$ is of order $\frac{n}{\gcd(n, \frac{n}{k})} = \frac{n}{\frac{n}{k}} = k$.

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 by Proposition 2.7 and 2.9, we have

$$k = |K| = o(g^d) = \frac{n}{\gcd(d, n)} = \frac{n}{d}.$$

It follows that $d = \frac{n}{k}$ and thus $K = \left\langle g^{\frac{n}{k}} \right\rangle$.

□

2.5 Non-Cyclic Group

Let X be a nonempty subset of a group G and let $\langle X \rangle = \{x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} : x_i \in X, k_i \in \mathbb{Z}, m \geq 1\}$ denote the set of all products of powers of (not necessarily distinct) elements of 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 $\left(x_1^{k_1} \cdots x_m^{k_m}\right)^{-1} = x_m^{-k_m} \cdots x_1^{-k_1} \in \langle X \rangle$. Hence $\langle X \rangle$ is a subgroup of G containing X, called the subgroup of G generated by X.

Example. 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. The symmetric group of degree 3, $S_3 = \{\epsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ where $\sigma^3 = \epsilon = \tau^2$ and $\sigma\tau = \tau\sigma^2$. Thus,

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

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

Note. One can take $\sigma = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 \end{pmatrix}$.

Definition 2.9 (**Dihedral Group**).

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

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

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

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

Note. When $n = 2$ or $n = 3$, we have

$$D_4 \cong K_4 \quad \text{and} \quad D_6 \cong S_3.$$

Exercise: For $n \geq 3$, consider a regular n-gon and its group of symmetries. How is it related to D_{2n}?

Hint: consider all possible rotations and reflections.

Remark. Dihedral group is a set of rigid motions for transforming a regular polygon back to its original position while changing the index of its vertices.

3 Normal Subgroups

3.1 Homomorphisms and Isomorphisms

Lecture 8

Definition 3.1 (**Homomorhism (HM)**).
Let G and H be groups. A mapping $\alpha : G \to H$ is a **homomorphism (HM)** if

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

Note. To simplify notation, we often write $\alpha(ab) = \alpha(a)\alpha(b)$.

Example. Consider the determinant map

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

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

One can show the following proposition.

Proposition 3.1. Let $\alpha : G \to H$ be a group homomorphism. Then

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

Proof. See Piazza exercise. □

Definition 3.2 (**Isomorphism (IM)**).
Let G and H be groups. Consider a mapping $\alpha : G \to H$. If α is a homomorphism and α is bijective, we say α is an **isomorphism (IM)**. In this case, we say G and H are isomorphic and denoted as $G \cong H$.

Proposition 3.2. We have

(1) The identity map $\mathrm{id} : G \to G$ is an isomorphism.

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

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

Remark. Thus, we see that $\cong$ is an equivalence relation.

Proof. See Piazza exercise. □

Example. Let $\mathbb{R}^+ = \{r \in R, r > 0\}$.

Claim. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}^+, \cdot)$.

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

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

Thus, σ is a homomorphism. It follows that σ is an isomorphism and thus $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$.

Example.

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

Suppose that $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ is an isomorphism. Then τ is onto. Thus, there exists $g \in \mathbb{Q}$ s.t. $\tau(g) = 2$. Write $\tau\left(\frac{g}{2}\right) = a \in \mathbb{Q}$. Since τ is an isomorphism, we have

$$a^2 = \tau\left(\frac{g}{2}\right) \cdot \tau\left(\frac{g}{2}\right) = \tau\left(\frac{g}{2} + \frac{g}{2}\right) = \tau(g) = 2,$$

which contradicts the fact that $a \in \mathbb{Q}$. Thus, such τ does not exist and have $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$.

3.2 Cosets and Lagrage's Theorem

Definition 3.3 (**Right, Left Cosets**).
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 generated by a. Similarly, we define

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

to be the **left coset** of H generated by a.

Since $1 \in H$, 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 $Ha = aH$.

Example. 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

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

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

Example. Let $S_3 = \{\epsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ with $\sigma^3 = \epsilon = \tau^2$ and $\sigma\tau\sigma = \tau$. Let $H = \{\epsilon, \tau\}$ be a subgroup of S_3. Since $\sigma\tau = \tau\sigma^{-1} = \tau\sigma^2$, the right cosets of H are $H\epsilon = \{\epsilon, \tau\} = H\tau$, $H\sigma = \{\sigma, \tau\sigma\} = H\tau\sigma$, $H\sigma^2 = \{\sigma^2, \tau\sigma^2\} = H\tau\sigma^2$.
Also, the left cosets of H are $\epsilon H = \{\epsilon, \tau\} = \tau H$, $\sigma H = \{\sigma, \tau\sigma^2\} = \tau\sigma^2 H$, $\sigma^2 H = \{\sigma^2, \tau\sigma\} = \tau\sigma H$.
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 $a, b \in G$. Then,

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

Proof.

(1) ($\Rightarrow$) If $Ha = Hb$, then $a = 1 \cdot a \in Ha = Hb$. Thus, $a = hb$ for some $h \in H$ and we have $ab^{-1} = h \in H$.

($\Leftarrow$) Suppose $ab^{-1} \in H$. Then $\forall h \in H$, we have $ha = ha(b^{-1}b) = h(ab^{-1})b \in Hb$. 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, $\forall h \in H$, we have

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

Thus, $Hb \subseteq Ha$, it follows that $Ha = Hb$.

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

(3) We have two cases.

(3 - 1) If $Ha \cap Hb = \emptyset$, then we are done.

(3 - 2) If $Ha \cap Hb \neq \emptyset$, then $\exists x \in Ha \cap Hb$. Since $x \in Ha$, by (2), we have $Ha = Hx$. Since $x \in Hb$, by (2), we have $Hb = Hx$. Thus, we have $Hx = Ha = Hb$.

□

Lecture 9

Remark. The algorithm of the above proposition also holds for left cosets. For (1), we have $aH = bH \iff b^{-1}a \in H$. Also, if we take the union of the right cosets, by iterating through all elements of G, we get

$$G = \bigcup_{a \in G} Ha.$$

By the previous proposition, we see that G can be written as a disjoint union of right cosets of H. We now define the following definition.

Definition 3.4 (**Index**). Let H be a subgroup of a group G. The number of disjoint cosets (either left or right) of H in G as the **index** of H in G, and denote this number by $[G : H]$.

Theorem 3.4 (**Lagrange's Theorem**).

Let H be a subgroup of a finite group G. Then

$$|H| \mid |G| \quad \text{and} \quad [G : H] = \frac{|G|}{|H|}.$$

Proof. Write $k = [G : H]$ and let $Ha_1, Ha_2, \ldots, Ha_k$ be the distinct right cosets of H in G such that $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$. Since $|Ha_i| = |H|, \forall i = 1, \ldots, k$, we have

$$|G| = \sum_{i=1}^{k} |Ha_i| = k\,|H| \implies |H| \mid |G| \quad \text{and} \quad [G : H] = k = \frac{|G|}{|H|}.$$

□

Corollary 3.5. Let G be a finite group.

(1) If $g \in G$, then $o(g) \mid |G|$.

(2) If $|G| = n$, then $\forall g \in G$, we have $g^n = 1$.

Proof.

(1) Take $H = \langle g \rangle$. By Lagrange's Theorem, we have $o(g) = |H| \mid |G|$.

(2) Let $o(g) = m$. Then by part (1), we have $g^n = (g^m)^{\frac{n}{m}} = 1^{\frac{n}{m}} = 1$.

□

Example (**Euler's Totient Function**).

For $n \in \mathbb{N}$ with $n \geq 2$, let $\mathbb{Z}_n^*$ be the set of all multiplicative invertible elements in $\mathbb{Z}_n$. Consider the Euler's φ function, $\varphi(n)$, denote the order of $\mathbb{Z}_n^*$. Recall from a previous example, we have seen that $\mathbb{Z}_n^*$ contains all natural number smaller than n (including 0) that is coprime with n. Hence

$$\varphi(n) = |\mathbb{Z}_n^*| = |\{k \in \mathbb{Z}_n : \gcd(k, n) = 1\}|.$$

As a direct result from previous corollary, we see that if $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

This is the Euler's Theorem. If $n = p$ where p is a prime, the Euler's Theorem implies that

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

which is the Fermat's Little Theorem.

Corollary 3.6. If G is a group with $|G| = p$ where p is a prime, then $G \cong C_p$, where C_p is the cyclic group of order p.

Proof. Let $g \in G$ and $g \neq 1$. Then by the previous corollary, we have $o(g) \mid |G|$. Since $g \neq 1$ and p is a prime, it follows that $o(g) = p$. Therefore,

$$|\langle g \rangle| = o(g) = p \implies G = \langle g \rangle \cong C_p.$$

□

Remark. This corrolary shows the generalization of isomorphism between finite group and cyclic group.

Corollary 3.7. Let H and K be finite subgroups of a group G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

Proof. First note that $H \cap K$ is indeed a subgroup of H and of K. Then by Langrange's Theorem, we know that $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$. Then $|H \cap K| \mid \gcd(|H|, |K|) \implies |H \cap K| = 1$. Thus, $H \cap K = \{1\}$. □

3.3 Normal Subgroups

Definition 3.5 (**Normal Subgroup**). 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 by $H \lhd G$.

Example. We have $\{1\} \lhd G$ and $G \lhd G$.

Example. The center of G, denoted by $Z(G)$, which is the set of all elements in G that commutes. Then $Z(G) \lhd G$. Thus, every subgroup of $Z(G)$ is also normal in G.

Example. If G is an abelian group, then every subgroup of G is normal in G. However, the converse is **NOT** true. See the quanternian group Q_8 in A3.

Proposition 3.8 (**Normality Test**).
Let H be a subgroup of a group G. The following are equivalent.

(1) $H \lhd G$.

(2) $gHg^{-1} \subseteq H$, for all $g \in G$.

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

Proof. We will start with (1) $\implies$ (2). Let $x \in gHg^{-1}$ and say $x = ghg^{-1}$ for some $h \in H$. Then by our assumption, $gh \in gH = Hg$. Thus, we can find $h_1 \in H$ such that $gh = h_1 g$. Therefore,

$$x = ghg^{-1} = h_1 gg^{-1} = h_1 \implies x \in H \implies gHg^{-1} \subseteq H.$$

For (2) $\implies$ (3). Take $g \in G$, we have $gHg^{-1} \subseteq H$. Taking g^{-1} in place of g, we have

$$g^{-1}Hg \subseteq H \implies H \subseteq gHg^{-1} \implies gHg^{-1} = H.$$

□

Lecture 10

Example. 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 the Normality Test, we have $H \lhd G$, i.e. $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

Proposition 3.9. 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, $Hg = G \setminus H$. Similarly, $gH = G \setminus H$. Thus, $Hg = gH$ for all $g \in G$, i.e. $H \lhd G$. □

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

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

Proposition 3.10. $\langle a \rangle \lhd D_{2n}$.

Let H and K be subgroups of a group G. The intersection $H \cap K$ is the 'largest' subgroup of G contained in both H and K. One may consider the "smallest" subgroup of G containing both H and K. Note that $H \cup K$ is the "smallest subset" containing H and K. However, we see in A2 that $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$. A more useful construction turns out to be the product of H and K defined as

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

Still, HK is not always a subgroup.

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

Lemma 3.11. Let H and K be subgroups of a group G. The following are equivalent.

(1) HK is a subgroup of G.

(2) $HK = KH$.

(3) KH is a subgroup of G.

Proof. We will prove (1) $\iff$ (2). Then (2) $\iff$ (3) follows by interchanging H and K.

(2) $\implies$ (1): We have $1 = 1 \cdot 1 \in HK$. Also, if $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Also,

for $hk, h_1k_1 \in HK$, we have $kh_1 \in KH = HK$, say $kh_1 = h_2k_2$. It follows that

$$(hk)(h_1k_1) = h(kh_1)k_1 = h(h_2k_2)k_1 = (hh_2)(k_2k_1) \in HK.$$

by the subgroup test, HK is a subgroup of G.

(1) $\implies$ (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

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

Thus, we have $KH \subseteq HK$.

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 3.12. 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 that $H \lhd G$. Then

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

By the previous Lemma, $HK = KH$ is a subgroup of G.

(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, 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

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

Note. We see that $H \lhd G \iff N_G(H) = G$. Note that in the proof of Proposition 3.12, we do not need the full assumption that $H \lhd G$, we only need $kH = Hk$ for all $k \in K$, i.e. $k \in N_G(H)$.

Corollary 3.13. 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.

Theorem 3.14. If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $HK \cong H \times K$.

As a direct consequence, we have the following.

Corollary 3.15. Let G be a finite group and let $H \lhd G$, $K \lhd G$, with $H \cap K = \{1\}$ and $|H|\,|K| = |G|$. Then $G \cong H \times K$.

Lecture 11

Proof of Theorem 3.14.

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. Consider $x = hk(kh)^{-1} = hkh^{-1}k^{-1}$. Note that $kh^{-1}k^{-1} \in kHk^{-1} = H$. Thus $x = h(kh^{-1}k^{-1}) \in H$. Similarly, since $hkh^{-1} \in hKh^{-1} = K$, we have $x = (hkh^{-1})k^{-1} \in K$. Since $x \in HcapK = \{1\}$, we have $hkh^{-1}k^{-1} = 1$, i.e. $hk = kh$. Thus, Claim 1 holds.

Since $H \lhd G$, by Propsition 3.12, HK is a subgroup of G. Define $\sigma : H \times K \to HK$ by $\sigma((h,k)) = hk$, $\forall h \in H, k \in K$. We will show that σ is an isomorphism. □

Claim (**2**). σ is an isomorphism.

Proof. Let $(h,k),(h_1,k_1) \in H \times K$. By Claim 1, we have $h_1 k = k h_1$. Then,

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

Thus, 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. $h_1 = h$ and $k_1 = k$. Thus, σ is one-to-one and Claim 2 holds. □

It follows that $HK \cong H \times K$. □

Example. Let $m,n \in \mathbb{N}$ with $\gcd(m,n) = 1$. 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 $|H|\,|K| = mn = |G|$. Since $\gcd(m,n) = 1$, by Corollary 3.7, we have $H \cap K = \{1\}$. Also, since G is cyclic and thus abelian, we have $H \lhd G$ and $K \lhd G$. Thus, by Corollary 3.15, we have $G \cong H \times K$, i.e. $C_{mn} \cong C_m \times C_n$. Hence, to consider finite cyclic groups, it suffices to consider cyclic group of prime power order.

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, i.e. $\{Ka : a \in G\}$ into a group.

A natural way to define multiplication on this set is

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

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

$$Ka = Ka_1 \text{ and } Kb = Kb_1 \implies Kab = Ka_1b_1.$$

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. The following are equivalent:

(1) $K \lhd G$.

(2) For $a, b \in G$, the multiplication $KaKb = Kab$ is well-defined.

Proof.

(1) $\implies$ (2): Let $Ka = Ka_1$ and $Kb = Kb_1$. Thus, $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$. To get $Kab = Ka_1b_1$, it suffices to show that $ab(a_1b_1)^{-1} \in K$. Notice 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) $\implies$ (1): If $a \in G$, to show $K \lhd G$, it suffices to show $aka^{-1} \in K$ for all $k \in K$. Since $Ka = Ka$ and $Kk = K1$, by (2), we have $Kak = Ka1$, i.e. $Kak = Ka$. It follows that $aka^{-1} \in K$. Thus $K \lhd G$. □

Proposition 4.2. Let $K \lhd G$, and write $G/K = \{Ka : a \in G\}$ for the 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 group homomorphism.

(3) If $[G : K]$ is finite, then $|G/K| = [G : K]$. In particular, $|G/K| = \frac{|G|}{|K|}$.

Proof.

(1) By Lemma 4.1, the operation is well-defined and G/K is closed under the operation. The identity of G/K is $K = K1$. Also, $Ka \cdot Ka^{-1} = K \cdot 1 = Ka^{-1} \cdot Ka$. Finally, $Ka(KbKc) = (KaKb)Kc$ by the associativity of G. Thus G/K is a group.

(2) φ is clearly onto. Also, for $a, b \in G$, we have $\varphi(a)\varphi(b) = (Ka)(Kb) = Kab = \varphi(ab)$. Thus φ is a group homomorphism.

(3) If $[G : K]$ is finite, by the definition of $[G : K]$, we have $[G : K] = |G/K|$. Also, if $|G|$ is finite, by Langrange's Theorem, $|G/K| = [G : K] = \frac{|G|}{|K|}$.

□

Lecture 12

Definition 4.1 (**Quotient Group, Coset Map**). 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 $\varphi : G \to G/K$ 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 of 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

$$\operatorname{Ker}\alpha = \{g \in G : \alpha(g) = 1_H\} \subseteq G,$$

and the **image** of α is defined by

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

Proposition 4.3. Let $\alpha : G \to H$ be a group homomorphism. Then

(1) $\operatorname{im}\alpha$ is a subgroup of H.

(2) $\operatorname{Ker}\alpha \lhd G$.

Proof.

(1) Note that $1_H = \alpha(1_G) \in \alpha(G)$. Also, for $h_1 = \alpha(g_1), h_2 = \alpha(g_2) \in \alpha(G)$, we have

$$h_1h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1g_2) \in \alpha(G).$$

Also, by Proposition 3.1, $\alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(G)$. By the subgroup test, $\alpha(G)$ is a sungroup of H.

(2) For $\operatorname{Ker}\alpha$, note that we have $\alpha(1_G) = 1_H$. Also, if $k_1, k_2 \in \operatorname{Ker}\alpha$, then

$$\alpha(k_1k_2) = \alpha(k_1)\alpha(k_2) = 1 \cdot 1 = 1,$$

and

$$\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1^{-1} = 1.$$

By the subgroup test, $\operatorname{Ker}\alpha$ is a subgroup of G. Note that if $g \in G$ and $k \in \operatorname{Ker}\alpha$, then

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g)1\alpha(g)^{-1} = \alpha(g)\alpha(g)^{-1} = 1.$$

Thus, $g(\operatorname{Ker}\alpha)g^{-1} \subseteq \operatorname{Ker}\alpha$. By the Normality test, we have $\operatorname{Ker}\alpha \lhd G$.

□

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

Example (**Sign**). 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 $\operatorname{sgn} : S_n \to \{\pm 1\}$ defined by $\sigma \mapsto \operatorname{sgn}(\sigma)$ is a homomorphism. Also, $\operatorname{Ker}(\operatorname{sgn}) = A_n$, the alternating group. Thus $A_n \lhd S_n$.

Theorem 4.4 (**First Isomorphism Theorem**).
Let $\alpha : G \to H$ be a group homomorphism. We have

$$G/\operatorname{Ker}\alpha \cong \operatorname{im}\alpha.$$

Proof. Let $K = \operatorname{Ker}\alpha$. Since $K \lhd G$, we have G/K is a group. Define the map $\bar{\alpha} : G/K \to \operatorname{im}\alpha$ by $\bar{\alpha}(Kg) = \alpha(g)$ for all $Kg \in G/K$. Note that

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

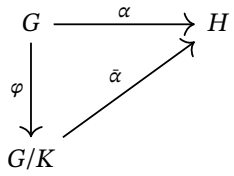
This $\bar{\alpha}$ is well-defined and one-to-one. Clearly, $\bar{\alpha}$ is onto. It remains to show that $\bar{\alpha}$ is a group homomorphism. For $g, h \in G$,

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

Thus, $\bar{\alpha}$ is a group homomorphism. Thus, $G/K \cong \operatorname{im}\alpha$. □

Remark. We must show that the map $\bar{\alpha}$ is well-defined, as above.

Let $\alpha : G \to H$ be a group homomorphism and $K = \operatorname{Ker}\alpha$. Let $\varphi : G \to G/K$ be the coset map and let $\bar{\alpha}$ be defined as in the proof of Theorem 4.4, we have the following diagram:



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

$$\bar{\alpha}\varphi(g) = \bar{\alpha}(Kg) = \alpha(g).$$

Thus, $\alpha = \bar{\alpha}\varphi$. On the other hand, if we have $\alpha = \bar{\alpha}\varphi$, then the action of $\bar{\alpha}$ is determined by α and φ as $\bar{\alpha}(Kg) = \bar{\alpha}\varphi(g) = \alpha(g)$. This shows the following proposition.

Proposition 4.5. Let $\alpha : G \to H$ be a group homomorphism and $K = \operatorname{Ker}\alpha$. Then α factors uniquely as $\alpha = \bar{\alpha}\varphi$, where $\varphi : G \to G/K$ is the coset map and $\bar{\alpha} : G/K \to H$ is defined by $\bar{\alpha}(Kg) = \alpha(g)$. (note that φ is onto and $\bar{\alpha}$ is one-to-one).

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

(1) If $o(g) = \infty$, then $\operatorname{Ker}\alpha = \{0\}$. By the First Isomorphism Theorem, we have $G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$.

(2) If $o(g) = n \in \mathbb{N}$, by Proposition 2.7, $\operatorname{Ker}\alpha = n\mathbb{Z}$. By the First Isomorphism Theorem, we have $G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

By (1) and (2), we can conclude that if G is a cyclic group, then $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}_n$ for some $n \in \mathbb{N}$.

Lecture 13

Theorem 4.6 (**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 $K \lhd G$, by Proposition 3.12, HK is a subgroup, $HK = KH$ and $K \lhd HK$ (since K is clearly a subgroup of HK). Consider the map

$$\alpha : H \to HK/K \quad \text{defined by} \quad \alpha(h) = Kh.$$

Then α is a group homomorphism (ex). Also, if $x \in HK = KH$, say $x = kh$, then $Kx = K(kh) = Kh = \alpha(h)$. Thus, α is onto.

Finally, by Proposition 3.3,

$$\operatorname{Ker}\alpha = \{h \in H : Kh = K\} = \{h \in H : h \in K\} = H \cap K,$$

so $H \cap K \lhd H$. By the First Isomorphism Theorem, we have

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

□

Remark. Instead of proving isomorphisms directly, we usually construct maps, then use isomorphism theorems.

Theorem 4.7 (**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 the map $\alpha : G/K \to G/H$ by $\alpha(Kg) = Hg$ for all $g \in G$. Note that if $Kg = Kg_1$, then

$gg_1^{-1} \in K \subseteq H$. Thus $Hg = Hg_1$ and α is well-defined. Clearly, α is onto. Note that

$$\operatorname{Ker}\alpha = \{Kg \in G/K : Hg = H\} = \{Kg \in G/K : g \in H\} = H/K.$$

By the First Isomorphism Theorem, we have $(G/K)/(H/K) \cong G/H$. □

Note. We need to justify that α is well-defined.

Remark. $\alpha : G \to H$ is well-defined means that for $g = h$ in G, we have $\alpha(g) = \alpha(h)$ in H.

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.

Proof. Let $G = \{g_1, \dots, g_n\}$ 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 to prove this theorem, 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 $ag = ag_1$, then $g = g_1$ by cancellation and $a(a^{-1}g) = g$. Hence 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 one-to-one homomorphism, and note that $\operatorname{Ker}\sigma = \{1\}$. By the First Isomorphism Theorem, we have $G \cong \operatorname{im}\sigma$, a subgroup of $S_G \cong S_n$. □

Example. Let H be a subgroup of a group G with $[G : H] = m < \infty$. Let $X = \{g_1H, g_2H, \dots, g_mH\}$ be the set of all distinct left cosets of H in G. For $a \in G$, define $\lambda_a : X \to X$ by $\lambda_a(gH) = agH$, $\forall gH \in X$. Note that $agH = ag_1H$ implies $gH = g_1H$ and $a(a^{-1}gH) = gH$. 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 $a \in \operatorname{Ker}\tau$, then λ_a is the identity permutation. In particular, $aH = \lambda_a(H) = H$. In particular, $a \in H$ and thus $\operatorname{Ker}\tau \subseteq H$.

Theorem 5.2 (**Extended Cayley's Theorem**).
Let H be a subgroup of a group G with $[G : H] = m < \infty$. If G has no normal subgroup contained in H except $\{1\}$, then G is isomorphic to a subgroup of S_m.

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 $K = \operatorname{Ker}\tau \subseteq H$. 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 $K = \{1\}$. It follows that $G \cong \operatorname{im}\tau$, a subgroup of $S_X \cong S_m$. □

Lecture 14

Corollary 5.3. 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 $H \lhd G$.

Remark. This result is a generalization of Proposition 3.9 in which $p = 2$.

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's Theorem with $K = \operatorname{Ker}\tau \subseteq H$. By the First Isomorphism Theorem, we have

$$G/K \cong \operatorname{im}\tau \subseteq S_p \quad (\subseteq \text{ means subgroup here}).$$

Thus, G/K is isomorphic to a subgroup of S_p. By Lagrange's 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, $pk \mid p!$ and hence $k \mid (p-1)!$. Since $k \mid |H|$, 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 $K = H$. Thus $H \lhd G$. □

5.2 Group Actions

Definition 5.1 (Group Action). Ler G be a group and X a non-empty set. A (left) **group action** of G on X is a map $G \times X \to X$ denoted by $(a, x) \mapsto ax$ such that

(1) $1 \cdot x = x, \forall x \in X$.

(2) $a \cdot (b \cdot x) = (ab) \cdot x, \forall a, b \in G, \forall x \in X$.

In this case, we say that $\underline{G \text{ acts on } X}$.

Remark. 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 (ex)

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

In particular, $a \cdot x = a \cdot y \iff x = y$.

Example. If G is a group, let G act on itself, i.e. $X = G$, by $a \cdot x = axa^{-1}, \forall a, x \in G$. In other words, we have $G \times G \to G$ with $(a, x) \mapsto axa^{-1}$. Note that

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

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

Remark. For $a \in G$, define $\sigma_a : X \to X$ by $\sigma_a(x) = a \cdot x, \forall x \in X$. Then one can show (see A5) the following:

(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 $\operatorname{Ker}\theta = \{a \in G : a \cdot x = x \ \forall x \in X\}$.

Note that the group homomorphism θ gives equivalence definition of group action of G on X.

If $X = G$ and $|G| = n$ and $\operatorname{Ker}\theta = \{1\}$ (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 Stabilizer).
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 by

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

the **stabilizer** of x.

Proposition 5.4. 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 stabilizer of x, respectively. Then

(1) $S(x)$ is a subgroup of G.

(2) There exists a bijection from $G \cdot x$ to $\{gS(x) : g \in G\}$ and thus $|G \cdot x| = [G : S(x)]$.

Proof.

(1) Since $1 \cdot x = x$, we have $1 \in S(x)$. Also, if $g, h \in S(x)$, then $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$. Thus $gh \in S(x)$ and $g^{-1}x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x$. Thus, $g^{-1} \in S(x)$. By the subgroup test, $S(x)$ is a subgroup of G.

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

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

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

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

□

Lecture 15

Theorem 5.5 (**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 $x \in X_f \iff |G \cdot x| = 1$). Let $G \cdot x_1, G \cdot x_2, \ldots, G \cdot x_n$ denote the distinct non-singleton orbits (i.e. $|G \cdot x_i| > 1$). Then

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

Proof. Note that for $a, b \in G$ and $x, y \in X$, we have

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

Thus, two orbits are either disjoint or the same. It follows that the orbits form a disjoint union of X. Since $x \in X_f \iff |G \cdot x| = 1$, the set $X \setminus X_f$ contains all non-singleton orbits, which are disjoint.

Thus, by Proposition 5.4,

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

□

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 $x \in G$, we have

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

The set is called the centralizer of x and is denoted 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 Theorem 5.5, we have the following.

Corollary 5.6 (**Class Equation**).
Let G be a finite group and $\{gx_1g^{-1} : g \in G\}, \dots, \{gx_ng^{-1} : g \in G\}$ denote the distinct non-singleton conjugacy classes of G. Then

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

Lemma 5.7. Let p be a prime and $m \in \mathbb{N}$. Let G be a group of order p^m acting on a finite set $X \neq \emptyset$. Let X_f be defined as in Theorem 5.5. Then, we have $|X| \equiv |X_f| \pmod{p}$.

Proof. By Theorem 5.5, we have

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)] \quad \text{with } [G : S(x_i)] > 1 (1 \le i \le n).$$

Since $[G : S(x_i)] \mid |G| = p^m$ and $[G : S(x_i)] > 1$, we have $p \mid [G : S(x_i)]$ for all i. It follows that

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

□

Theorem 5.8 (**Cauchy's Theorem**).
Let p be a prime and G a finite group. If $p \mid |G|$, then G contains an element of order p.

Proof by J. Mckay. Define

$$X = \{(a_1, a_2, \dots, a_p) : a_i \in G \text{ and } a_1 a_2 \cdots a_p = 1\}.$$

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

$$k \cdot (a_1, a_2, \dots, a_p) = (a_{k+1}, a_{k+2}, \dots, a_p, a_1, a_2, \dots, a_k).$$

Exercise: One can verify that this action is well-defined.

Let X_f be defined as in Theorem 5.5. Then

$$(a_1, \dots, a_p) \in X_f \iff a_1 = a_2 = \cdots = a_p.$$

Clearly, $(1, \dots, 1) \in X_f$ and hence $|X_f| \ge 1$. Since $|\mathbb{Z}_p| = p$, by Lemma 5.7, we have $|X| \equiv |X_f| \equiv 0 \pmod{p}$. Since $|X_f| \equiv 0 \pmod{p}$ and $|X_f| \ge 1$, it follows that $|X_f| \ge p$. Thus, there exists $a \ne 1$ such that $(a, \dots, a) \in X_f$, which implies $a^p = 1$. Since p is a prime and $a \ne 1$, the order of a is p. □

6 Sylow Theorems

6.1 p-Groups

Lecture 16

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 Cauchy's theorem, we have the following.

Corollary 6.1. A finite group G is a p-group $\iff$ $|G|$ is a power of p.

Note. G is a p-group $\iff$ $|G| = p^k$ for some $k \in \mathbb{N} \cup \{0\}$.

Lemma 6.2. The center $Z(G)$ of a non-trivial finite p-group G contains more than one element.

Proof. The class equation of G states that

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

where $[G : C_G(x_i)] > 1$. Since G is a p-group, by Corollary 6.1, $p \mid |G|$. By Lemma 5.7, $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$. It follows that $p \mid |Z(G)|$. Since $1 \in Z(G)$ and $|Z(G)| \geq p$, $Z(G)$ has at least p elements. □

Lemma 6.3. If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

Proof. We recall that

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

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 $x \in G$, we have

$$\begin{aligned} xH \in X_f &\iff hxH = xH \text{ for all } h \in H \\ &\iff x^{-1}hxH = H \text{ for all } h \in H \\ &\iff x^{-1}Hx = H \\ &\iff x \in N_G(H). \end{aligned}$$

Thus, $|X_f|$ is the number of cosets xH with $x \in N_G(H)$, and hence $|X_f| = [N_G(H) : H]$. By Lemma 5.7,

$$[N_G(H) : H] = |X_f| \equiv |X| = [G : H] \pmod{p}.$$

□

Corollary 6.4.
Let H be a p-subgroup of a finite group G. If $p \mid [G : H]$, then $p \mid [N_G(H) : H]$ and $N_G(H) \neq H$.

Proof. Since $p \mid [G : H]$, by Lemma 6.3, we have

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

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

Lecture 17

6.2 Sylow's Three Theorems

Theorem 6.5 (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 (with $i < n$) is normal in some subgroup of order p^{i+1}.

Note. The last part can be viewed as a generalization of Cauchy's theorem ($i = 1$).

Proof. We prove this theorem by induction on i. For $i = 1$, since $p \mid |G|$, by Cauchy's theorem, G contains an element of order p, i.e. $|\langle a \rangle| = p$. Suppose that the statement holds for some $1 \leq i < n$, say H is a subgroup of G of order p^i. Then $p \mid [G : H]$. By Corollary 6.4, $p \mid [N_G(H) : H]$ 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,

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

□

Definition 6.2 (**Sylow p-subgroup**). A subgroup P of a group G is said to be a **Sylow p-subgroup** of G if P is a maximal p-group of G, i.e. $P \subseteq H \subseteq G$ with H a p-group, then $P = H$.

As a direct consequence of Theorem 6.5, we have the following.

Corollary 6.6. Let G be a group of order $p^n m$, where p is a prime, $n \geq 1$ and $\gcd(p, m) = 1$. Let H be a p-subgroup of G. Then

(1) H is a Sylow p-subgroup $\iff$ $|H| = p^n$.

(2) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(3) If there is only one Sylow p-subgroup, say P, then $P \lhd G$.

Theorem 6.7 (**Second Sylow Theorem**).
If H is a p-subgroup of a finite group G, and P is any Sylow p-subgroup of G, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let X be the set of all left cosets of P in G and let H act on X by left multiplication. By Lemma 5.7, 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

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

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

Theorem 6.8 (**Third Sylow Theorem**).
If G is a finite group and a prime p with $p \mid |G|$, 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 Theorem 6.7, the number of Sylow p-subgroups 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 $Q \in X_f \iff gQg^{-1} = Q \quad \forall g \in P$. The latter condition holds if and only if $Q \subseteq N_G(Q)$. Both P and Q are Sylow p-subgroups of G and hence of $N_G(Q)$. Thus, by Corollary 6.6, they are conjugate in $N_G(Q)$. Since $Q \lhd N_G(Q)$, this can only occur if $Q = P$ and $X_f = \{P\}$. By Lemma 5.7, we have $|X| \equiv |X_f| \equiv 1 \pmod{p}$. Thus, $|X| = kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$. □

Remark. Suppose that 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 $p \nmid n_p$, we have $n_p \mid m$.

Example.

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, $n_3 = 1$. Similarly, $n_5 \mid 3$ and $n_5 \equiv 1 \pmod{5}$. Thus, $n_5 = 1$. It follows that there is only one Sylow 3-subgroup and one Sylow 5-subgroup of G, say P_3 and P_5 respectively. Thus, $P_3 \lhd G$ and $P_5 \lhd G$. Consider

$|P_3 \cap P_5|$, which divides 3 and 5. Thus, $|P_3 \cap P_5| = 1$ and $P_3 \cap P_5 = \{1\}$. Also, $|P_3||P_5| = 15 = |G|$. It follows that $G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. □

Exercise: Construct a cyclic group of order > 100.

Lecture 18

Example.

Claim. There are two isomorphism classes of groups of order 21.

Proof. Let G be a group with $|G| = 21 = 3 \cdot 7$. Let n_p be the number of Sylow p-subgroups of G. By the Third Sylow Theorem, we have $n_3 \mid 7$ and $n_3 \equiv 1 \pmod 3$. Thus, $n_3 = 1$ or 7. Also, we have $n_7 \mid 3$ and $n_7 \equiv 1 \pmod 7$. Thus, $n_7 = 1$. It follows that G has a unique Sylow 7-subgroup, say P_7. Note that $P_7 \lhd G$ and P_7 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 $H = \langle y \rangle$ with $y^3 = 1$. Since $P_7 \lhd G$, we have $yxy^{-1} = x^i$ for some $0 \le i \le 6$. It follows that

$$\begin{aligned} x = y^3xy^{-3} &= y^2(yxy^{-1})y^{-2} = y^2x^iy^{-2} \\ &= y(yx^iy^{-1})y^{-1} = yx^{i^2}y^{-1} = x^{i^3}. \end{aligned}$$

Since $x = x^{i^3}$ and $x^7 = 1$, we have $i^3 - 1 \equiv 0 \pmod 7$. Since $0 \le i \le 6$, we have $i = 1, 2, 4$. □

Remark.

(1) If $i = 1$, then $yxy^{-1} = x$, i.e. $yx = xy$. Thus, G is an abelian group and $G \cong \mathbb{Z}_{21}$. (Note that $P_3 \lhd G$ and $P_7 \cap P_3 = \{1\}$ and $|G| = |P_7|\,|P_3|$).

(2) If $i = 2$, then $yxy^{-1} = x^2$. Thus, $G = \{x^iy^j : 0 \le i \le 6, 0 \le j \le 2, yxy^{-1} = x^2\}$.

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

$$y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^4y^{-1} = x^{16} = x^2.$$

Note that y^2 is also a generator of H. Then by replacing y by y^2, we get back to Case (2). It follows that there are two isomorphism classes of group of order 21.

7 Finite Abelian Groups

7.1 Primary Decomposition

Definition 7.1 (Notation).
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 $1 = 1^m \in G^{(m)}$. Also, if $g, h \in G^{(m)}$ since G is abelian, we have $(gh)^m = g^m h^m = 1$ and thus $gh \in G^{(m)}$. Finally, if $g \in G^{(m)}$, we have $(g^{-1})^m = g^{-m} = (g^m)^{-1} = 1$ and thus $g^{-1} \in G^{(m)}$. By the Subgroup Test, $G^{(m)}$ is a subgroup of G. □

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) $\left|G^{(m)}\right| = m$ and $\left|G^{(k)}\right| = k$.

Proof.

(1) Since G is abelian, we have $G^{(m)} \trianglelefteq G$ and $G^{(k)} \trianglelefteq G$. Also, since $\gcd(m, k) = 1$, $\exists x, y \in \mathbb{Z}$ s.t. $mx + ky = 1$.

Claim (1). $G^{(m)} \cap G^{(k)} = \{1\}$.

proof of Claim 1. If $g \in G^{(m)} \cap G^{(k)}$, then $g^m = 1 = g^k$. We have

$$g = g^{mx+ky} = (g^m)^x (g^k)^y = 1^x 1^y = 1.$$

The claim follows. □

Claim (2). $G = G^{(m)} G^{(k)}$.

proof of Claim 2. If $g \in G$, then

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

It follows that $g^k \in G^{(m)}$ and $g^m \in G^{(k)}$. Thus, $g = g^{mx+ky} = (g^k)^y (g^m)^x \in G^{(m)}G^{(k)}$. □

Combining Claim 1 and Claim 2, by Theorem 3.14, we have $G \cong G^{(m)} \times G^{(k)}$.

(2) Write $\left|G^{(m)}\right| = m'$ and $\left|G^{(k)}\right| = k'$. By (1), we have $mk = |G| = m'k'$.

Claim. $\gcd(m, k') = 1$.

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

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

By (1), we have $g \in G^{(m)} \cap G^{(k)} = \{1\}$, 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 $mk = m'k'$, it follows that $m = m'$ and $k = k'$. □

□

Lecture 19

As a direct consequence of Proposition 7.2.

Theorem 7.3 (**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) $\left|G^{(p_i^{n_i})}\right| = p_i^{n_i}$ with $1 \leq i \leq k$.

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

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

and

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

By Theorem 7.3, we have $\mathbb{Z}_{13}^* \cong \{1, 5, 8, 12\} \times \{1, 3, 9\}$.

7.2 Structure Theorem of Finite Abelian Groups

By Theorem 7.3, to understand finite abelian groups, it suffices to consider finite abelian groups of prime power order. We recall that if $|G| = p$, then $G \cong \mathbb{Z}_p$. If $|G| = p^2$, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Question: How about when $|G| = p^3, p^4, \ldots$?

Proposition 7.4.
If G is a finite abelian p-group that contains only one subgroup of order p, then G is cyclic.
In other words, if a finite abelian p-group G is not cyclic, then G has at least two subgroups of order p.

Proof. Let $y \in G$ be of maximal order, i.e. $o(y) \geq o(x)\ \forall x \in G$.

Claim. $G = \langle y \rangle$.

proof of Claim. Suppose that $G \neq \langle y \rangle$. Then, the quotient group $G/\langle y \rangle$ is a non-trivial p-group, which contains an element z of order p by Cauchy's Theorem. In particular, $z \neq 1$. Consider the coset map $\pi : G \to G/\langle y \rangle$. Let $x \in G$ s.t. $\pi(x) = z$. 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 $m \in \mathbb{Z}$. We consider two cases:

Case 1: $p \nmid m$.

If $p \nmid m$, since $o(y) = p^r$ for some $r \in \mathbb{N}$,by Proposition 2.12, $o(y^m) = o(y) = p^r$. Since y is of max order, we have

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

which leads to a contradiction.

Case 2: $p \mid m$.

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 subgroup of order p in G, say H. On the other hand, the cyclic group $\langle y \rangle$ contains a subgroup of order p, which must be the one and only H. Thus, $xy^{-k} \in \langle y \rangle$, which implies that $x \in \langle y \rangle$. It follows that $z = \pi(x) = 1$, which is a contradiction. By combining the above two cases, we see that $G = \langle y \rangle$. □

□

Proposition 7.5. Let $G \neq \{1\}$ be a finite abelian p-group and let C be a cyclic subgroup of max order. Then G contains a subgroup B such that $G = CB$ and $C \cap B = \{1\}$.
Thus by Theorem 3.14, we have $G \cong C \times B$.

Theorem 7.6. Let $G \neq \{1\}$ be a finite abelian p-group. Then G is isomorphic to a direct product of cyclic groups.

Proof. By Proposition 7.5, there exists a cyclic group C_1 and a subgroup B_1 of G s.t. $G \cong C_1 \times B_1$. Since $|B_1| \mid |G|$ by Lagrange's Theorem, the group B_1 is also a p-group. Thus if $B_1 \neq \{1\}$, by Proposition 7.5, there exists a cyclic group C_2 and a subgroup B_2 s.t. $B_1 \cong C_2 \times B_2$. By repeating this process to get cyclic groups $C_1, C_2, \dots, C_k$ until we get $B_k = \{1\}$ for some $k \in \mathbb{N}$. Then

$$G \cong C_1 \times C_2 \times \cdots \times C_k.$$

□

Remark. One can show that the decomposition of a finite abelian p-group into a direct product of cyclic groups is unique up to their orders. Moreover, one can show (see Piazza) that if G is a finite abelian p-group and $G \cong C_1 \times \cdots \times C_k \cong D_1 \times \cdots \times D_l$ are two decompositions of G as products of cyclic group C_i and D_j of order p^{n_i} and p^{m_j} respectively. Then, $k = l$ and after a suitable rearrangement, we have $n_1 = m_1, n_2 = m_2, \dots, n_k = m_k$.

Lecture 20

Proof of Proposition 7.5. We prove this result by induction. If $|G| = p$, we take $C = G$ and $B = \{1\}$, then 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 $|G| = p^n$. There are two cases:

Case 1: If $G = C$, then by taking $B = \{1\}$, the result follows.

Case 2: If $G \neq C$, then G is not cyclic. By Proposition 7.4, there exists at least two subgroups of order p. Since C is cyclic, by Theorem 2.13, it contains exactly one subgroup of order p. Thus, there exists a subgroup D of G with $|D| = p$ and $D \nsubseteq C$. Since $|D| = p$ and $D \nsubseteq C$, 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 $\operatorname{Ker} \pi|_C = C \cap D = \{1\}$.

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

Claim (1). $G = CB$.

Proof of Claim 1. Note that since E is a subgroup containing $\{1\}$, we have $\pi^{-1}(\{1\}) = D \subseteq B$. If $x \in G$, since $\pi(C)\pi(B) = \pi(C)E = G/D$, $\exists u \in C$ and $v \in B$ s.t. $\pi(x) = \pi(u)\pi(v)$. 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). $C \cap B = \{1\}$.

Proof of Claim 2. Let $x \in C \cap B$. Then $\pi(x) \in \pi(C) \cap \pi(B) = \pi(C) \cap E = \{1\}$. Since $\pi(x) = 1 in G/D$, we have $x \in D$. Since $x \in C \cap D = \{1\}$, we have $x = 1$. By combining Claim 1 and Claim 2, the result follows. □

□

Remark.

1. The restriction of π on C, $\pi|_C$, means that we restrict the domain of π to work solely for the subset C. In plain words, we are only considering the case where π is applied onto elements of C.
2. π^{-1} is the pre-image of E (π is not a bijection, so do not have an inverse).

Theorem 7.7 (**Structure Theorem of Finite Abelian Groups**).
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 $p_i^{n_i}$ $(1 \leq i \leq k)$. Note that p_i are not necessarily distinct. The number $p_i^{n_i}$ are uniquely determined up to the order.

Remark. Note that if p_1, p_2 are distinct primes, then

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

Hence we have the following theorem (useful in PMATH 348).

Theorem 7.8 (**Invariant Factor Decomposition of Finite Abelian Groups**).
Let G be a finite abelian group. Then

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

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

Example. Let G be an abelian group of order $48 = 2^4 \cdot 3$. By Theorem 7.3, $G \cong H \times \mathbb{Z}_3$, where H is an abelian group of order 2^4. The options for H are

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

Thus, we have

$$G \cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48}$$
$$G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_{24}$$
$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_{12}$$
$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6.$$

Lecture 21

8 Rings

8.1 Rings

Definition 8.1 (**Ring**). A set R is a (unitary) **ring** if it has 2 operations, addition $+$ and multiplication $\cdot$, such that $(R,+)$ is an abelian group and $(R,\cdot)$ satisfies closure, associativity and identity properties of a group, in addition to the distributive law.

More precisely, if R is a ring, then for all $a,b,c \in R$, we have

(1) $a+b \in R$.

(2) $a+b=b+a$.

(3) $a+(b+c)=(a+b)+C$.

(4) There exists $0 \in R$ s.t. $a+0=a=0+a$, 0 is called the zero of R.

(5) There exists $-a \in R$ s.t. $a+(-a)=0=(-a)+a$, $-a$ is called the inverse of a.

(6) $ab := a \cdot b \in R$.

(7) $a(bc)=(ab)c$.

(8) There exists $1 \in R$ s.t. $a1=a=1a$, 1 is called the unity of R.

(9) $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$ (distributive law).

The ring R is called a commutative ring if is also satisfy:

(10) $ab=ba$.

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

Example. 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. 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 O and the unity being the identity matrix I. Note that $M_n(\mathbb{R})$ is not commutative.

Remark (**Warning**). Note that since $(R,\cdot)$ is not a group, there is no left or right cancellation. For example, in $\mathbb{Z}$, $0 \cdot x = 0 = 0 \cdot y$ does not imply $x=y$.

Definition 8.2 (**Notation**). Given a ring R, to distinguish the difference between multiples in addition and in multiplication, for $n \in \mathbb{N}$ and $a \in R$, we write

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

and

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

We recall that for a group G and $g \in G$, we have $g^0 = 1$, $g^1 = g$, and $(g^{-1})^{-1} = g$. Thus for addition, we have $\underbrace{0}_{\text{integer}} a = \underbrace{0}_{0 \text{ in } R}$, $1a = a$, and $-(-a) = a$.
For $n \in \mathbb{N}$, we define

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

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

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

Also, by Proposition 1.2, for $n, m \in \mathbb{Z}$, we have $(na) + (ma) = (n+m)a$, $n(ma) = (nm)a$, and $n(a+b) = na + nb$.

Exercise: One can prove the following.

Proposition 8.1. Let R be a ring and $r, s \in R$.

(1) If 0 is the zero of R, then $0r = 0 = r0$ (all 0's are zeros of R).

(2) $(-r)s = r(-s) = -(rs)$.

(3) $(-r)(-s) = rs$.

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

Definition 8.3 (**Trivial Ring**).
A **trivial ring** is a ring of only one element. In this case, we have $1 = 0$.

Remark. If R is a ring with $R \neq \{0\}$, since $r = r \cdot 1 \ \forall r \in R$, we have $1 \neq 0$ (otherwise, $r = r1 = r0 = 0$ by Proposition 8.1).

Example (**Direct Product**). Let $R_1, \dots, R_n$ be rings. We define component-wise operations on the product $R_1 \times \cdots \times R_n$ as follows

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

One can check that $R_1 \times \cdots \times R_n$ is a ring with zero being $(0_{R_1}, \dots, 0_{R_n})$ and the unity being $(1_{R_1}, \dots, 1_{R_n})$. This set $R_1 \times \cdots \times R_n$ is called the direct product of $R_1 \dots, R_n$.

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 $(R, +)$:

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

For $k \in \mathbb{Z}$, we write $kR = 0$ to mean that $kr = 0$ for all $r \in R$. By Proposition 8.1, we have

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

Thus, $kR = 0 \iff k1_R = 0$.

By Propsition 2.7 and 2.8, we have the following.

Proposition 8.2. Let R be a ring and $k \in \mathbb{Z}$.

(1) If $\mathrm{ch}(R) = n \in \mathbb{N}$, then $kR = 0 \iff n \mid k$.

(2) If $\mathrm{ch}(R) = 0$, then $kR = 0 \iff k = 0$.

Example. Each of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ has characteristic 0. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ has characteristic n.

Lecture 22

8.2 Subrings

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).

Note. Properties (2), (3), (7), (9) of rings are automatically satisfied. Thus, to show that S is a subring, it suffices to show the Subring Test.

Theorem 8.3 (**Subring Test**).

(1) $1_R \in S$.

(2) If $s, t \in S$, then $st \in S$ and $s - t \in S$.

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

Example. We have a chain of commutative rings:

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

Example (**Center of a Ring**). If R is a ring, the center $Z(R)$ of R is defined as

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

Note that $1_R \in Z(R)$. Also, if $s, t \in Z(R)$, then for all $r \in R$, we have

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

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

Note. Addition is already commutative.

Example. Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$. Then one can show that $\mathbb{Z}[i]$ 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:

$$R/A = \{r + A : r \in R\} \text{ with } r + A = \{r + a : a \in A\}.$$

Using the known properties about cosets and quotient groups, we have the following.

Proposition 8.4. Let R be a ring and A an additive subgroup of R. For $r, s \in R$, we have

(1) $r + A = s + A \iff r - s \in A$.

(2) $(r + A) + (s + A) = (r + s) + A$.

(3) $0 + A = A$ is the additive identity of R/A.

(4) $-(r + A) = (-r) + A$.

(5) $k(r + A) = kr + A$ for $k \in \mathbb{Z}$.

Note. These are just a translation of the properties of cosets and quotient groups to the language of addition in rings.

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

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

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

$$r + A = r_1 + A \text{ and } s + A = s_1 + A \implies rs + A = r_1 s_1 + A.$$

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

Proposition 8.5. Let A be an additive subgroup of a ring R.

For $a \in A$, define $Ra = \{ra : r \in R\}$ and $aR = \{ar : r \in R\}$. The following are equivalent:

(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.

Proof.

(1) $\implies$ (2): If $r + A = r_1 + A$ and $s + A = s_1 + A$, we need to show that $rs + A = r_1 s_1 + A$. Since $(r - r_1) \in A$ and $(s - s_1) \in A$ by Proposition 8.4 (1), we have

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

Thus, $rs + A = r_1 s_1 + A$ by Proposition 8.4 (1).

(2) $\implies$ (1): Let $r \in R$ and $a \in A$. By Proposition 8.1 (1), we have

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

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

Definition 8.6 (**Ideal**). An additive subgroup A of a ring R is an **ideal** of R if $Ra \subseteq A$ (left ideal) and $aR \subseteq A$ (right ideal) for all $a \in A$.

Note. Thus a subset 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 $ra, ar \in A$. Also, ideal in ring theory is like normal subgroup in group theory.

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

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

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

Then one can show that I is an ideal of R (see Piazza).

Lecture 23

Proposition 8.6. 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 of R and $1_R \in A$, we have $r = r1_R \in A$. It follows that $R1_R = R \subseteq A$. Thus, $A = R$. □

Remark. This shows that if we want a non-trivial ideal, then the ideal should not contain the 1.

Proposition 8.7. Let A be an ideal of a ring R. Then the additive quotient group R/A is a ring with the multiplication $(r + A)(s + A) = rs + A$ for all $r, s \in R$, and the unity of R/A is $1 + A$.

Proof. Since A is an additive subgroup of a ring R, we have R/A is an additive abelian group. By Proposition 8.5, the multiplication on R/A is well-defined. The multiplication is associative, since $\forall r, s, t \in R$, we have

$$\begin{aligned}(r + A)((s + A)(t + A)) &= (r + A)(st + A) = rst + A \\ &= (rs + A)(t + A) \\ &= ((r + A)(s + A))(t + A).\end{aligned}$$

We also have

$$(r + A)(1 + A) = r + A = (1 + A)(r + A)$$

and so the unity of R/A is $1 + A$. The distributive property is inherited from R. □

Definition 8.7 (**Quotient Ring**).
Let A be an ideal of a ring R. The ring R/A is called the **quotient ring** of R by A.

Definition 8.8 (**Principal 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 the **principal ideal** generated by a and denote by $A = \langle a \rangle$.

Example. If $n \in \mathbb{Z}$, then $\langle n \rangle = n\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$, since $\mathbb{Z}$ is commutative.

Proposition 8.8. 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 $\mathbb{Z}$. Note that if $A = \{0\}$, then $A = \langle 0 \rangle$. Otherwise, choose $a \in A$ with $a \neq 0$ such that $|a|$ is minimal. Clearly, $\langle a \rangle = a\mathbb{Z} \subseteq A$. To prove the other inclusion, let $b \in A$. By the Division Algorithm, we can write $b = qa + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < |a|$. If $r \neq 0$, since A is an ideal and $a, b \in A$, we have $qa \in A$ and hence $r = b - qa \in A$. Note that $|r| < |a|$, which contradicts that $|a|$ is minimal. Thus, $r = 0$, $b = qa \in \langle a \rangle$ and so $A \subseteq \langle a \rangle$. Thus, $A = \langle a \rangle$. □

8.4 Ring Isomorphism Theorems

Definition 8.9 (**Ring Homomorphism**).
Let R, S be rings. A mapping $\theta : R \to S$ is a **ring homomorphism** if $\forall a, b \in R$, we have

(1) $\theta(a + b) = \theta(a) + \theta(b)$.

(2) $\theta(ab) = \theta(a)\theta(b)$.

(3) $\theta(1_R) = 1_S$.

Remark. Note that (2) $\not\Longrightarrow$ (3) because $\theta(1_R) \in S$ does not necessarily have a multiplicative inverse, since S is a ring.

Example. The mapping $k \mapsto [k]$ from $\mathbb{Z}$ to $\mathbb{Z}_n$ is a surjective ring homomorphism.

Example. If R_1, R_2 are rings, the projection

$$\pi_1 : R_1 \times R_2 \to R_1 \quad \text{by} \quad \pi_1(r_1, r_2) = r_1$$

is a surjective ring homomorphism. So is $\pi_2 : R_1 \times R_2 \to R_2$ by $\pi_2(r_1, r_2) = r_2$.

Proposition 8.9 (**Properties of Ring Homomorphism**).
Let $\theta : R \to S$ be a ring homomorphism and let $r \in R$. Then

(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 $u \in R^*$, the set of elements of R with multiplicative inverse, such u is called a unit of R, then $\theta(u^n) = \theta(u)^n$ for all $n \in \mathbb{Z}$.

Proof.

(1) Note that $\theta(r) = \theta(0_R + r) = \theta(0_R) + \theta(r)$. Thus, $\theta(0_R) = 0_S$.

(2) Note that $0_S = \theta(0_R) = \theta(r + (-r)) = \theta(r) + \theta(-r)$. Thus, $\theta(-r) = -\theta(r)$.

(3) Oberve that $\theta(kr) = \theta(\underbrace{r + \cdots + r}_{k \text{ times}}) = \underbrace{\theta(r) + \cdots + \theta(r)}_{k \text{ times}} = k\theta(r)$.

(4) Follows by induction on the definition of a ring homomorphism.

(5) Follows as a result from (4) because if $u \in R^*$, then $u^{-1} \in R^*$ such that $uu^{-1} = 1_R$.

□

Definition 8.10 (**Ring Isomorhpism**).
Let R, S be rings. A mapping $\theta : R \to S$ is a **ring isomomorphism** if θ is a bijective ring homomorphism. In this case, we say that R and S are **isomorphic** and write $R \cong S$.

Lecture 24

Definition 8.11 (**Kernel, Image**).
Let $\theta : R \to S$ be a ring homomorphism. The **kernel** of θ is defined by

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

and the **image** of θ is defined by

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

We have learned from group theory that $\operatorname{Ker}\theta$ and $\operatorname{im}\theta$ are additive subgroups of R and S, respectively.

Proposition 8.10. Let $\theta : R \to S$ be a ring homomorphism. Then

(1) $\operatorname{im}\theta$ is a subring of S.

(2) $\operatorname{Ker}\theta$ is an ideal of R.

Proof.

(1) Since $\operatorname{im}\theta = \theta(R)$ is an additive subgroup of S, it suffices to show that $\theta(R)$ is closed under multiplication and $1_S \in \theta(R)$. Note that $1_S = \theta(1_R) \in \theta(R)$. Also, 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.

(2) Since $\operatorname{Ker}\theta$ is an additive subgroup of R, it suffices to show that $ra, ar \in \operatorname{Ker}\theta$ for all $r \in R$ and $a \in \operatorname{Ker}\theta$. If $r \in R$ and $a \in \operatorname{Ker}\theta$, then

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

Thus, $ra \in \operatorname{Ker}\theta$. Similarly, $ar \in \operatorname{Ker}\theta$. Thus, $\operatorname{Ker}\theta$ is an ideal of R.

□

Theorem 8.11 (First Ring Isomorphism Theorem).
Let $\theta : R \to S$ be a ring homomorphism. We have

$$R/\operatorname{Ker}\theta \cong \operatorname{im}\theta.$$

Proof. Let $A = \operatorname{Ker}\theta$. Since A is an ideal, we have R/A is a ring. Define the ring map

$$\overline{\theta} : R/A \to \operatorname{im}\theta \quad \text{by} \quad \overline{\theta}(r + A) = \theta(r) \ \ \forall r + A \in R/A.$$

Note that

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

Thus, $\overline{\theta}$ is well-defined and one-to-one. Also, $\overline{\theta}$ is clearly onto. One can show that $\overline{\theta}$ is a ring homomorphism. It follows that $\overline{\theta}$ is an isomorphism and $R/\operatorname{Ker}\theta \cong \operatorname{im}\theta$. □

Example (**Exercise**). 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 of R 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

$$A + B = \{a + b : a \in A \text{ and } b \in B\}.$$

Then, one can show the following Proposition (Piazza Exercise).

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.

Using the First Ring Isomorphism Theorem, one can show the following (see A7).

Theorem 8.13 (**Second Ring 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

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

Theorem 8.14 (**Third Ring Isomorphism Theorem**).
Let A and B be ideals of a ring R with $A \subseteq B$. Then B/A is an ideal of R/A and

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

Theorem 8.15 (**Chinese Remainder Theorem**).
Let A and B be ideals of a ring 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. Since (2) is a direct consequence of (1), it suffices to prove (1). Define

$$\theta : R \to R/A \times R/B \quad \text{by} \quad \theta(r) = (r + A, r + B) \ \ \forall r \in R.$$

Then θ is a ring homomorphism (exercise). Also, $\operatorname{Ker}\theta = A \cap B$.

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 exists $a \in A$ and $b \in B$ s.t. $a + b = 1$. Let $r = sb + ta$. Then

$$s - r = s - sb - ta = s(1 - b) - ta = sa - ta = (s - t)a \in A$$
$$t - r = t - sb - ta = t(1 - a) - sb = tb - sb = (t - s)b \in B.$$

Thus, $s + A = r + A$ and $t + B = r + B$. Thus, $\theta(r) = (r + A, r + B) = (s + A, t + B)$. By the First Ring Isomorphism Theorem, we have $R/(A \cap B) \cong R/A \times R/B$. □

Example (Why is above called the Chinese Remainder Theorem?)**.** Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. By Bezout's lemma, we have $1 = mr + ns$ for some $r, s \in \mathbb{Z}$. 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 $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$. By the Chinese Remainder Theorem, we have the following.

Corollary 8.16.

(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's φ-function.

Proof.

(1) Follows from the Chinese Remainder Theorem.

(2) From (1), we have $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

□

Remark. By Corollary 8.16, for $[a] \in \mathbb{Z}_m$ and $[b] \in \mathbb{Z}_n$, there exists a unique $[c] \in \mathbb{Z}_{mn}$ s.t. $[c] = [a]$ in $\mathbb{Z}_m$ and $[c] = [b]$ in $\mathbb{Z}_n$, i.e. it is equivalent to say that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ has a unique solution $x \equiv c \pmod{mn}$.

Lecture 25

Example. Combining the Third Ring Isomorphism Theorem and the fact that all ideals of $\mathbb{Z}$ are principal, we have all ideals of $\mathbb{Z}_n$ are principal.

Let p be a prime. Recall that a consequence of Lagrange's Theorem is that every group of prime order is cyclic, i.e. $G \cong C_p$. Thus, we have an analogous result for rings as follows.

Proposition 8.17. If R is a ring with $|R| = p$ where p is prime. then $R \cong \mathbb{Z}_p$.

Proof. Define $\theta : \mathbb{Z}_p \to R$ by $\theta([k]) = k \cdot 1_R$. Note that since R is an additive group with $|R| = p$, then $o(1_R) = 1$ or p. Since $1_R \neq 0_R$, we have $o(1_R) = p$. Thus by Proposition 8.2, we have

$$[k] = [m] \iff p \mid k - m \iff (k-m)1_R = 0_R \iff k1_R = m1_R.$$

Thus, θ is well-defined and one-to-one. Also, θ is a ring homomorphism (exercise). Since $|R| = |\mathbb{Z}_p|$ and θ is one-to-one, we have θ is onto and hence θ is an isomorphism, and $R \cong \mathbb{Z}_p$. □

We have seen in a group G with $|G| = p^2$, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.
Super Piazza Exercise: What are the possible rings R with $|R| = p^2$?

9 Commutative Rings

9.1 Integral Domains and Fields

Definition 9.1 (**Units**). Let R be a ring. We say that $u \in R$ is a **unit** if u has a multiplicative inverse in R denoted it by u^{-1}. We have $uu^{-1} = 1 = u^{-1}u$.

Note. If $u \in R$ is a unit and $r, s \in R$, we have

$$ur = us \implies r = s \quad \text{Left Cancellation}$$
$$ru = su \implies r = s \quad \text{Right Cancellation.}$$

Let R^* denote the set of all units in R. One can show that $(R^*, \cdot)$ is a group, and is called the group of units of R.

Example. Note that 2 is a unit in $\mathbb{Q}$, but it is not a unit in $\mathbb{Z}$. We have $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ and $\mathbb{Z}^* = \{1, -1\}$.

Exercise: Consider the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\} \subseteq \mathbb{C}$. 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 $N(a) = 1 \iff a \in \mathbb{Z}[i]^*$ is a unit.

Definition 9.2 (**Division Ring, Field**).
A ring $R \neq \{0\}$ is a **division ring** if $R^* = R \setminus \{0\}$. In other words, every non-zero element of R is a unit in R. A commutative division ring is called a **field**.

Example. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.

Example. $\mathbb{Z}_n$ is a field $\iff$ n is prime.
This is because the equation $[a][x] = [1]$ in $\mathbb{Z}_n$ has a solution $\iff \gcd(a, n) = 1$. Thus if $n = p$ is prime, then $\gcd(a, p) = 1$ for all $a \in \{1, 2, \ldots, p-1\}$. Thus, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, and $\mathbb{Z}_p$ is a field. However, if n is not prime, say $n = ab$ with $1 < a, b < n$, then the non-zero

congruence classes $[a], [b]$ are not units in $\mathbb{Z}_n$ as there is no solution for $[a][x] = [1]$ and hence $\mathbb{Z}_n^* \neq \mathbb{Z}_n \setminus \{0\}$. Thus, $\mathbb{Z}_n$ is a field $\iff$ n is prime.

Remark. If R is a field, its only ideals are $\{0\}$ and R since if $A \neq \{0\}$ is an ideal of R then $\exists a \in A$, $a \neq 0$ s.t. $1 = aa^{-1} \in A$. By Proposition 8.6, $A = R$. As a consequence, if we have a ring homomorphism θ from a field F to a ring S, since $\operatorname{Ker}\theta$ is an ideal, $\operatorname{Ker}\theta = \{0\}$ or F. Hence, θ is injective or the zero map.

Super Piazza Exercise: Prove Wedderburn's Little Theorem: every finite division ring is a field.

Lecture 26

Note that to solve $x^2 - x - 6 = 0$ in $\mathbb{Z}$, we write $(x-3)(x+2) = 0$. This gives $x = 3$ or $x = -2$. However, in $\mathbb{Z}_6$, we have $[2][3] = [0]$. Hence if we have $[x-3][x-2] = [0]$, it does not necessarily mean that $[x] = [3]$ or $[-2]$ (exercise).

Definition 9.3 (**Zero Divisor**). Let $R \neq \{0\}$ be a ring. For $0 \neq a \in R$, we say that a is a **zero divisor** if $\exists 0 \neq b \in R$ s.t. $ab = 0$.

Example. In $\mathbb{Z}_6$, $[2], [3], [4]$ are zero divisors, since $[2][3] = [0] = [4][3]$.

Example. The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{R})$ since

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Proposition 9.1. Given a ring R, the following are equivalent:

(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. We prove (1) $\iff$ (2) and the proof for (1) $\iff$ (3) is similar.

(1) $\implies$ (2): Let $ab = ac$ with $a \neq 0$. Then $a(b-c) = 0$. By (1), since $a \neq 0$, we have $b - c = 0$ and hence $b = c$.

(2) $\implies$ (1): Let $ab = 0$ in R. Consider two cases:

Case 1: If $a = 0$, then we are done.

Case 2: If $a \neq 0$, then $ab = 0 = a0$. By (2), since $a \neq 0$, we have $b = 0$. □

Definition 9.4 (**Integral Domain**). A commutative ring $R \neq \{0\}$ is an **integral domain** if it has no zero divisors, i.e. if $ab = 0$ in R, then $a = 0$ or $b = 0$.

Example. $\mathbb{Z}$ is an integral domain.

Example. Note that 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 $\iff$ n is prime.

Proposition 9.2. Every field is an integral domain.

Proof. Let $ab = 0$ in a field R. We want to show that $a = 0$ or $b = 0$. Consider two cases:

(1) If $a = 0$, then we are done.

(2) If $a \neq 0$, since R is a field, $a \in R^*$ and there exists $a^{-1} \in R$. Then

$$b = 1 \cdot b = (a^{-1} \cdot a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

Thus, R is an integral domain.

□

Remark. Using the same proof, one can show that every subring of a field is an integral domain.

Remark. The converse of Proposition 9.2 is not true. For example, $\mathbb{Z}$ is an integral domain but not a field.

Example. The Gaussian ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$ is an integral domain (exercise). Since $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$, $\mathbb{Z}[i]$ 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, $ar = as$ and $a \neq 0 \implies r = s$. Hence, θ is injective. Since R is finite, θ is also surjective. In particular, $\exists b \in R$ s.t. $ab = 1$. Since R is commutative, we have $ab = 1 = ba$, i.e. a is a unit in R. Thus, $R^* = R \setminus \{0\}$ and hence R is a field. □

We recall that the characteristic of a ring R, denoted by $\mathrm{ch}(R)$, is the order of 1_R in $(R, +)$. We write $\mathrm{ch}(R) = 0$ if $o(1_R) = \infty$ and $\mathrm{ch}(R) = n$ if $o(1_R) = n \in \mathbb{N}$.

Proposition 9.4. The characteristic of any integral domain is either 0 or a prime p.

Proof. Let R be an integral domain. Consider two cases:

(1) If $\mathrm{ch}(R) = 0$, then we are done.

(2) If $\mathrm{ch}(R) = n \in \mathbb{N}$, note that since $R \neq \{0\}$, we have $n \neq 1$. If $\mathrm{ch}(R) = n \in \mathbb{N} \setminus \{1\}$, suppose that n is not a prime, say $n = ab$ with $1 < a, b < n$. If 1 is the unity of R, then by Proposition 8.1, we have

$$(a \cdot 1)(b \cdot 1) = (a \cdot b) \cdot (1 \cdot 1) = n \cdot 1 = 0.$$

Since R is an integral domain, we have $a \cdot 1 = 0$ or $b \cdot 1 = 0$, which leads to a contradiction since $o(1_R) = n$. Thus, n must be a prime.

□

Lecture 27

Remark. Let R be an integral domain with $\mathrm{ch}(R) = p$, a prime. For $a, b \in R$, we have (Binomial Theorem):

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \cdots + \binom{p}{p-1} ab^{p-1} + b^p$$

Since p is a prime, we have $p \mid \binom{p}{i}$ for all $1 \leq i \leq p-1$. Since $\mathrm{ch}(R) = p$, 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 $b \in p\mathbb{Z}$. This motivates the following definition.

Definition 9.5 (**Prime Ideal**). Let R be a commutative ring. An 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. $\{0\}$ is a prime ideal of $\mathbb{Z}$.

Example. For $n \in \mathbb{N}$ with $n \geq 2$, $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z} \iff n$ is prime.

Proposition 9.5. If R is a commutative ring, then an ideal P of R is a prime ideal $\iff R/P$ is an integral domain.

Proof. Since R is a commutative ring, so is R/P. Note that

$$R/P \neq \{0\} \iff 0 + P \neq 1 + P \iff 1 \notin P \iff P \neq R.$$

Also, for $r, s \in R$, we have

$$\begin{aligned} P \text{ is a prime ideal} &\iff rs \in P \text{ implies that } r \in P \text{ or } s \in P \\ &\iff (r+P)(s+P) = 0 + P \text{ implies that } r + P = 0 + P \text{ or } s + P = 0 + P \\ &\iff R/P \text{ is an integral domain.} \end{aligned}$$

□

Definition 9.6 (**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 $A = R$.

Remark. Let M be a maximal ideal of R and $r \notin M$. Then the ideal $\langle r \rangle + M$ (exercise) is equal to R since $M \subseteq \langle r \rangle + M \subseteq R$ and $M \neq \langle r \rangle + M$.

Proposition 9.6. If R is a commutative ring, then an ideal M of R is a maximal ideal $\iff$ R/M is a field.

Proof. Since R is a commutative ring, so is R/M. Note that

$$R/M \neq \{0\} \iff 0 + M \neq 1 + M \iff 1 \notin M \iff M \neq R.$$

Also, for $r \in R$, note that $r \notin M \iff r + M \neq 0 + M$. Thus, we have

$$\begin{aligned} M \text{ is a maximal ideal} &\iff \langle r \rangle + M = R \text{ for any } r \notin M \\ &\iff 1 \in \langle r \rangle + M \text{ for any } r \notin M \\ &\iff \text{for any } r \notin M, \exists s \in R \text{ s.t. } 1 + M = rs + M \\ &\iff \text{for any } r + M \neq 0 + M, \exists s + M \in R/M \text{ s.t. } (r + M)(s + M) = 1 + M \\ &\iff R/M \text{ is a field.} \end{aligned}$$

□

Combining Proposition 9.2 (every field is an integral domain), 9.5 and 9.6, we have:

Corollary 9.7. Every maximal ideal of a commutative ring is a prime ideal.

Remark. The converse of this corollary is not true. For example, in $\mathbb{Z}$, $\{0\}$ is a prime ideal but not a maximal ideal.

Example. 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 $\theta(a+bx) = a+bi$. Also, one can check that $\operatorname{Ker} \theta = \langle x^2 + 1 \rangle$ (see Piazza). By the First Ring Isomorphism Theorem, we have $\mathbb{Z}[x]/\langle x^2 + 1 \rangle \cong \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is an integral domain but not a field, we conclude that the ideal $\langle x^2 + 1 \rangle$ is a prime ideal but not a maximal ideal.

9.3 Fields of Fractions

We have seen that every subring of a field is an integral domain. The converse also holds: every integral domain R is isomorphic to a subring of a field.

Lecture 28

Remark. An ideal P is a prime ideal $\iff$ R/P is an integral domain. An ideal M is a maximal idea $\iff$ R/M is a field. Our goal in this section is that given an integral domain R, we want to construct a field F of all fractions $\frac{r}{s}$ in R.

Let R be an integral domain and let $D = R \setminus \{0\}$. Consider the set

$$X = R \times D = \{(r, s) : r \in R, s \in D\}.$$

We say that

$$(r, s) \equiv (r_1, s_1) \iff rs_1 = r_1 s.$$

One can show that $\equiv$ is an equivalence relation. In particular,

(1) $(r, s) \equiv (r, s)$.

(2) $(r, s) \equiv (r_1, s_1) \iff (r_1, s_1) \equiv (r, s)$.

(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 that $R = \mathbb{Z}$, we can now define the fraction $\frac{r}{s}$ to be the equivalence class $[(r, s)]$ of the pairs (r, s) on X.

Definition 9.7 (**Fraction**). Let R be an integral domain, $D = R \setminus \{0\}$, and $X = R \times D$. The **fraction** $\frac{r}{s}$ is the equivalence class $[(r, s)]$ of the pairs $(r, s) \in X$.

Let F denote the set of all these fractions. That is,

$$F = \{[(r, s)] : r \in R, s \in D\} = \left\{\frac{r}{s} : r, s \in R, s \neq 0\right\}.$$

The addition and multiplication of F are defined to be

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + sr_1}{ss_1}$$
$$\frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

where $ss_1, rs_1 + r_1 s, rr_1$ are elements of R. Note that $ss_1 \neq 0$ since R is an integral domain and thus the operations are well-defined. Then one can show that with the above defined addition and multiplication, F becomes a field with the zero being $\frac{0}{1}$, and the unity being $\frac{1}{1}$. The negative of $\frac{r}{s}$ is $\frac{-r}{s}$. Moreover, if $\frac{r}{s} \neq 0$ in F, then $r \neq 0$ and thus $\frac{s}{r} \in F$. We have

$$\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{sr} = \frac{1}{1} \in F.$$

In addition, we have $R \cong R'$ where $R' = \left\{\frac{r}{1} : r \in R\right\} \subseteq F$. Thus, we have the following theorem.

Theorem 9.8. Let R be an integral domain. Then there exists a field F consisting of fractions $\frac{r}{s}$ with $r, s \in R$ and $s \neq 0$. By identifying $r = \frac{r}{1}$ for all $r \in R$, we can view R as a subring of F, such a field F is called the **field of fractions** of R.

Remark (**Ring of Fractions**).
Given an integral domain, one can generalize the above set $D = R \setminus \{0\}$ to any subsets $D \subseteq R$ satisfying the following conditions:

(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 $D^{-1}R$.

Remark (**Localization at Prime Ideal**).
If R is an integral domain and P is a prime ideal, take $D = R \setminus P$. Then D satisfies the above conditions. The resulting $D^{-1}R$ is called the **localization of** R **at prime ideal** P.

10 Polynomial Rings

10.1 Polynomials

Definition 10.1 (**Polynomials**). Let R be a ring and x be a variable. Let

$$R[x] = \left\{ f(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + a_m x^m \,:\, m \in \mathbb{N} \cup \{0\}, a_i \in R, 0 \le i \le m \right\}.$$

Since $f(x)$ is called a polynomial in x over R, if $a_m \neq 0$, we say that $f(x)$ has **degree** m, denoted by $\deg f = m$ and we say that a_m is the **leading coefficient** of $f(x)$.
Specially, when the leading coefficient is 1, we say that $f(x)$ is **monic**. Note that

$$f(x) = 0 \iff a_0 = a_1 = \cdots = a_m = 0.$$

We define $\deg 0 = -\infty$ (reason why will be discussed latter). Note that $f(x) = 0$ is also a **constant polynomial**.

Let

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \in R[x]$$
$$g(x) = b_0 + b_1 x + \cdots + b_n x^n \in R[x]$$

with $m \le n$. Then, we write $a_i = 0$ for any $m+1 \le i \le n$. We can define the addition and multiplication on $R[x]$ as follows:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1 x + \cdots + a_m x^m)(b_0 + b_1 x + \cdots + b_n x^n) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \cdots + (a_m b_n)x^{m+n} \\ &= c_0 + c_1 x + \cdots + c_{m+n} x^{m+n} \end{aligned}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0$ for $0 \le i \le m+n$.

Proposition 10.1. Let R be a ring and x be a variable.

(1) $R[x]$ is a ring with the above operations.

(2) R is a subring of $R[x]$.

(3) If $Z = Z(R)$ denote the center of R, then $Z(R[x]) = Z[x]$.

Proof.

(1) Exercise.

(2) R is the same as the set of constant polynomials in $R[x]$.

(3) Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in Z[x]$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n \in R[x]$. We have

$$f(x)g(x) = c_0 + c_1x + \cdots + c_ix^i + \cdots + c_{m+n}x^{m+n}$$

with $c_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$. Since $a_i \in Z$, we have$a_ib_j = b_ja_i$ for all i, j. Thus, we get $f(x)g(x) = g(x)f(x)$ for all $g(x) \in R[x]$ and hence $Z[x] \subseteq Z(R[x])$.

To show the other inclusion, let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in Z(R[x])$, then $f(x)b = bf(x)$ for all $b \in R \subseteq R[x]$. It follows that $a_ib = ba_i$ for all $0 \leq i \leq m$. It implies that $a_i \in Z$ and hence $Z(R[x]) \subseteq Z[x]$. Therefore, $Z(R[x]) = Z[x]$.

□

Lecture 29

Remark (**Warning**). 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. For example, there are only 4 different functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$ but there are infinitely many polynomials in $\mathbb{Z}_2[x]$ (infinite set).

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 $\deg(fg) = \deg(f) + \deg(g)$. This is called the product formula.

(3) The units in $R[x]$ are R^*, the units in R.

Proof. We will prove (1) and (2) together.

(1) & (2) Suppose that $f(x) \neq 0$ and $g(x) \neq 0$ are polynomials in $R[x]$, say $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$, with $a_m \neq 0$ and $b_n \neq 0$. Then, we have

$$f(x)g(x) = (a_mb_n)x^{m+n} + \cdots + (a_0b_0).$$

Since R is an integral domain, $a_mb_n \neq 0$ and hence $f(x)g(x) \neq 0$. It follows that $R[x]$ is an integral domain. Moreover, we see that

$$\deg(fg) = m + n = \deg(f) + \deg(g).$$

Thus, (1) and (2) follow.

(3) Let $u(x) \in R[x]$ be a unit with the inverse $v(x)$. Since $u(x)v(x) = 1$, we have

$$\deg(uv) = \deg(u) + \deg(v) = \deg(1) = 0.$$

Since $u(x)v(x) = 1$, we have $u(x) \neq 0$ and $v(x) \neq 0$. Since $\deg(u) \geq 0$ and $\deg(v) \geq 0$, the above equations imply that $\deg(u) = 0 = \deg(v)$. Thus, $u(x)$ and $v(x)$ are units in R and hence $R[x]^* \subseteq R^*$. Since $R^* \subseteq R[x]^*$, we have $R[x]^* = R^*$.

□

Remark. 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 when R is an integral domian.

Remark. To extend the product formula to 0, we define $\deg(0) = \pm\infty$.

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 10.2 (**Division of Polynomials**).
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 $\exists h(x) \in F[x]$ s.t. $g(x) = f(x)h(x)$.

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 $u(x), v(x) \in F[x]$.

Remark. (1) is TD in MATH 135 and (2) is DIC in MATH 135.

Proposition 10.4. Let F be a field and $f(x), g(x) \in F[x]$ be monic polynomials. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.

Remark. Polynomials being monic is analogous to integers being positive.

Lecture 30

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, $f(x) = r(x)s(x)f(x)$. By Proposition 10.2, we have $\deg(f) = \deg(r) + \deg(s) + \deg(f)$, which implies that $\deg(r) + \deg(s) = 0$. Thus, $f(x) = sg(x)$ for some $s \in F$. Since both $f(x)$ and $g(x)$ are monic, we have $s = 1$ and hence $f(x) = g(x)$. □

Proposition 10.5 (**Division Algorithm**). Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then, there exists unique $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x)f(x) + r(x) \quad \text{with } \deg(r) < \deg(f).$$

Note that this includes the case for $r = 0$.

Remark. This explains why we define $\deg(0) = -\infty$.

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 $g(x) = 0 \cdot f(x) + g(x)$ and we are done. Suppose that $n \geq m$ and that the result holds for all $g(x) \in F[x]$ with $\deg(g) < n$. Write $f(x) = a_0 + a_1x + \cdots + a_mx^m$ with $a_m \neq 0$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ with $b_n \neq 0$. Such F is a field, then a_m^{-1} exists. Consider

$$\begin{aligned} g_1(x) &= g(x) - b_n a_m^{-1} x^{n-m} f(x) \\ &= (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) - b_n a_m^{-1} x^{n-m}(a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0) \\ &= 0 \cdot x^n + (b_{n-1} - b_n a_m^{-1} a_{m-1}) x^{n-1} + \cdots \end{aligned}$$

Since $\deg(g_1) < n$, by induction, 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 $\deg(r) < m$. It follows that

$$\begin{aligned} g(x) &= g_1(x) + b_n a_m^{-1} x^{n-m} f(x) \\ &= (q_1(x)f(x) + r_1(x)) + b_n a_m^{-1} x^{n-m} f(x) \\ &= (q_1(x) + b_n a_m^{-1} x^{n-m}) f(x) + r_1(x). \end{aligned}$$

By taking $q(x) = q_1(x) + b_n a_m^{-1} x^{n-m}$ and $r(x) = r_1(x)$, the result follows.

To prove uniqueness, suppose that we also have $g(x) = q_1(x)f(x) + r_1(x)$ with $\deg(r_1) < m$. Then, we have

$$r(x) - r_1(x) = (q(x) - q_1(x))f(x).$$

If $q_1(x) - q(x) \neq 0$, we get

$$\deg(r - r_1) = \deg((q - q_1)f) = \deg(q - q_1) + \deg(f) \geq \deg(f),$$

which leads to a contradiction since $\deg(r - r_1) < \deg(f)$. Thus, $q_1(x) - q(x) = 0$ and hence $r(x) - r_1(x) = 0$. It follows that $q_1(x) = q(x)$ and $r_1(x) = r(x)$. □

Proposition 10.6. Let F be a field and $f(x), g(x) \in F[x]$ with $f(x) \neq 0$ and $g(x) \neq 0$. Then, $\exists d(x) \in F[x]$ 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 $u(x), v(x) \in F[x]$.

Note that if both $d(x)$ and $d_1(x)$ satisfy the above conditions, since $d(x) \mid d_1(x)$ and $d_1(x) \mid d(x)$ and both of them are monic, by Proposition 10.4, we have $d(x) = d_1(x)$. We call such $d(x)$ the **greatest common divisor** of $f(x)$ and $g(x)$, denoted by $d(x) = \gcd(f(x), g(x))$.

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 nonzero polynomials and thus contains monic polynomials (since F is a field, if $h(x) \in X$ with leading coefficient a, then $a^{-1}h(x) \in X$ and is monic). Among all monic polynomials in X, choose $d(x) = u(x)f(x) + v(x)g(x)$ of minimal degree. Then (1) and (4) are satisfied. For (3), if $e(x) \mid f(x)$ and $e(x) \mid g(x)$, since $d(x) = u(x)f(x)+v(x)g(x)$, by Proposition 10.3, we have $e(x) \mid d(x)$. It remains to prove (2). By the division algorithm, 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 $c \neq 0$ be the leading coefficient of $r(x)$. Since F is a field, c^{-1} exsts. The above expression of $r(x)$ shows that $c^{-1}r(x)$ is a monic polynomial in X with $\deg(c^{-1}r) = \deg(r) < \deg(d)$, which contradicts the choice of $d(x)$. Thus, $r(x) = 0$ and hence $d(x) \mid f(x)$. Similarly, we can show that $d(x) \mid g(x)$ and thus (2) is satisfied. □

Lecture 31

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 $b = \pm 1$ (note that ± 1 are the units in $\mathbb{Z}$).

Definition 10.3 (**Irreducible**). If F is a field, a polynomial $\ell(x) \neq 0$ in $F[x]$ is **irreducible** if $\deg(\ell) \geq 1$ and whenever $\ell(x) = \ell_1(x)\ell_2(x)$ in $F[x]$, we have $\deg(\ell_1) = 0$ or $\deg(\ell_2) = 0$ (degree 0 polynomials are the units in $F[x]$).

Remark. Polynomials that are not irreducible are **reducible**.

Example. If $\ell(x) \in F[x]$ satisfies $\deg(\ell) = 1$, then $\ell(x)$ is irreducible.

Example. If $\deg(f) = 2$ or 3, then f is irreducible $\iff$ $f(d) \neq 0$ for any $d \in F$ (see A10).

Example. 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 $\ell(x) \mid g(x)$.

Note. This is called Euclid's Lemma in MATH 135.

Proof. Suppose that $\ell(x) \mid f(x)g(x)$. Consider two cases:

(1) If $\ell(x) \mid f(x)$, then we are done.

(2) If $\ell(x) \nmid f(x)$, then $d(x) = \gcd(\ell(x), f(x)) = 1$. By Proposition 10.6, we have $1 = u(x)\ell(x) + v(x)f(x)$ for some $u(x), v(x) \in F[x]$. Then $g(x) = g(x)u(x)\ell(x) + g(x)v(x)f(x)$. Since $\ell(x) \mid \ell(x)$ and $\ell(x) \mid f(x)g(x)$, by Proposition 10.3, we have $\ell(x) \mid g(x)$.

□

Remark. Let $f_1(x), \ldots, f_n(x) \in F[x]$ and let $\ell(x) \in F[x]$ be irreducible. If $\ell(x) \mid f_1(x) \cdots f_n(x)$, by applying Proposition 10.7 repeatedly, we have $\ell(x) \mid f_i(x)$ for some i.

We will state some results (no proof) and then come back so that we can start working on A10.

Theorem 10.8 (Unique Factorization Theorem).
Let F be a field and $f(x) \in F[x]$ with $\deg(f) \geq 1$. Then we can write

$$f(x) = c\ell_1(x) \cdots \ell_m(x)$$

where $c \in F^*$ is a unit and $\ell_i(x)$ are monic irreducible polynomials in $F[x]$. This factorization is unique up to the order of ℓ_i.

Exercise: Use Theorem 10.8 to prove that there are ∞ many irreducible polynomials in $F[x]$.

We recall that in $\mathbb{Z}$, all ideals are of the form $\langle n \rangle = n\mathbb{Z}$ for some $n \in \mathbb{Z}$ and if $n \in \mathbb{N}$, then n is unique.

Proposition 10.9. 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 $\langle h(x)\rangle \neq 0$ and $h(x)$ is monic, then the generator is uniquely determined.

Proof. Let A be an ideal of $F[x]$. If $A = \{0\}$, then $A = \langle 0\rangle$. Assume that $A \neq \{0\}$, then it contains a nonzero polynomial. Since A is an ideal and F is a field, A contains a monic polynomial. Among all monic polynomials in A, choose $h(x) \in A$ of minimal degree. Clearly, $\langle h(x)\rangle \subseteq A$. To prove the other inclusion, let $f(x) \in A$. Bt the Division Algorithm, we have $f(x) = q(x)h(x) + r(x)$ for some $q(x), r(x) \in F[x]$ with $\deg(r) < \deg(h)$. If $r(x) \neq 0$, then let $u \neq 0$ be the leading coefficient of $r(x)$. Since A is an ideal of $F[x]$, 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 of degree less than $\deg(h)$, i.e. $\deg(u^{-1}r) = \deg(r) < \deg(h)$. This contradicts the choice of $h(x)$. Thus, $r(x) = 0$ and hence $f(x) = q(x)h(x) \in \langle h(x)\rangle$. Thus, $A \subseteq \langle h(x)\rangle$ and hence $A = \langle h(x)\rangle$.
To show uniqueness, suppose that $A = \langle h(x)\rangle = \langle k(x)\rangle$. Then we must have $h(x) \mid k(x)$ and $k(x) \mid h(x)$. Since both $h(x)$ and $k(x)$ are monic, by Proposition 10.4, we have $h(x) = k(x)$. □

Let A be a nonzero ideal of $F[x]$. By Proposition 10.9, we know that A is a principal ideal and can be written as $A = \langle h(x)\rangle$ for a unique monic polynomial $h(x) \in F[x]$. Suppose that $\deg(h) = m \geq 1$. Consider the unique quotient ring $R = {}^{F[x]}\!/_{A}$, and so we have

$$R = \{\bar{f}(x) = f(x) + A \,:\, f(x) \in F[x]\}.$$

Write $t = \bar{x} = x + A$, then by the Division Algorithm, one can show that

$$R = \{\bar{a}_0 + \bar{a}_1 t + \cdots + \bar{a}_{m-1}t^{m-1} \,:\, \bar{a}_i \in F\}.$$

Now consider the map $\theta : F \to R$ given by $\theta(a) = \bar{a} = a + A$. Since θ is not the zero map, and $\operatorname{Ker}\theta$ is an ideal of F, we have $\operatorname{Ker}\theta = \{0\}$. Thus θ is an injective ring homomorphism. Since $F \cong \theta(F)$, by identifying F with $\theta(F)$, we can write

$$R = \{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} \,:\, a_i \in F, h(t) = 0\}.$$

Moreover, in R, one can show that

$$a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} = b_0 + b_1 t + \cdots + b_{m-1}t^{m-1} \iff a_i = b_i \ \forall 1 \leq i \leq m-1$$

which gives us the following theorem.

Theorem 10.10. 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 a given By

$$R = \{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} : a_i \in F \text{ and } h(t) = 0\}$$

in which an element of R can be uniquely represented in the above form.

Remark. In $\mathbb{Z}$, when we divide an integer by n, the remainder satisfies $0 \leq r < n$, that is, $r \in \{0, 1, \ldots, n-1\}$. Then, we have

$$\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle = \{[0], [1], \ldots, [n-1]\} = \{0 + \langle n\rangle, 1 + \langle n\rangle, \ldots, (n-1) + \langle n\rangle\}.$$

This is analogous to the above theorem.

Example. Consider the ring $\mathbb{R}[x]$. Let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. By the above theorem, we have

$${}^{\mathbb{R}[x]}\!/_{\langle x^2+1\rangle} = \{a + bt : a, b \in \mathbb{R} \text{ and } t^2 + 1 = 0\} \cong \{a + bi : a, b \in \mathbb{R} \text{ and } i^2 = -1\} = \mathbb{C}.$$

Similarly, in $F[x]$, when we divide a polynomial by $h(x)$ of degree m, the remainder $r(x)$ satisfy $\deg(r) < m$, i.e. $r(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} \in F[x]$. Then we have

$$\begin{aligned} {}^{F[x]}\!/_{\langle h(x)\rangle} &= \{[0], [1], \ldots, [h(x)-1]\} \\ &= \{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} : a_i \in F \text{ and } h(t) = 0\}. \end{aligned}$$

We recall that $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ is a field (or integral domain) $\iff$ n is prime. The following is an analogue in $F[x]$.

Proposition 10.11. Let F be a field and $h(x) \in F[x]$ with $\deg(h) \geq 1$. The following are equivalent:

(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. In the previous example where $h(x) = x^2 + 1 \in \mathbb{R}[x]$, we see that $x^2 + 1$ is irreducible in $\mathbb{R}[x]$. Then, $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is a field (which is true since $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$).

Example (Construct a Field of 8 Elements).
Consider $x^3 + x + 1 \in \mathbb{Z}_2$. Since $x = 0$ and $x = 1$ are not roots of $x^3 + x + 1$, the polynomial is irreducible in $\mathbb{Z}_2$. 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. In fact, in this way we construct a field of 8 elements, since there are 2 choices for each of a, b, c and hence we have $2^3 = 8$ choices for the elements in the field. We will denote this field by $\mathbb{F}_8$.

Note. This is essentially different from $\mathbb{Z}_8$ since $\mathbb{Z}_8$ is not a field (i.e. some nonzero elements fails to have a multiplicative inverse).

Lecture 32

Filled out the missing parts and proofs from Lecture 31.

Lecture 33

Proof of Proposition 10.11. Write $A = \langle h(x) \rangle$.

(1) $\implies$ (2): A field is an integral domain.

(2) $\implies$ (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), 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) $\implies$ (1): Note that ${}^{F[x]}\!/_{A}$ is a commutative ring. Thus to show it is a field, it suffices to show 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, $f(x) \notin A$ and hence $h(x) \nmid f(x)$. Since $h(x)$ is irreducible and $h(x) \nmid f(x)$, we have $\gcd(f(x), h(x)) = 1$. By Proposition 10.6, $\exists u(x), v(x) \in F[x]$ such that $1 = u(x)f(x) + v(x)h(x)$. Thus,

$$(u(x) + A)(f(x) + A) = 1 + A \text{ (since } h(x) \in A).$$

It follows that $f(x) + A$ has an inverse in ${}^{F[x]}\!/_{A}$ and hence ${}^{F[x]}\!/_{\langle h(x) \rangle}$ is a field. □

Analogies between $\mathbb{Z}$ and $F[x]$ (F: field):

	$\mathbb{Z}$	$F[x]$
elements	m	$f(x)$
size	$\lvert m\rvert =$ absolute value	$\deg f$
units	$\{\pm 1\}$	$F^* = F \setminus \{0\}$
	$\mathbb{Z} \setminus \{0\} = \pm\mathbb{N}$	$F[x] \setminus \{0\} = \{h : h \text{ is monic}\}$
unique factorization	$m = \pm 1 p_1^{\alpha_1} \dots p_n^{\alpha_n}$	$f(x) = c\ell_1(x)^{\alpha_1} \dots \ell_r(x)^{\alpha_r}$
	p_i prime	$\deg f \geq 1, \ell_i$ are irreducible, $c \in F^*$
ideals	$\langle n\rangle$ (unique if $n \in \mathbb{N}$)	$\langle h(x)\rangle$ (unique if $h(x)$ is monic)
	$\mathbb{Z}/\langle n\rangle$ is a field	$F[x]/\langle h(x)\rangle$ is a field
	$\iff n$ prime	$\iff h(x)$ is irreducible

10.3 Fermat's Last Theorem in $F[x]$ (not on the exam)

We recall that Fermat's Last Theorem states that for $n \geq 3$, the equation

$$x^n + y^n = z^n$$

has no non-trivial solutions in $\mathbb{Z}$ (trivial solutions are like $(1, 0, 1)$).

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 that (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 10.12. 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 solutions for the equation

$$f(x)^n + g(x)^n = h(x)^n$$

with $f(x), g(x), h(x) \in F[x]$.

Proof. Suppose we have a non-trivial solution. WLOG, suppose that

$$\deg(f) = \deg(h) \geq \max\{\deg(g), 1\}.$$

Write $f'(x) = \frac{\mathrm{d}f}{\mathrm{d}x}$. Since we have $f^n + g^n = h^n$, by taking 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 multiplying both sides by h, we have

$$f^{n-1}f'h + g^{n-1}g'h = h^nh' = f^ng' + g^nf'$$

since $h^n = f^n + g^n$. 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, $(n-1)\deg(f) \leq \deg(g) + \deg(h) - 1$. Since $\deg(f) = \deg(h) \geq \deg(g)$, we have $(n-2)\deg(f) \leq \deg(g) - 1$, which gives a contradiction if $n \geq 3$. Thus, there is no non-trivial solutions of $f^n + g^n = h^n$ in $F[x]$. □

Lecture 34

10.4 Prime Number Theorem and Riemann Hypothesis (not on the exam)

Define $\pi(x) = \#\{p \leq x : p : \text{prime}\}$, i.e. $\pi(x)$ counts the number of primes p s.t. $p \leq x$.

Conjecture of Gauss

$$\pi(x) \sim \mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\log(t)}\, dx.$$

- The probability that a number is a prime is $\frac{1}{\log(x)}$. For example, for $n \in \mathbb{N}$ with $1 \leq n \leq e^{100}$, about 1% of them are prime.

Definition 10.4 (**Riemann Zeta Function**).

For $s \in \mathbb{C}$, the **Riemann zeta function** is defined to be

$$\begin{aligned}\zeta(s) = \sum_{n\in\mathbb{N}} \frac{1}{n^s} &= \prod_{p:\text{prime}} \frac{1}{1-p^{-s}} \\ &= \prod_{p:\text{prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right)\end{aligned}$$

- $\zeta(s)$ converges absolutely for $\mathrm{Re}(s) > 1$.
- $\zeta(s)$ can be extended to the whole $\mathbb{C}$.

Note. Take PMATH 440/640 Analytic Number Theory!

Definition 10.5 (**Riemann Hypothesis**).

There is no non-trivial zero for $\mathrm{Re}(s) > \frac{1}{2}$.

Theorem 10.13 (**Prime Number Theorem**). For any $n \in \mathbb{N}$,

$$\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{(\log(x))^n}\right).$$

Note. $O(f(x))$ means $Cf(x)$ for some constant C.

Assuming the Riemann Hypothesis, we have

$$\pi(x) = \mathrm{li}(x) + O(x^{\frac{1}{2}+\epsilon}) \quad \text{for any } \epsilon > 0.$$

Note. Proved by Hadamard and de la Vallée Poussin.

Let us 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 $\mathbb{Z}_p[t]$ is

$$\zeta_p(s) = \sum_{f:\text{monic}} \frac{1}{|f|^s} = \prod_{\substack{\ell:\text{monic}\\ \text{irreducible}}} \left(1 - \frac{1}{|\ell|^s}\right)^{-1}.$$

Note that $\#\{f \in \mathbb{Z}_p[x] : \text{monic}, \deg(f) = d\} = p^d$. 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 the following:

$$\begin{aligned}\pi_p(x) &= \#\{\ell : \text{monic irreducible}, |\ell| \le x\} \\ &= \frac{p}{p-1} \cdot \frac{x}{\log_p(x)} + O\left(x^{\frac{1}{2}+\epsilon}\right) \quad \text{for any } \epsilon > 0.\end{aligned}$$

$\longrightarrow$ Riemann Hypothesis holds in $\mathbb{Z}_p[x]$.

Question: Are problems in $F[x]$ always easier than in $\mathbb{Z}$?

Taylor Series

For $F(t) \in \mathbb{Z}[t]$ and $a \in \mathbb{Z}$,

$$F(t) = \sum_{i=0}^{\infty} a_i (t-a)^t \quad \text{with } a_i = \frac{F^{(i)}(a)}{i!}.$$

Let $G_x(t) \in \left(\mathbb{Z}_p[x]\right)[t]$. For $b \in \mathbb{Z}_p[x]$, one may consider to write

$$G_x(t) = \sum_{i=0}^{\infty} b_i (t-b)^i \quad \text{with } b_i = \frac{G_x^{(i)}(b)}{i!}.$$

- If $\deg(G_x) \ge p$, at least one of $b_i(x-b)^i$ should be nonzero if $i \ge p$.
- If $i \ge p$, then

  $$i! = 1 \cdot 2 \cdot 3 \cdots p \cdot (p+1) \cdots i = 0.$$

  Thus b_i is NOT well-defined.

Remark. We cannot use Taylor series in $\mathbb{Z}_p[x]$.

END OF PMATH 347!