MATH410 Fall 2022 Lecture Notes

Arya Wang

December 12, 2022

Contents

1 Chapter 1: Matrices (Review)

Proposition 1.1

Augmented matrices $\left[A\vec{b}\right]$ and $\left[A'\vec{b}'\right]$ are row equivalent $\Leftrightarrow A\vec{x} = \vec{b}$ and $A'\vec{x} = \vec{b}'$

Theorem 1.2

The following are equivalent:

(1) A is invertible

(2) $A\vec{x} = \vec{b}$ has a unique solution for any column vector $\vec{b}$.

(3) $A\vec{x} = \vec{0}$ has only one solution $\vec{x} = \vec{0}$.

Theorem 1.3

$\det(A) \neq 0 \Leftrightarrow A$ invertible.
$\det(AB) = \det(A)\det(B)$

Definition 1.4: Symmetric group

Symmetric group S_n is a set of all bijection on set $\{1, 2, ..., n\}$

Proposition 1.5

Every permutation can be written as a non-unique product of not necessarily disjoint transpositions (2-cycle)

Proposition 1.6

P is permutation matrix for permutation p, then

(1) P has a single 1 in each row and each column

(2) $\det(P) = \pm 1$

(3) pq composition $= PQ$ matrix

Definition 1.7: Sign of permutation

$$\text{sign}(p) = \det(P) = \begin{cases} +1 & \text{even number of transpositions} \\ -1 & \text{odd number of transpositions} \end{cases}$$

3 Chapter 3 (Quick review)

Definition 3.1: Vector Space

A set V is a vector space over $\mathbb{R}$ equipped with two operations: $+ : V \times V \to V$ and $\cdot : \mathbb{R} \times V \to V$:

(1) $(V, +)$ is an abelian group.

(2) $1 \cdot v = v$ for all $v \in V$.

(3) $(ab) \cdot v = a \cdot (b \cdot v)$

(4) $(a+b)v = av + bv, a(v+w) = av + aw$

Theorem 3.2

If V is n-dim vector space over $\mathbb{R}$, then exists invertible linear function $f : V \to \mathbb{R}^n$

Definition 3.3: Bases

An (ordered) set $B = \{\vec{v_1}, \vec{v_2}, ..., \vec{v_n}\}$ is a base of V:

(1) B is linearly independent

(2) B spans V

Note: B is a base $\Leftrightarrow$ B is invertible.

Proposition 3.4

A set $\{v_1, v_2, ..., v_n\}$ is linearly independent if $a_1v_1 + ... + a_nv_n = 0$ has only one trivial solution $a_1 = a_2 = ... = a_n = 0$

Definition 3.5: Coordinate vector

Given some vector $\vec{v} \in V$, the coordinate vector $[\vec{v}]_B$ is the column matrix such that

$$B[\vec{v}]_B = \vec{v}$$

Definition 3.6: Subspace

$W \subseteq V$ is a subspace of V if it

(1) closed under $+$,

(2) closed under scalar multiplication $\cdot$

Definition 3.7: Direct Sum

V is the direct sum of subspaces of $W_1, W_2, ..., W_k$ if

(1) $W_1 + W_2 + ... + W_k = V$.

(2) $W_1, W_2, ..., W_k$ are independent subspaces, which means for any $i, j \in \mathbb{Z}^*, W_i \cap W_j = \{\vec{0}\}$

2 Chapter 2: Groups

2.2 Groups and Subgroups

Definition 2.1: Group

A group is a set G together with a binary operator $G \times G \to G$ s.t.

(1) associative: $a(bc) = (ab)c$;

(2) identity: $e \in G$ s.t. $ea = a = ae, \forall a \in G$

(3) inverse: for each $a \in G$, there exists $b \in G$ s.t. $ab = e = ba$.

Proposition 2.2

Suppose $a \in S$, exist $la = e = ar$. Then $l = r$.

Example 2.3.

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

(2) $M_n(\mathbb{R})$

(3) $C^0(\mathbb{R})$ = {invertible continuous functions $\mathbb{R} \to \mathbb{R}$};
$C^1(\mathbb{R})$ = {invertible continuous differential functions $\mathbb{R} \to \mathbb{R}$};

(4) S_n symmetric group of n letters

Note: NOT ALL GROUPS ARE ABELIAN

Proposition 2.4: Cancellation

$a, b, c \in G$. If $ab = ac$ or $ba = ca$ then $b = c$. And if $ab = a$ or $ba = a$ then $b = e$.

Proof. Suppose $ab = ac$. Since $a \in G$, $A^{-1} \in G$. And so we mult. both sides by a^{-1}. So we have

$$a^{-1}ab = a^{-1}ac$$

$$eb = ec$$

Second, $ab = a, \implies a^{-1}ab = a^{-1}a = e \implies b = e$ □

Definition 2.5: Subgroup

A subset $H \subset G$ that is itself a group under the operation inherited from G is called a subgroup.

(a) closure over multiplication ($A, B \in H \implies AB \in H$)

(b) $e \in H$

(c) inverse in H

Example 2.6. $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) : |A| = 1\}$,$SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

Proposition 2.7

G is a group and $H \subset G$ is a subgroup if for every $a, b \in H$ we have $ab^{-1} \in H$.

Example 2.8. $\mathbb{S} = \{z \in \mathbb{C}^* : \|z\| = 1\}$ is a subgroup of $\mathbb{C}^*$

Definition 2.9: Proper subgroup

Every group G has subgroups $\{e\}$ and G. Proper subgroup is subgroup that isn't either of them.

Division in $\mathbb{Z}$: For any $a > b$ in $\mathbb{Z}$, we can write $a = qb + r$, for some $q \in \mathbb{Z}$ and some $r \in \mathbb{Z}$ s.t. $0 \leqslant r \leqslant b - 1$.

2.3 Subgroup of Additive Group of Integer

Theorem 2.10: Subgroups of $\mathbb{Z}$

If $S \subseteq \mathbb{Z}$ the $S = \{0\}$ or $S = \mathbb{Z}a$ where a is the smallest positive integer in S.

Proof. $S \subset Z \implies 0 \in S$. Suppose that $x \in S$ s.t. $x \neq 0$. If not, $S = \{0\}$. If $x > 0$, then OK. If $x < 0$, then $-x \in S$ because $S \subset \mathbb{Z}$. Therefore, we can always choose a positive integer $x \in S$.
Consider $\mathbb{Z}a$: since $S \subset \mathbb{Z}$, we know that $a \in S \implies a + a + ... + a \in S$, and $(-a) + (-a) + ..(-a) \in S$. So $\mathbb{Z}a \subset S$.
Consider S: choose the smallest positive integer $a \in S$. Now consider $m \in S$, $m = qa + r$ where $0 \leqslant r < a$ by integer

division. Since $a \in S \implies qa \in S$, and $m \in S \implies m - qa \in S \implies r \in S$. However, a is the smallest positive integer in S, so r has to be zero. That is $m = qa \implies m \in \mathbb{Z}a$. Therefore, $S \subset \mathbb{Z}a$.
Conclude: $S = \mathbb{Z}a$. □

Proposition 2.11

The group $\mathbb{Z}a + \mathbb{Z}b = \langle a, b\rangle = \{$all possible products of a and b under group operation$\}$ is equal to group $\mathbb{Z}d$ for some integer d. d is the greatest common divisor of a, b (write as $\gcd(a, b)$)

Proposition 2.12

$a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. We have:

(1) $d \mid a$ and $d \mid b$

(2) $m \mid a$ and $m \mid b \implies m \mid d$.

(3) there exists $r, s \in \mathbb{Z}$ s.t. $d = ra + sb$.

Recall: given a, b we can use Euclidean algorithm to find d.

Example 2.13. $a = 321, b = 123$. Find $ax + by = \gcd(a, b)$.
Solution:

$$
\begin{aligned}
321 &= 2 * 123 + 75 \\
123 &= 75 + 48 \\
75 &= 48 + 27 \\
48 &= 27 + 21 \\
27 &= 21 + 6 \\
21 &= 3 * 6 + 3 \\
6 &= 2 * 3
\end{aligned}
$$

So $\gcd(a, b) = 3$, then:

$$
\begin{aligned}
3 &= 21 - 3 * 6 \\
&= (27 - 6) - 3 * 6 \\
&= 27 - 4 * (27 - 21) \\
&= 4 * (48 - 27) - 3 * 27 \\
&= 4 * 48 - 7 * (75 - 48) \\
&= 11 * (123 - 75) - 7 * 75 \\
&= 11 * 123 - 18 * (321 - 2 * 123) \\
&= 47 * 123 - 18 * 321
\end{aligned}
$$

Corollary 2.14: to the last prop

a, b are relatively prime $(\gcd(a,b) = 1) \leftrightarrow$ there exists $r, s \in \mathbb{Z}$ s.t. $ra + sb = 1$

Corollary 2.15

$p \mid ab \implies p \mid a$ or $p \mid b$

2.4 Cyclic Group

Definition 2.16: Cyclic groups

A group generated by a single element is called a *cyclic group*.
Notation: $G = \langle g \rangle = \{...g^{-2}, g^{-1}, e, g^1, g^2, ...\} = \{g^n \mid n \in \mathbb{Z}\}$

Proposition 2.17

Let $x \in G$, and consider the cyclic group $S = \langle x \rangle$. Let $S = \{k \in \mathbb{Z} \mid x^k = e\} \subseteq \mathbb{Z}$,

(1) S is a subgroup of $\mathbb{Z}$.

(2) $x^r = x^s \Leftrightarrow x^{r-s} = e \Leftrightarrow r - s \in S$

(3) $S = \mathbb{Z}n$ for some positive integer n and $1, x, x^2, x^3, ..., x^{n-1}$ distinct.

Proof. .
(1). Check definition of subgroup:
Closure:

$$\begin{aligned} r, s \in S &\implies x^r = e \text{ and } x^s = e \\ &\implies x^r x^s = ee \\ &\implies x^{r+s} = e \\ &\implies r + s \in S \end{aligned}$$

Inverse: $r \in S \implies x^r = e$. Now consider $x^{-r} = (x^r)^{-1} = e^{-1} = e \implies -r \in S$
$S \subseteq \mathbb{Z}$
(3). By theorem 2.3.3 and (1), $s \subseteq \mathbb{Z} \implies S = \mathbb{Z}n$ for smallest positive integer $n \in S$. Now consider $x^k = x^{qn+r}$ for $0 \leqslant r < n$ (by integer theorem).So,

$$\begin{aligned} x^k &= (x^n)^q x^r \\ &= e^q x^r \\ &= x^r \end{aligned}$$

Now we know that n is the minimum positive integer k s.t. $x^k = e$. Since $x^k = x^r$ and $r < n$, none of

$e, x, x^2, ..., x^{n-1} = e$. Suppose not: $x^k = x^l$ for $k < l < n$. Then $e = x^{l-k}$, but $l - k < n$. Contradiction. So $e, x, x^2, ..., x^{n-1}$ unique and the order of H, $|H| = n$ □

Definition 2.18: Infinite cyclic group

A group generated by element of infinite order. $x^k \neq e$ for all $k \in \mathbb{Z}$. Then $\langle x \rangle = ..., x^{-2}, x^{-1}, e, x, x^2, ...$ are all distinct (actually $\cong \mathbb{Z}$).

Definition 2.19: Order

(1) x has order n if n is the smallest positive integer s.t. $x^n = e$.

(2) Cyclic group $\langle x \rangle$ has order n means it has n number(s) of elements, written as $|\langle x \rangle| = n$.

Example 2.20. $S_3 = \langle (123), (12) \rangle$.

Notice an n-cycle is order n. $(123)^3 = e, (12)^2 = e$. A cyclic subgroup $H = \langle (123) \rangle = \{(123), (132), e\}$ has order 3. Another cyclic subgroup $L = \langle (12) \rangle = \{(12), e\}$ has order 2.

Example 2.21. $GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0 \right\}$:

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order. $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ has order 6.

Proposition 2.22

Suppose x has order n ($\text{ord}(x) = 0$) and $k = nq + r (0 \leqslant r < n)$

(1) $x^k = x^r$

(2) $x^k = e \Leftrightarrow r = 0$

(3) $d = \gcd(k, n) \implies \text{ord}(x^k) = \frac{n}{d}$

Definition 2.23: Cyclic group generated by set

$S \subseteq G$ is a subset and consider $H = \langle S \rangle$, then H is the smallest subgroup containing all of S

Example 2.24. The smallest non-cyclic group is the **Klein four group**

$$V = \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \right\}$$

Notice: if V was cyclic, then it would have an element of order 4. But all elements are order 2.

And $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, where $\mathbb{Z}_2$ is a cyclic group of order 2.

Proposition 2.25

What is the order of

$$\{g \in G \mid \text{ord}(g) = |G|\}$$

Equivalently: how many elements generate all of G?

$$\phi(n) = \{g^s \mid 0 \leqslant s < n, \gcd(s,n) = 1\}$$

2.5 Homomorphism

Definition 2.26: Homomorphism

A function $\phi : G_1 \to G_2$ between groups G_1, G_2 is a homomorphism if $\phi(g*, h)$:

(1) $(G_1, *_1)$ and $e_1 \in G_1$ identity;

(2) $(G_2, *_2)$ and $e_2 \in G_2$ identity;

(3) $\phi(gh) = \phi(g)\phi(h)$.

Example 2.27.

(1) $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ because $\det(AB) = \det(A)\det(B)$.

(2) Sign: $S_n \to \{1, -1\}$ because $\text{sign}(\sigma\tau) = \text{sign}(\sigma)\text{sign}(\tau)$

(3) $\exp : \mathbb{R} \to \mathbb{R}^\times$ because $e^{x+y} = e^x e^y$

(4) $\phi : \mathbb{Z} \to G (a \in G)$ because $n \to a^n = aa...a$

(5) $\mathbb{C}^\times \to \mathbb{R}^\times$ s.t. $z \to |z|$ because $|zw| = |z||w|$

(6) A trivial homo: $\phi : G_1 \to G_2$ where $\phi(g) = e_2$ for all $g \in G_1$.

(7) An inclusion homo: $H \subseteq G, H \hookrightarrow G, h \to h$

Proposition 2.28

$\phi : G_1 \to G_2$ is a homomorphism then:

(a) $\phi(g_1 g_2 ... g_n) = \phi(g_1)...\phi(g_n)$

(b) $\phi(e_1) = e_2$

(c) $\phi(g^{-1}) = \phi(g)^{-1}$

Definition 2.29: Subgroups associated to how $G_1 \to G_2$

(1) Image of ϕ : $\mathrm{im}(\phi) = \phi(G_1) = \{g \in G_2 \mid g = \phi(h) \text{ for some } h \in G_1\}$

(2) Kernel of ϕ : $\ker(\phi) = \{g \in G_1 \mid \phi(g) = e_2\} \subseteq G_1$

Claim: $\mathrm{im}(\phi)$ is a subgroup of G_2

Proof. **Closure:** $g, h \in \mathrm{im}(e)$, so $g = \phi(x), h = \phi(y)$ for some $x, y \in G$. So $gh = \phi(x)\phi(y) = \phi(xy) \implies \mathrm{im}(\phi)$ because $xy \in G_1$. **Inverse:** $g \in \mathrm{im}(\phi) \implies g = \phi(x)$ for some $x \implies g^{-1} = \phi^{-1}(x) = \phi(x^{-1}) \implies g^{-1} \in \mathrm{im}(\phi)$ because $x^{-1} \in G_1$. □

Claim: $\ker(\phi)$ is a subgroup of G_1

Proof. **Closure:** $x, y \in \ker(l) \implies \phi(x) = e = \phi(y) \implies e^2 = \phi(x)\phi(y) \implies e = \phi(xy) \implies xy \in \ker(\phi)$.
Inverse: $x \in \ker(\phi) \implies \phi(x) = e \implies \phi^{-1}(x) = \phi(x^{-1}) = e^{-1} = e$, so $x^{-1} \in \ker(e)$. □

Example 2.30.

(1) $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$, $\ker(\det) = SL_n(\mathbb{R})$ (a set of $n \times n$ matrices with determinant 1)

(2) sign: $S_n \to \{1, -1\}$, $\ker(\text{sign}) = A_n$

Proposition 2.31

$\phi : G_1 \to G_2$ is homomorphism, $K = \ker(\phi) \subseteq G_1$, for $a, b \in G$, the following are equivalent:

(1) $\phi(a) = \phi(b)$;

(2) $a^{-1}b \in K$;

(3) $b \in aK$.

Corollary 2.32

(IMPORTANT) $\phi : G_1 \to G_2$ is injective $\Leftrightarrow \ker(\phi) = \{e\}$.
Note: injective means $\phi(x) = \phi(y)$ for $x, y \in G \implies x = y$

Definition 2.33: Normal subgroup

A subgroup $N \leqslant G$ is normal if $gNg^{-1} \leqslant N$ for any $g \in G$. In another word, the conjugation of N by g is still inside N.

Theorem 2.34

Equivalent:

(1) $gN = Ng$

(2) $N \subseteq gNg^{-1}$

(3) $gNg^{-1} = N$

Proposition 2.35

Let ϕ be homomorphism, $\ker(\phi)$ is a normal subgroup.

Proof. $x \in \ker(\phi)$ and $g \in G$. Now consider gxg^{-1}.

$$\begin{aligned}\phi(gxg^{-1}) &= \phi(g)\phi(x)\phi(g^{-1}) \\ &= \phi(g)e\phi^{-1}(g) \\ &= \phi(g)\phi^{-1}(g) \\ &= e\end{aligned}$$

So $gxg^{-1} \in \ker(\phi)$ □

Definition 2.36: Center of a group

The center of a group G is the set of all elements commuting with everything in G.
Notation: $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$

Proposition 2.37

$Z(G)$ is normal in G. Notation: $Z(G) \trianglelefteq G$.

Proof. Choose $x \in Z(G)$ and $g \in G$, then $gxg^{-1} = gg^{-1}x = x \in G$. □

2.6 Isomorphism

Definition 2.38: Isomorphism

An bijective homomorphism is called an isomorphism. That is $\phi : G_1 \to G_2$ is isomorphism $\Leftrightarrow$

$$\phi(G_1) = G_2(\text{surjective}); \ker(\phi) = G_1(\text{injective})$$

Example 2.39.

(1) exp: $\mathbb{R}^+ \to (0,\infty)^\times, x \to e^x$

(2) $a \in G$ is an element of infinite order. Define $\phi : \mathbb{Z} \to \langle a \rangle, \phi(n) = a^n$. $\langle a \rangle$ infinite cyclic is isomorphic to $\mathbb{Z}$, $\mathbb{Z} \cong \langle a \rangle$

(3) Let $P_n \leqslant GL_n$ of permutation matrices. $S_n \to P_n$ s.t. $\sigma \to$ permutation of matrix associated to $sigma$.

Lemma 2.39.1

$\phi : G_1 \to G_2$ is isomorphism $\implies$ $\phi^{-1} : G_2 \to G_1$ is also an isomorphism

Definition 2.40: Automorphism

$\phi : G \to G$ isomorphism
Trivial: $\phi(g) = g$ identity map on G
Inner automorphism: $\phi_g : G \to G$, $x \to gxg^{-1}$

Proposition 2.41

Abelian group G. We have:

(1) $H \leqslant G \implies H \trianglelefteq G$,

(2) $Z(G) = G$

(3) all inner automorphisms are trivial because $\phi_g(x) = gxg^{-1} = x$.

Definition 2.42: Conjugation automorphism

$\phi_g : G \to G$, $x \to gxg^{-1}$ is a conjugation automorphism.

Proof. **Homomorphism:** $x, y \in G$, then $\phi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y)$. **Isomorphism:** Let's look at $\ker(e_g)$. $x \in \ker(e_g) \implies \phi_g(x) = e \implies gxg^{-1} = e \implies x = geg^{-1} = e$. So $\ker(e_g) = \{e\}$, so ϕ_g is injective. □

Notice: normal subgroups are "fixed" by inner automorphism

Definition 2.43: Commutator subgroup

$a, b \in G$, then their commutator is $aba^{-1}b^{-1}$ and is denoted $[a, b]$. $[G, G] = \left\{aba^{-1}b^{-1} \mid a, b, \in G\right\}$ is the commutator subgroup.
Note: if $[a, b] = e$, then $ab = ba$.

2.7 Equivalence relation

Definition 2.44: Equivalence relation

Equivalence relations on set S denoted as $a \sim b$ for $a, b \in S$,

(1) transitive $a \sim b$ and $b \sim c \implies a \sim c$.

(2) symmetric $a \sim b \implies b \sim a$.

(3) reflexive $a \sim a$ for all $a \in S$

Example 2.45. Conjugacy on a group. Because $a \sim b \Leftrightarrow$ exists g s.t. $a = gbg^{-1}$

Definition 2.46: Partition of S

Subdivide S into non-intersecting (disjoint) and non-empty subsets. $S = S_1 \cup S_2 \cup ... \cup S_n$ s.t. $S_i \cap S_j = \varnothing$ for $i \neq j$, is written as:

$$S = S_1 \sqcup S_2 \sqcup ... \sqcup S_n$$

Example 2.47.

(1) $\mathbb{Z} = \text{Even} \sqcup \text{Odd}$

(2) $S_3 = \{e\} \sqcup \{y, xy, x^2y\} \sqcup \{x, x^2\}$, where $x = (123), y = (12)$

Proposition 2.48

Equivalence relation on S is equivalent to partition on S.

Proof. We want to prove $a \sim b \Leftrightarrow a$ and b are in the same subset in the partition. □

Lemma 2.48.1

Equivalence classes for $a \in S$, $C_a = \{b \in S \mid a \sim b\}$ partition S.

Proof. Main point: if $C_a \cap C_b \neq \varnothing$, then $C_a = C_b$.Suppose $C_a \cap C_b \neq \varnothing$, we'll show that $C_b \subseteq C_a$, and the following proof is also applicable to get $C_a \subseteq C_b$.
$x \in C_b \implies b \sim x$. Now let $d \in C_a \cup C_b$. Then $a \sim d$ and $b \sim d$. By symmetry, $d \sim b$. Now $a \sim d \sim b \sim x$. So by transitivity, $a \sim x$. So $x \in C_a$. So $C_b \subseteq C_a$ and similarly $C_a \subseteq C_b$. So $C_a = C_b$
So S is partitioned by disjoint equivalence classes. □

Definition 2.49: Set of equivalent classes

Set S with relation $\sim$:

$$\overline{S} = \{[C_a] \mid a \in S\}$$

C_a is a set of all equivalent classes that are equal to C.

Example 2.50.
$\mathbb{Z} =$ Even $\sqcup$ Odd.
Even $= C_0 = C_2 = C_4 = ... \to$ [Even] $= \overline{0}$
Odd $= C_1 = C_3 = C_4 = ... \to$ [Odd] $= \overline{1}$
So group $\overline{\mathbb{Z}} = \{\overline{1}, \overline{0}\}$

Definition 2.51: Map and Function of equivalence relation

For any equivalence relation $\sim$ on S, we can define a surjection map

$$\pi S \to \overline{S}, a \to [C_a]$$

So, $\pi(a) = \pi(b) \Leftrightarrow C_a = C_b$.
Furthermore, let $f : S \to T$, for $a, b \in S$,

$$a \sim b \Leftrightarrow f(a) = f(b) \in T$$

(Only) If f is a bijective function, the **fibre** of function f is:

$$f^{-1} = \{s \in S \mid f(s) = t\}$$

Example 2.52.

(1) $|G| < \infty$, ord: $G \to \mathbb{N}$. Equivalent classes are: $C_n = \{\text{elements of } G \text{ of order } n\}$

(2) $f : \mathbb{C}^\times \to \mathbb{R}^\times$ defined by $f(z) = |z|$

Proposition 2.53

Let $K = \ker(\phi)$. The following are equivalent:

(1) $aK = bK$

(2) $a^{-1}b \in K$

(3) $b \in aK$

Proposition 2.54

Let $K = \ker(\phi)$, the fibre of ϕ containing $a \in G_1$ corresponds to coset aK. And these coset partition the group G.

2.8 Cosets

Definition 2.55: Coset

$H \subseteq G$ is a subgroup and $a \in G$ s.t.

$$aH = \{ah \mid h \in H\} = \{g \in G \mid g = ah \text{ for some } h \in H\}$$

These aH are cosets of H in G.

Corollary 2.56

Left cosets of $H \in G$ partition G.

Example 2.57. $G = S_3$, $H = \langle y \rangle$. Let $x = (123), y = (12)$. $H = \{e, y\} = yH$. And $xH = \{x, xy\} = xyH$. And $x^2H = \{x^2, x^2y\} = x^2yH$.

Proposition 2.58

$a, b \in G$ and $H \leqslant G$. The following are equivalent:

(1) $b = ah$ for some $h \in H$.

(2) $a^{-1}b \in H$.

(3) $b \in aH$.

(4) $aH = bH$.

Definition 2.59

Number of left cosets of a subgroup $H \leqslant G$ is called the index of H in G, and it is denoted $[G : H]$

Lemma 2.59.1

All left cosets of $H \leqslant G$ has same order

Proof. $f : H \to aH$, $f(h) = ah$. It's a bijection because $f^{-1} = a^{-1}h$. So $|H| = |aH|$ □

Proposition 2.60: I

H is a subgroup of G and $[G : H] = 2$, then H is normal. (proved in worksheet or hw)

Theorem 2.61: Lagrange's Theorem

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

Proof. Cosets are all order $|H|$, and $[G : H]$ cosets partition G. □

Corollary 2.62

let $g \in G$, $\text{ord}(g) \mid |G|$

Corollary 2.63

$|G| = p$ (i.e. G is cyclic of prime order), then for every $a \in G$ s.t. $a \neq e$, $G = \langle a \rangle$.

Corollary 2.64

Let $\phi : G \to G'$ homomorphism

(1) $|G| = |\ker(\phi)||\mathrm{im}(\phi)|$

(2) $|\ker(\phi)| \mid |G|$

(3) $|\mathrm{im}(\phi)| \mid |G|$ and $|\mathrm{im}(\phi)| \mid |G'|$

Proposition 2.65: Multiplicativity of index

$K \leqslant H \leqslant G \implies [G : K] = [H : K][G : H]$

We can also do everything with right cosets

2.9 Modular Arithmetic

Definition 2.66: Congruence

$a \equiv b \mod n \Leftrightarrow n \mid b - a \Leftrightarrow a = kn + b$

Note: it's an equivalence relation on $\mathbb{Z}$

Proof. .

(1) Transitivity: $a \equiv b, b \equiv c \implies a \equiv c$

(2) Symmetry: $a \equiv b \implies b \equiv a$

(3) Reflexivity: $a \equiv ae = a$

Notation: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ □

Proposition 2.67

There are n congruence classes modulo n. And $[\mathbb{Z} : n\mathbb{Z}] = n$

Lemma 2.67.1

$$\overline{a + b} = \overline{a} + \overline{b};$$
$$\overline{ab} = \overline{a} \cdot \overline{b}$$

Definition 2.68: Congruence

$a \equiv b \mod n \Leftrightarrow n \mid b-a \Leftrightarrow a = kn+b$

Note: it's an equivalence relation on $\mathbb{Z}$

Proof. .

(1) Transitivity: $a \equiv b, b \equiv c \implies a \equiv c$

(2) Symmetry: $a \equiv b \implies b \equiv a$

(3) Reflexivity: $a \equiv ae = a$

Notation: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ □

Proposition 2.69

There are n congruence classes modulo n. And $[\mathbb{Z} : n\mathbb{Z}] = n$

Lemma 2.69.1

$$\overline{a+b} = \overline{a} + \overline{b};$$
$$\overline{ab} = \overline{a} \cdot \overline{b}$$

Example 2.70. For what n does 2 have a multiplicative inverse modulo n. That is $2a \equiv 1 (\text{mod } n)$

$2a = qn + 1$. Since $2a$ is even, qn must be odd. So q, n are odd. Then we write $n = 2k+1$, $k = 2m+1$. So

$$\begin{aligned} 2a &= (2m+1)(2k+1)+1 \\ &= 4mk + 2m + 2k + 2 \\ &= 2(2mk + m + k + 1) \end{aligned}$$

Example 2.71: Proof of Chinese Remainder Theorem. (General idea)

The theorem:

$$x \equiv a \mod m$$
$$x \equiv b \mod n$$

And $\gcd(m, n) = 1$.

Proof.

$$\begin{aligned} x &= arm + bsn \\ &= a(1 - sn) + bs \\ &= a - asn + bsn \\ &= a + (bs - as)n \end{aligned}$$

□

2.10 Congruence Theorem

Definition 2.72: Restriction

Let $\phi : G \to G'$ be a homomorphism, and $H \leqslant G$. We may restrict ϕ to H s.t.

$$\phi|_H = H \to G$$

We have:

$$\ker(\phi|_H) = \ker(\phi) \cap H$$
$$\operatorname{im}(\phi|_H) = \phi(H)$$

Corollary 2.73

Let $\phi : H \to G'$

(1) $|\phi(H)| \mid |H|$

(2) $|\phi(H)| \mid |G'|$

So if $\gcd(|H|, |G|) = 1 \implies \phi(H) = \{e\}, H \leqslant \ker(\phi)$.

Example 2.74. $H \leqslant$ a subgroup, sign: $S_n \to \{1\}$. Since $|\text{sign}(S_n)| = 2$, $|\phi(H)| = 1 \implies H \leqslant \ker(\text{sign}) = A_n$

Proposition 2.75

Let $\phi : G \to G'$, $K = \ker(\phi), H' \leqslant G'$.

(1) $K \leqslant \phi^{-1}(H') \leqslant G$

(2) If $H' \trianglelefteq G'$, $\phi^{-1}(H') \trianglelefteq G$

(3) If ϕ is surjective (i.e. $\phi(G) = G'$), then $\phi^{-1}(H') \trianglelefteq G \implies H' \trianglelefteq G'$

Example 2.76. $\det GL_n(\mathbb{R}) \to \mathbb{R}^\times, H = (0,\infty) \trianglelefteq \mathbb{R}^\times$ is normal because $\mathbb{R}^\times$ is abelian. So

$$\det^{-1}(H) \trianglelefteq GL_n(\mathbb{R})$$

Theorem 2.77: Correspondence Theorem

Let $\phi : G \to G'$ be surjective, $K = \ker(e)$. Then there exists a bijection in

$$\{K \leqslant H \leqslant G\} \leftrightarrow \{H' \leqslant G'\}$$

and the bijection relation is:

$$H \to \phi(H)$$
$$H' \to \phi^{-1}(H')$$

And $H \trianglelefteq G \Leftrightarrow H' \trianglelefteq G'$, $|H| = |H'| \cdot |K|$.
Critical fact: $\phi(K) = \{e\}$.

Proof. We need

(1) $\phi(H) \leqslant G'$.

(2) $K \leqslant \phi^{-1}(H') \leqslant G$.

(3) $H' \trianglelefteq G' \Leftrightarrow \phi^{-1}(H') \trianglelefteq G$.

(4) Bijective: $\phi(\phi^{-1}(H')) = H'$. This is true for any surjective function. More precisely, $H \subseteq \phi^{-1}(\phi(H))$ for any surjective function H. Now we want to prove the inverse containment. Let $x \in \phi^{-1}(\phi(H)) = \{x \in G \mid \phi(x) \in \phi(H)\}$. So we can write $x = \phi(h)$ for some $h \in H$. So $\phi(x)\phi(h)^{-1} = e \implies \phi(xh^{-1}) = e \implies xh^{-1} \in K$. But by hypothesis, $K \leqslant H$, so $xh^{-1} \in H$. And $h \in H$, so $xh^{-1}h = x \in H$. So $\phi^{-1}(\phi(H)) \subseteq H \implies H = \phi^{-1}(\phi(H))$

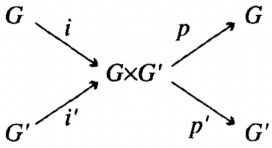
(5) $|\phi^{-1}(H')| = |H'| \cdot |K|$.

□

2.11 Product groups

Definition 2.78

We have two group G, G'. The product group $G \times G' = \{(g, g') \mid g \in G, g' \in G'\}$ with operation given component-wise: $(g_1 g_1')(g_2 g_2') = (g_1 g_2, g_1' g_2')$



(2.11.2)

They are defined by $i(x) = (x, 1)$, $i'(x') = (1, x')$, $p(x, x') = x$, $p'(x, x') = x'$. The

Product group example in book

Theorem 2.79

$\gcd(r, s) = 1$ then $C_{rs} = C_r \times C_s$.
Notation: C_n = cyclic group of order n.

Example 2.80.

(1) $C_6 \cong C_2 \times C_3$. Let $C_6 = \langle x \rangle, C_2 = \langle y \rangle, C_3 = \langle z \rangle$. $f : C_6 \to C_2 \times C_3$ is defined by $f(x) = (y, z)$, (y, z) has order 6.

(2) (Non-example) $C_4 \ncong C_2 \times C_2$

When is $G \cong H \times K$ for $H, K \leqslant G$

Proposition 2.81

Define $f : H \times K \to G$ to be $f(h, k) = hk$. Its image is the set $\{hj \in G \mid h \in H, g \in G\}$

(1) f is injective $\Leftrightarrow H \cap K = \{e\}$.

(2) f is a homomorphism $\Leftrightarrow$ elements of K commute with elements of H.

(3) H is normal in G $\implies Hk \leqslant G$

(4) f isomorphism $\Leftrightarrow H \cap K = \{e\}, HK = G, H, K \trianglelefteq G$

Proof. (1) (Left to right) Suppose that $x \in H \cap K$ such that $x \neq e \implies x^{-1} \in H, x \in K$ and $f(x^{-1}, x) = e = f(e, e) \implies f$ is not injective. (Right to left) $H \cap K = \{e\}$. Now let $(h_1, k_1) \neq (h_2, k_2) \in H \times K$ such that $f(h_1, k_1) = f(h_2, k_2) \implies h_1 k_1 = h_2 k_2 \implies h_2^{-1} h_1 = k_2 k_1^{-1}$. So because $h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K = \{e\}$, $h_2 = h_1$ and $k_2 = k_1 \implies$ f injective

(2) (Left to right) f homomorphism, $(h_1, k_1), (h_2, k_2) \in H \times K \implies (h_1 h_2, k_1 k_2) \in H \times K$ and $f(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = f(h_1, k_1) \times f(h_2, k_2) = h_1 k_2 h_2 k_2 \implies h_2 k_1 = k_1 h_2$. So we prove commutative since the elements h_2, k_1 are arbitrary. (The inverse direction is the same logic)

(3) Let $H \trianglelefteq G$, which means $KH = \bigcup_{k \in K} kH$, $HK = \bigcup_{k \in K} Hk$. Since normal, $kH = Hk \implies KH = HK$. So HK is closed under multiplication: $HKHK = HHKK = HK$. And inverse exists: $hk \in HK \implies (hk)^{-1} = k^{-1} h^{-1} \in KH = HK$.

(4) (Right to left) Suppose $H, K \trianglelefteq G, G = HK, H \cap K = \{e\}$. Define $f = H \times K \to G$. We already know surjective and injective $\implies$ f is a bijection. By (2) we just need to show $hk = kh$ for all $h \in H, k \in K$. Consider the commutator $\underbrace{(hkh^{-1})k^{-1}}_{\text{Product of two elements in } K} = \underbrace{h(kh^{-1}k^{-1})}_{\text{Product of two elements in } H} \in H \cap K = \{e\}$. So $hkh^{-1}k^{-1} = e \implies hk = kh$

□

Proposition 2.82: Classification of groups of order 4

There are two isomorphism classes of groups of order 4, the class of the cyclic group C_4 of order 4 and the class of the Klein Four Group, which is isomorphic to the product $C_2 \times C_2$ of two groups of order 2.

Proof. Let $|G| = 4 \implies x \in G, \text{ord}(x) = 1, 2, 4$.

Case 1: there is an element s.t. $\text{ord}(x) = 4$, then clearly $G \cong \langle x \rangle$.

Case 2: no element of order 4 (only 2 for $x \neq e$).

$$\begin{aligned} x, y \in G &\implies \text{ord}(x) = \text{ord}(y) = 2 \\ &\quad\ \ \text{ord}(xy) = 2 \\ &\implies x = x^{-1}, y = y^{-1} \\ &\implies xyx^{-1}y^{-1} = xyxy = e \\ &\implies x, y \text{ commute} \implies G \text{ abelian} \end{aligned}$$

Now by prop 2.11.4, $G \cong \langle x \rangle \times \langle y \rangle \cong C_2 \times C_2$ □

2.12 Quotient Groups

Why we care about normal:

$N \trianglelefteq G$, consider G/N = set of left cosets of $N \in G = \{gN \mid g \in G\} \implies G/N$ is a group. Notice: If N is not normal then G/N is not a group because $(gN)(hN)$ may not be of form xN.

Theorem 2.83

If N is a normal subgroup then G/N (G mod N) is itself a group. And the function $\pi : G \to G/N$ s.t. $\pi(g) = gN = \overline{g}$ is a surjective group homomorphism such that $\ker(\pi) = N$. The π is usually referred to as *canonical map*.

Lemma 2.83.1

$N \trianglelefteq G, aN, bN \in G/N$ then $(aN)(bN) = (ab)N$

Proof. $a \underbrace{Nb}_{\text{right coset}} N = abNN$ (because it's normal) $= abN$. □

Lemma 2.83.2

G group, Y a set with composition and $\phi G \to Y$ surjective function such that $\phi(ab) = \phi(a)\phi(b) \implies Y$ is a group and ϕ is homomorphism.

Proof. Now prove the theorem:

(1) group operation on G/N.

(2) G/M is a group (closure, identity, inverse) by Lemma 2.

(3) π surjective homomorphism.
π is surjective by definition and $\pi(gh) = ghN = gNhN = \pi(a)\pi(b)$ so homomorphism.

(4) $\ker(\pi) = N$.
$a \in N \Leftrightarrow \pi(a) = \pi(e) = \overline{e} \Leftrightarrow aN = eN = N$

□

Corollary 2.84

$a_1, a_2, ...a_k \in G$ such that $\prod_{i=1}^{k} a_i \in N$. Then $\pi(a_1a_2...a_k) = \pi(a_1)\pi(a_2).. = \overline{e}$

Example 2.85. $H = \langle(12)\rangle \in S_3$ which is not normal. $eH(123)H = \{(123), (123)(12), (123)^2(12), (123)^2\}$ and it's not a left coset of H.

Theorem 2.86: First Isomorphism Theorem

Let $\phi : G \to G'$ to be a surjective group homomorphism with $\ker(\phi) = N$. Then $G/N \cong G'$.

Proposition 2.87

If $G/Z(G)$ is cyclic, then G is abelian. (Used in hw but not mentioned in class)

Proof. We can write $G/Z(G) = \langle xZ(G)\rangle$ for some $x \in G$. Then for any $g \in G$, we have $gZ(G) = x^m Z(G), m \in \mathbb{N}$. Then according to proposition 2.8.4 about cosets, $gZ(G) = x^m Z(G) \implies (x^m)^{-1}g \in Z(G)$. Suppose there's another arbitrary element $h \in G$, let $(x^m)^{-1}g = z_1 \in Z(G), (x^n)^{-1}g = z_2 \in Z(G)$,

$$\begin{aligned} gh &= x^m z_1 x^n z_2 \\ &= x^m x^n z_1 z_2 \\ &= x^n z_1 x^m z_2 \\ &= hg \end{aligned}$$

So G is abelian. □

3 Group Actions

Galois: $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}_2$

CAYLEY: $|G| = n$ is isomorphic to a subgroup of S_n

Definition 3.1: Group action

G acting on a set X is $\alpha : G \times X \to X$ such that $\alpha(g, h) = \alpha_g(x)$.

Or equivalently, $\alpha : G \to \text{Perm}(X) \cong S_{|x|}$ such that $\alpha(g) = \alpha_g$

The action satisfies:

(1) $\alpha_e(x) = x$

(2) $\alpha_g(\alpha_h(x)) = \alpha_{gh}(x)$

Notation: the action gives $x \in X \to g \cdot x \in X$

Definition 3.2: Orbits

The subsets of X given by $G \cdot x = \{y \in X \mid y = g \cdot x \text{ for some } g \in G\}$

Notice: Orbits partition G.

Proposition 3.3

The group action is transitive if there is only one orbit.

Transitive: for any $x \in X$, we can find $g \in G, y \in X$ such that $x = g \cdot y$

Proposition 3.4

The group action defines an equivalence relation on X with equivalence classes $=$ orbits

Definition 3.5: Stabilizers

For $x \in X$, stabilizers is the subgroup of G, $G_x = \{g \in G \mid g \cdot x = x\}$.

We say the action is **free** if all stabilizers are trivial (no non-identity elements of G has a fixed point $g \cdot x = x$).

Theorem 3.6: Orbit-Stabilizer Theorem

$|G| = |G_x| \times |G \cdot x| =$ (order of stabilizer of x) $\times$ (order of orbit of x).

Proof. (Lagrange's Theorem staff) □

Lemma 3.6.1

The group actions give homomorphism $\alpha : G \to \text{Perm}(X)$

Theorem 3.7: Cayley's Theorem

Every finite group G is (isomorphic to) a subgroup of a symmetric group. Specifically: $|G| = n, G \cong S \leqslant S_n$.

Example 3.8. Groups acting on themselves:

(1) Left multiplication: $m : G \to \text{Perm}(G)$ such that $m_g(x) = mg$. The orbits of this action are left cosets.

(2) Conjugation: $\alpha : G \to \text{Perm}(G)$ which is $G \to \text{Auto}(G)$ actually. $\alpha_g(x) = gxg^{-1} = \underbrace{x^g}_{\text{conjugation notation}}$

For part (2):
Orbits = conjugacy classes

$$Cl(x) = \left\{y \in G \mid y = gxg^{-1} = x^g \text{ for some } g \in G\right\}$$

Stabilizers: centralizers

$$G_x = C_G(x) = \left\{g \in G \mid gxg^{-1} = x\right\} = \{g \in G \mid gx = xg\}$$

Note: If x conjugate to y then $Cl(x) = Cl(y)$

Proposition 3.9

FACT:

(1) $|G| = |C_G(x)| \times |Cl(x)| \implies |Cl(x)| = [G : C_G(x)] \implies |Cl(x)| \mid |G|$ for every x.

(2) Class equation: $G = \sqcup_i Cl(g_i)$, g_i representatives of conjugacy classes. This means

$$|G| = \sum_i |Cl(g_i)| = \sum_i [G : C_G] = |Z(G)| + \underbrace{\sum_{i=k} [G : C_G(x_i)]}_{\text{sum of } |Cl(x)| \neq 1}$$

(3) If $x \in Z(G)$, $|Cl(x)| = 1$

3.1 p-groups

Proposition 3.10: 7.3.1

Center of a p-group is non-trivial. (Note if G is a p-group, $|G| = p^k$ for some integer k.

Proof. $|G| = p^k$. By class equation, $|G| = |Z(G)| + \sum_i [H : C_G(x_i)]$. Suppose $|Z(G)| = 1$, so $p^k = 1 + \sum_i [G : C_G(x_i)]$.

And $[G : C_G(x_i)] \mid p^k \implies = p^{m_i}$. So

$$\begin{aligned} p^k &= 1 + \sum_{i=1}^{k} p^{m_i} \\ &= 1 + p(p^{m_1 - 1} + p^{m_2 - 1} + \ldots + p^{m_k - 1}) \\ &\equiv 1 (\text{mod } p) \end{aligned}$$

Contradiction. So $|Z(G)| \neq 1$. □

Proposition 3.11: 7.3.3

Groups of order p^2 are abelian.

Proof. $|G| = p^2$, we want to show $|Z(G)| = p^2$. By previous proposition, $|Z(G)| \neq 1$, so $|Z(G)| = p$ or p^2. We want to rule out the possibility of order being p. $|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)]$. Notice the order cannot exceed p^2, the nontrivial conjugacy classes should have order p. Note that if $x \notin Z(G)$, then $Z(G) < C_G(x) \implies |C_G(x)| = p^2$, which is a contradiction. □

3.2 Dihedral Groups

Definition 3.12: Dihedral Group

Groups of symmetries of regular n-gons = $\{n$ rotations, n reflection$\}$
Notation: D_n (in book) or D_{2n} (modern notation).
We have

$$D_{2n} = \left\langle r, s \mid r^n = e, s^2 = e, srs = r^{-1} \right\rangle$$

Another general rule: compose two reflection, get the rotation corresponding $2 \times \theta$ where θ = angle between the axes of rotations.

Proposition 3.13

n odd:

- $Z(D_{2n}) = \{e\}$
- All reflections are conjugate (they are all in the same conjugacy class)

n even:

- $Z(D_{2n}) = \left\{e, r^{\frac{n}{2}}\right\}$
- Vertex axis reflections are conjugate, fare axis reflections are conjugate. That is, there are two conjugacy classes: vertex axis reflections and fare axis reflections

Example 3.14. Class equation for D_8 = {symmetries of square}

We can think about the elements of D_8 as the elements of S_4 because each element permutes the vertices:

$$r \to (1234)$$
$$s_1 \to (23)$$
$$s_2 \to (12)(34)$$

(1) $Z(D_8) = \{e, (13)(24)\} = \{e, r^2 \equiv S_1S_3\}$

(2) $Cl((13)) = \{(13), (24)\}$ (vertex axis reflections)
$Cl((12)(34)) = \{(12)(34), (14)(23)\}$ (fare axis reflections)
$Cl(r) = Cl((1234)) = \{(1234)(1432)\}$ (order 4 rotations)

Homework hint (problem 10): Classify group of order 8 =

(1) 3 abelian $= \begin{cases} \mathbb{Z}/8\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases}$

(2) 2 non-abelian $= \begin{cases} D_8 \\ Q_8 = \{1, i, j, k, -1, -i, -j, -k\} \end{cases}$

3.3 Simple groups

Definition 3.15: Simple groups

Simple groups have no non-trivial normal subgroups. The simple groups are the building blocks of all groups (Some side reading: classification of simple groups)

Lemma 3.15.1: 7.4.2

For normal subgroup $N \trianglelefteq G$ ($gNg^{-1} = N$), we have

(1) $x \in N \implies Cl(x) \subseteq N$

(2) $N = \bigcup_x Cl(x)$

(3) $|N| = \sum_{x \text{ represents of distinct conjugacy class}} |Cl(x)|$

Theorem 3.16: 7.4.3

A_5 is simple where A_5 = icosahedral group = even parts of permutation in S_5

Proof. We've given that A_5 has the following class equation:

$$|A_5| = 60 = 1 + 20 + 12 + 12 + 15$$

which is established with geometry in book section 7.4.
Suppose N is normal in A_5, then $|N| \mid 60$. By proposition (3) in the lemma, $|N| = 1 + m$ where m = sum of subset of $\{20, 12, 12, 15\}$. But no such integer m with these combined property $\Longrightarrow$ no normal subgroup. □

The theorem of **Galois group** (we don't need to know for now): Galois group of polynomial $\Leftrightarrow$ polynomial is solvable by radicals. We have $Gal(\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_5)/\mathbb{Q}) \leqslant A_5$. Since A_5 is not solvable, degree 5 polynomials are not solvable by radicals (has no formula of roots in terms of n)

3.4 Conjugacy classes in S_n

Example 3.17. We can think about S_5 as $\phi : \{1, 2, 3, 4, 5\} \to \{a, b, c, d, e\}$. Consider $p \in S_n$, $\phi \circ p \circ \phi^{-1} : \{a, b, c, d, e\} \to \{a, b, c, d, e\}$. Let $q = (1452), p = (134)(25)$. We have

$$qpq^{-1} = (1452)(134)(25)(2541) = (435)(12) = p'$$

We find that p and its conjugate p' have same disjoint cycle decomposition (cycle structure). And we find that $\phi : \{1, 2, 3, 4, 5\} \to \{4, 1, 3, 5, 2\}$ maps p to p', which is exactly the same as q.

Proposition 3.18: 7.5.1

p and p' are conjugate in Sn $\Leftrightarrow$ cycle decompositions are the same length (see the example above).

Example 3.19. Consider class equation for S_4:

Conjugacy classes	partition of 4	#
e	1+1+1+1	1
(**)	1+1+2	6
(**)(**)	2+2	3
(***)	1+3	8
(****)	4	6

Table 1

Group of order 8 (Problem 10): If abelian, $= 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$. If not, $= 1 + 1 + 2 + 2 + 2$
Example for abelian case: Let $|G| = p^2q^2$, the possible groups are $\mathbb{Z}/p^2q^2\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q^2\mathbb{Z}, ...$ ($p \times p \times q^2, p^2 \times q \times q, p \times p \times q \times q$ of the same form)
Now let's see $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. We know $(-1)^2 = 1, i^2 = j^2 = k^2 = -1, ijk = -1$. And $Z(Q_8) = \{\pm 1\}$.
Class equation for Q_8: Recall $|Cl(x)| = [Q_8 : C_G(x)]$, and $C_G(i) = \{x \in Q_8 \mid xi = ix\} = \{1, i, -1, -i\}$. Similarly $C_G(j) = \{1, -1, j, -j\}, C_G(k) = \{1, -1, k, -k\}$. So $[Q_8 : C_G(x)] = 2$ for all $x = i, j, k$.
To distinguish D_8 and Q_8, see what their normal subgroups are.

3.5 Normalizers

Definition 3.20: Normalizer

The stabilizer of the conjugation operation of G on its subgroup H is called the normalizer of H, and is denoted by

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

Proposition 3.21: 7.6.3

Let $H \leqslant G$, we have:

(1) $H \trianglelefteq N_G(H)$

(2) $H \trianglelefteq G \Leftrightarrow N_G(H) = G$

(3) $|H| \mid |N_G(H)|$ and $|N_G(H)| \mid |G|$

3.6 Sylow theorem

Definition 3.22: Sylow subgroups

Let $|G| = p^k m$ where the prime number $p \nmid m$ and k is the largest possible integer. Then $H \leqslant G$ with $|H| = p^k$ is called a Sylow p-subgroup.

Theorem 3.23: Sylow I

$p \mid |G| \implies G$ must have a Sylow p-subgroup

Corollary 3.24: Cauchy's theorem

$p \mid |G| \implies$ exists $x \in G$ with $\text{ord}(x) = p$.

Theorem 3.25: Sylow II

(a) Sylow p-subgroups are conjugate. In other words, if $P, Q \leqslant G$ are Sylow p-subgroups, then exists $g \in G$ such that $gPg^{-1} = Q$.

(b) Every p-subgroup is itself a subgroup of a Sylow p-subgroup.

Corollary 3.26

If $s_p = 1$, the Sylow p-subgroup is normal in G.

Theorem 3.27: Sylow III

Let s_p denote the number of Sylow p-subgroup. Then $s_p \mid m$ and $s_p \equiv 1 (\text{mod } p)$

Proposition 3.28: Facts about Finite Group

(1) $Aut(C_p) \cong C_p^\times = C_{p-1}$

(2) $|G| = p^2 \implies G$ is abelian (i.e. $G = C_{p^2}$ or $C_p \times C_p$)

(3) $|G| = pq$ s.t. $p < q$ and $p \nmid (p-1) \implies G$ is cyclic (i.e. $G = C_{pq}$)

Theorem 3.29: Generalized Cayley's theorem

Any subgroup $H \leqslant G$, then there exists a homomorphism $\phi : G \to S_{[G:H]}$ with $H \leqslant \ker(\phi)$.
Consequences:

- By 1st isomorphism theorem, $|G/\ker(\phi)| \mid [G:H]$
- $|G/\ker(\phi)| \mid |G|$

Definition 3.30: Semidirect product

$N \trianglelefteq G$, $H \leqslant G$ such that $HN = G$ and $H \cap N = \{e\}$. We know if $H \trianglelefteq G$, then $G = N \times H$. This is called direct product. We defined semi-direct product as $G = N \rtimes_\phi H$ where $\phi : H \to Aut(N)$ with $h \to \phi_h$ ($\phi_h : n \to hnh^{-1}$). Example:

$$(n_1, h_1)(n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2)$$

3.7 Generators and Relations

Recall that

$$C_n = \langle x \mid x^n = e \rangle$$
$$D_{2n} = \langle r, s \mid r^n = s^2 = e, srs^{-1} = r^{-1} \rangle$$
$$S_n = \langle x, y \mid x^n = y^2 = e, yxy = x^2 \rangle$$
$$C_n \times C_m = \langle x, y \mid x^n = y^m = e, xy = yx \rangle$$

Definition 3.31: Free Groups

$F_n = \langle x_1, x_2, x_3, ..., x_n \rangle$. The only rule is $x_i x_i^{-1} = x_i^{-1} x_i = e$.
Example: $F_2 < a, b >= \{abab, a^2b, a^3ba, ...\}$. Note that we don't assume commutative.

Recall: $\pi : G \to G/N$ for $N \trianglelefteq G \Leftrightarrow \ker(\pi) = N$. Consider a normal subgroup $R \trianglelefteq F_n$ and then F_n/R gives a presentation $\langle F_n \mid R \rangle$. Example:

(1) $C_n = F_1/\langle x^n\rangle = \langle x \mid x^n = e\rangle$

(2) $D_{2n} = F_2/\left\langle r^n, s^2, srs^{-1}r\right\rangle$

(3) $S_n = F_2/\left\langle x^n, y^2, yx^{-1}yx^2\right\rangle$

Example 3.32. Classification of groups of order 30, $|G| = 30 = 2\cdot 3\cdot 5$
By Sylow III:

$$n_2 \equiv 1(\text{mod } 2) \quad n_2 \mid 3\cdot 5 \quad n_2 = 1,3,5,15$$
$$n_3 \equiv 1(\text{mod } 3) \quad n_3 \mid 2\cdot 5 \quad n_3 = 1,10$$
$$n_5 \equiv 1(\text{mod } 5) \quad n_5 \mid 3\cdot 2 \quad n_5 = 1,6$$

Case $n_5 = 1$: Exists Sylow 5-subgroup $N \trianglelefteq G$ where $|N| = 5$. Now choose (by Sylow I) $S \leqslant G$ a Sylow 3-subgroup. Since the orders $\gcd(|S|,|N|) = 1$, we know $N \cap S = \{e\}$ and $|NS| = 15$ and $[G : NS] = 2 \implies NS \trianglelefteq G$. Now choose $H \in G$ a Sylow 2-subgroup. Again, we know $H \cap NS = \{e\}$ and $NSH = G$. So we can write $G = NS \rtimes_\phi H$.
Now look at $\phi : H \to Aut(NS)$ where $\phi(h) = \phi_h = hnh^{-1}$. Recall $|H| = 2 \to H = \langle h\rangle\,(h^2 = e) \implies \phi_h$ is either order 1 or 2 in group $Aut(NS)$. Also, $|NS| = 3\times 5$ and $3 \nmid 5-1 \implies NS \cong C_{15}$. So: $\phi : C_2 \to Aut(C_3\times C_5) \cong C_2\times C_4$. Suppose $\phi : \langle h\rangle \to \langle a\rangle\times\langle b\rangle$. If ϕ_h has order 1 $\implies \phi_h = e \implies G_1 = NS\times H \cong C_{15}\times C_2 \cong C_{30}$. If ϕ_h has order 2, let $NS \cong C_{15} \cong C_3\times C_5 = \langle\alpha\rangle\times\langle\beta\rangle$. Then

$$h \mapsto \begin{cases} \phi_h(\alpha,\beta) = (\alpha^2,\beta^4) \\ \phi_h(\alpha,\beta) = (\alpha,\beta^4) \\ \phi_h(\alpha,\beta) = (\alpha^2,\beta) \end{cases} \quad = h(\alpha,\beta)h^{-1} \cong \begin{cases} (a,e) \\ (e,b^2) \\ (a,b^2) \end{cases}$$

$\implies$

$$G_2 = \left\langle h,\alpha,\beta \mid h^2 = \alpha^3 = \beta^5 = e, h\alpha h^{-1} = \alpha^2, h\beta h^{-1} = \beta\right\rangle = C_5\times(C_3\times C_2) = C_5\times D_6$$
$$G_3 = \left\langle h,\alpha,\beta \mid h^2 = \alpha^3 = \beta^5 = e, h\alpha h^{-1} = \alpha, h\beta h^{-1} = \beta^4\right\rangle = C_3\times(C_5\times C_2) = C_3\times D_{10}$$
$$G_4 = \left\langle h,\alpha,\beta \mid h^2 = \alpha^3 = \beta^5 = e, h\alpha h^{-1} = \alpha^2, h\beta h^{-1} = \beta^4\right\rangle = D_{30}$$

Case $n_5 = 6$: 6 Sylow 5-subgroups and since each of the $K_i \leqslant G$ have $|K_i| = 5$, we have $K_i \cap K_j = \{e\} \implies 6\times 4 = 24$ elements of order 5 $\implies$ 2 order 2 elements and 3 order 3 elements $\implies$ Sylow 2-subgroup and Sylow 3-subgroup are both normal. Let $m \trianglelefteq G$, $|M| = 2$ and $N \trianglelefteq G, |N| = 3$. Now since $M \cap N = \{e\}$ (because co-prime order), we have $|MN| = 6$ and since $MN \trianglelefteq G$, consider semi-direct product: $K \leqslant G, MN \trianglelefteq G$ and how $\phi : K \to Aut(MN)$. Notice that both N and M are also normal in MN, so $MN \cong C_3\times C_2$. Now we know that $Aut(MN) \cong C_2\times C_1 \implies$ now ϕ is trivial. That is not possible because K is not normal in G.

Example 3.33. Classify $|G| = 12 = 2^2\times 3$.

By Sylow III:

$$n_3 = 1, 4$$
$$n_2 = 1, 3$$

Case $n_3 = 4$: Suppose K_1, K_2, K_3, K_4 are these Sylow 3-subgroups. Since K_i are prime order, either $K_i = K_j$ (We don't want) or $K_i \cap K_j = \{e\} \implies 4 \times 2 = 8$ order 3 elements $\implies$ 3 elements of order 2, hence there is only one Sylow 2-subgroup $H \leqslant G$ since $|H| = 4$. So $H \trianglelefteq G$.

Now look at possible semi-products $G = H \rtimes_\phi K$. So $\phi : K \to Aut(H)$, H has order 4 $\implies \begin{cases} H \cong C_4 \\ H \cong C_2 \times C_2 \end{cases}$

In Artin: Conjugation action (exists by Sylow II) of G on the Sylow 3-subgroups $G \curvearrowright \{K_1, K_2, K_3, K_4\}$ gives homomorphism $\phi : G \to S_4$.

Look at automorphism of $C_2 \times C_2 = \left\{ e, \underbrace{x, y, xy}_{\text{bijection of this set is an element of } S_3} \right\}$

Case $H \cong C_2 \times C_2$:

$$\phi : K \to Aut(C_2 \times C_2)$$
$$\langle k \rangle \mapsto (123), (132)$$

Since k has order 3, $\phi(k) = (123)$ or (132). Then we have two possibility:

(1) $\phi_k(x) = y, \phi_k(y) = xy, \phi_k(xy) = x$

(2) $\phi_k(x) = xy, \phi_k(y) = x, \phi_k(xy) = y$

So

$$G_1 = \left\langle k, x, y \mid kxk^{-1} = y, kyk^{-1} = xy, kxyk^{-1} = x, k^3 = x^2 = y^2 = e, xy = yx \right\rangle$$
$$G_2 = \left\langle k, x, y \mid kxk^{-1} = xy, kxyk^{-1} = y, kyk^{-1} = x, k^3 = x^2 = y^2 = e, xy = yx \right\rangle$$

See $G_1 \cong G_2 \cong A_4$ according to their presentation.

Case $H \cong C_4$: Let $\phi : K \to Aut(C_4) \cong C_2 \implies \phi$ is a trivial map going to id:$H \to H \implies K$ is normal, which contradicts the assumption $n_3 = 4$.

Case $n_3 = 1$: Let K be the Sylow 3-subgroup, hence K is a normal subgroup of order 3. Choose a Sylow 2-subgroup H which has order 4. Now consider possible semi-direct products: $G = K \rtimes_\phi H$. So we want to look at $\phi : H \to Aut(K) \cong Aut(C_3) \cong C_2$.

Case $H \cong C_4$: Let $H = \langle h \rangle$ (ord$(h) = 4$, ord$(h^2) = 2$). So $\phi_h : C_3 \to C_3$ is order 2, i.e. $\phi_h(x) = x^l \implies x^{l^2} = \phi_h^2(x_0 = x \implies l^2 \equiv 1 (\text{mod } 3) \implies l = 2 \implies \phi_h(x) = x^2 \implies hxh^{-1} = x^2$. So

$$G = \left\langle h, x \mid h^4 = x^3 = e, hxh^{-1} = x^2, hx = xh \right\rangle$$

Warning: $Aut(C_p \times C_q) \cong C_p^\times \times C_p^\times$ if $\gcd(p, q) = 1$

3.8 Midterm Review and Homework

Solution : Homework 7 #7

If $H \trianglelefteq G \implies N_G(H) = G$, so done. So we assume H is not normal in G.
Let $X = \{\text{conjugate subgroups of } H\} = \{gHg^{-1} \mid g \in G\}$. By a book theorem, we know $|X| = [G : N_G(H)]$. Let $H \curvearrowright X$ by conjugation. Since $H < G$ are p-groups, every orbit is a power of p. See that the orbit of $H \in X$ is order 1: $O_H = \{H\}$. Therefore, we have at least $p-1$ other orbits of order 1. So there exists some other $gHg^{-1} \in X$ whose orbits $= \{gHg^{-1}\}$. So $agHg^{-1}a^{-1} = gHg^{-1}$ for all $a \in H$. And then for $g \in G$ and any $a \in H$, we have $g^{-1}agHg^{-1}a^{-1}g = H \implies g^{-1}ag \in N_G(H)$ for all $a \in H$. However, since we are now looking at the situation where $gHg^{-1} \neq H$, there must exists some $a \in H$ such that $gag^{-1} \notin H$. Hence H is a proper subgroup of $N_G(H)$.
Suppose $H \in G$ is maximal. By previous conclusion, we know that $H < N_G(H) \implies N_G(H) = G \implies H \trianglelefteq G$. Lastly, we want to show maximal $H < G$ has $[G : H] = p$. Now consider the $Z(G) \neq G$ which must be non-trivial. And consider
Base case: $|G| = p^2$, abelian, so done
Induction: $|G| = p^k$ for $k < n$ has maximum normal subgroup of index p. Consider $|G| = p^n$ and then $|G/Z(G)| < p^n \implies G/Z(G)$ has a maximum subgroup of index p.

4 Midterm review

4.1 Group action

$G \curvearrowright X \Leftrightarrow \phi : G \to Perm(X) = S_{|X|}$. We can consider ϕ as a group homomorphism.
→ Definitions come directly:

$$\text{Orbits } (x \in X) : O_x = G \cdot x = \{y \in X \mid y = g \cdot x \text{ for some } g \in G\}$$
$$\text{Stabilizers } (x \in X) : \text{Stab}(x) = G_x = \{g \in G \mid g \cdot x = x\}$$

Proposition 4.1: Some important facts and properties

(1) Orbits partition X

(2) **Orbit-stabilizer theorem**: $|O_x| = [G : G_x] \implies |G| = |G_x| \cdot |O_x|$

(3) **Transitive** action has only one orbit. $(x, y \in X, \exists g \in G \text{ s.t. } g \cdot x = y)$
Free action: $g \cdot x = x \implies g = e$ and stabilizers all trivial
Faithful action: $g \cdot x = x$ for all $x \in X \implies g = e$

Some navigation:
- 6.7: group action
- 6.8 action of G on G/H.
- 6.10 action of G on subsets

Definition 4.2: Libraries of group actions

(1) $G \curvearrowright G$ by left multiplication

$$\phi : G \to Perm(G) = S_{|G|}$$
$$g \mapsto \phi_g : G \to G(\phi_g(x) = gx)$$

Free action $\implies$ ϕ injectibe (Cayley's thoerem)

(2) $G \curvearrowright G/H$ by left multiplication. Free action $\implies$ ϕ injective $\implies$ generalized Cayley.
Main idea: $H \leqslant \ker(\phi)$
Consequence:

$$|G/\ker(\phi)| \mid [G : H]!$$
$$|G/\ker(\phi)| \mid |G|$$

(3) $G \curvearrowright G$ by conjugation:

$$\phi : G \to Aut(G)$$
$$g \mapsto \phi_G : G \to G(\phi_x = gxg^{-1})$$

We know

$$\mathrm{Orb}(x) = Cl(x) = \left\{gxg^{-1} \mid g \in G\right\}$$
$$G_x = C_G(x) = \left\{g \in G \mid gxg^{-1} = x\right\}$$
$$|Cl(x)| = [G : C_G(x)]$$

This action is often used to find the class equation. And recall that $|Cl(x)| = 1 \implies x \in Z(G)$

(4) $G \curvearrowright$ Subgroups(G) (e.g. $G \curvearrowright \left\{gHg^{-1} \mid g \in G\right\}$ for $H \leqslant G$).
Consider the example: The action is forced to be transitive since X is exactly the set of conjugates of $H \leqslant G$. And $\mathrm{Stab}(K) = N_G(K)$ for $K \in X$. And by orbit-stabilizer thm,

$$|G| = |N_G(H)| \cdot (\text{number of conjugate subgroups of } H \leqslant G)$$

So

$$N_G(H) = G \Leftrightarrow H \trianglelefteq G \neq G$$

Notice: $|\mathrm{Orb}(H)| = 1$ for $H \trianglelefteq G \neq G$ in either action

(5) $G \curvearrowright \{S \subseteq G \mid |S| = m\}$ action given by left multiplication. Note this action gives a free action: $G \to S_m$

5 Ring

5.1 Intro to Ring

Definition 5.1

A ring is a set R together with two binary operation $+$ and $\cdot$ satisfying:

(1) $(R, +)$ is an abelian group (unit $= 0$)

(2) $\cdot$ is associative with unit (unit $= 1$)

(3) Distributive: $a \cdot (b + c) = ab + ac$

Definition 5.2: Commutative Ring

A commutative ring is a ring with commutative multiplication. (For our class, we'll only look at commutative ring)

Definition 5.3: Field

A field is a commutative ring where every element has a multiplicative inverse.
(An element of a ring with a multiplicative inverse is a unit.)

Example 5.4.

(1) $\mathbb{Z}$ with usual $+$ and $\cdot \to \mathbb{Z}^\times = \{+1, -1\}$.

(2) $\mathbb{Z}/n\mathbb{Z}$ with $+$ and $\cdot$ mod n. $\to (\mathbb{Z}/n\mathbb{Z})^\times = \{x \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(x, n) = 1\} \to (\mathbb{Z}/p\mathbb{Z})^\times \cong (\mathbb{Z}/(p-1)\mathbb{Z})^\times$

Notice: $R^\times = R \backslash \{0\} \Leftrightarrow R$ is a field

Proposition 5.5

Only ring where the $+$ identity (0) and the $\cdot$ identity (1) are equal is the 0 ring:

$$R = \{0\}$$

Proposition 5.6: Zero divisors

Element $a \in R$ such that exists $b \neq 0, b \in R$ such that $ab = 0$.

Definition 5.7: Domain

A ring with no zero divisors is called a (integral) domain.

Example 5.8. Non-commutative example ($\mathbb{F}$ is a field):

(1) $R = GL_n(\mathbb{F})$ → all non-0 elements are invertible, but not commutative so not a field.

(2) $R = M_(\mathbb{F})$ → non-invertible elements and some obvious zero divisors.

Now look at some other "integer" rings

- $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Check if ring:

  (1) $a + bi, c + di \in \mathbb{Z}[i] \to a + c + (b + d)i \in \mathbb{Z}[i]$

  (2) $a + bi \in \mathbb{Z}[i]$ then $-a - bi \in Z[i]$

  (3) $0 = 0 + 0i \in \mathbb{Z}[i]$

  (4) $(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in Z[i]$ because $\mathbb{Z}$ is a ring

  (5) Distributive: $(a + bi)[(c + di) + (e + fi)] = (a + bi)(c + di) + (a + bi)(e + fi)$

Definition 5.9: Polynomial ring

Let R be a ring and define the polynomial ring over R is the set $R[x]$ for some indeterminate element x given by:

$$R[x] = \left\{a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \mid n \in \mathbb{Z} \leqslant 0, a_0, a_1, ..., a_n \in R\right\}$$

Notice: $R \subset R[x]$ = degree 0 polynomials

Just like with integers, we have division in $\mathbb{Z}[x]$ in the following sense: fix $p(x) \in \mathbb{Z}[x]$ and then any $f(x) \in \mathbb{Z}[x]$ can be written

$$f(x) = q(x)p(x) + r(x)$$

Here the degree of r is strictly less than f. Then notice:

$$f(x) \in R[x], f(a) = 0 \Leftrightarrow (a - x) \in R[x] \text{ divides } f(x)$$

5.2 Division of Ring

Notation:

$$R[x] = \left\{a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \mid a_0, .., a_n \in R, n \in \mathbb{Z}_{\geqslant 0}\right\}$$

(It's a polynomial ring in one variable over R)

Proposition 5.10: 11.2.8

R commutative ring define a unique commutative ring structure on $R[x]$ satisfying:

(1) Addition: $f(x) + g(x) = \sum_k (a_k + b_k)x^k$

(2) Multiplication: $f(x) + g(x) = \sum_{i+j=k} a_i b_j x^{i+j}$

Proposition 5.11: 11.2.9 Division theorem for polynomial ring

Let $f, g \in R[x]$, f is a monic polynomial and there exists unique $q, r \in R[x]$ such that

$$g(x) = q(x)f(x) + r(x)$$

with degree $r <$ degree f.
(monic = lead coeff is 1)

Corollary 5.12: 11.2.10

Can divide by $f \in R[x]$ if the lead coeff is a unit in R.

Corollary 5.13: 11.2.11

$g \in R[x], x \in R$ then remainder of division of $g(x)$ by $x - \alpha$ is $g(\alpha) \in R$

5.3 Ring homomorphism

Definition 5.14: Ring homomorphism

Let R, S be rings, then a function $\phi : R \to S$ is a ring homomorphism if:

(1) $\phi(a + b) = \phi(a) + \phi(b)$

(2) $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$

(3) $\phi(1_R) = 1_S$

Example: $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

Definition 5.15: Evaluation homomorphism

Evaluation homomorphism $\alpha \in R$:

$$\phi_\alpha : R[x] \to R$$
$$P(x) \mapsto P(\alpha)$$

Proposition 5.16: 11.3.4: Substitution Principle

$\phi : R \to S$ a ring homomorphism

(a) $\alpha \in S$, then there exists a unique $\Phi : R[x] \to S$ which agrees with ϕ on R = constant polynomials $\subseteq R(x)$

and so that $x \mapsto \alpha$. That is,

$$\begin{cases} \Phi(r) = \phi(r) & r \in R \\ \Phi(x) = \alpha \end{cases}$$

(i.e.

$$\begin{aligned} \Phi(r_0 + r_1 x + r_2 x^2 + ... + r_n x^n) &= \Phi(r_0) + \Phi(r_1)\Phi(x) + ... \\ &= \phi(r_0) + \phi(r_1)\alpha + \phi(r_2)\alpha^2 + ... \end{aligned}$$

(b) $\alpha_1, ...\alpha_n \in S$, there exists unique $\Phi : R[x_1, ..., x_n] \to S$ that agrees with ϕ on R = degree 0 polynomials $\subseteq R[x]$ and $\Phi(\alpha_i) = x_i, i = 1, 2, ..., n$

Proof. Check that Φ is a ring homomorphism first, we'll skip addition and identity check here. Then multiplication: Let

$$f(x) = \sum_{i=0}^{n} a_i x^i;$$
$$g(x) = \sum_{j=0}^{n} b_j x^j.$$

Then

$$\begin{aligned} \Phi(fg) &= \Phi(\sum_{i,j=0}^{n} a_i b_j x^{i+j}) \\ &= \sum_{i,j=0}^{n} \Phi(a_i b_j x^{i+j}) \\ &= \sum_{i,j=0}^{n} \phi(a_i b_j)\alpha^{i+j} \\ &= \sum_{i,j=0}^{n} \phi(a_i)\phi(b_j)\alpha^{i+j} \\ &= (\sum_{i=0}^{n} \phi(a_i)\alpha^i)(\sum_{j=0}^{n} \phi(b_j)\alpha^j) \\ &= \Phi(f)\Phi(g) \end{aligned}$$

□

Example 5.17. Look at

$$\psi : R \to S$$
$$i : S \hookrightarrow S[x]$$

Compose: $\phi = (i \circ \psi) : R \to S[x]$. Apply substitution principle, ϕ can be extended to $R[x]$, $\Phi : R[x] \to S[x]$, which is a coefficient change homomorphism.

Specific example: $\phi : \mathbb{Z} \to \mathbb{F}_p, a \mapsto \overline{a} (\text{mod } p)$. Then $\Phi : \mathbb{Z}[x] \to \mathbb{F}_p[x]$, i.e.

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \mapsto \overline{f}(x) = \overline{a_0} + \overline{a_1} x + \overline{a_2} x^2 + ... + \overline{a_n} x^n$$

which changes in coefficient from $\mathbb{Z}$ to $\mathbb{F}_p$.

Another example: $R, P = R[x]$, apply substitution principle,

$$\Phi : R[x, y] \to P[y] = R[x][y]$$
$$p(x, y) = p_0 + p_1(x) y + p_2(x) y^2 + ... + p_n(x) y^n$$

Proposition 5.18: 11.3.10

R be a ring, exists unique homomorphism $\phi : \mathbb{Z} \to R$ defined

$$\phi : \mathbb{Z} \to R$$
$$n \mapsto \underbrace{1 + 1 + ... + 1}_{n \text{ times}}$$

Definition 5.19: Kernel of Ring

Kernel of $\phi : R \to S$ is: $\ker(\phi) = \{r \in R \mid \phi(r) = 0_s\}$

Definition 5.20: Ideal

The ideal $I \subseteq R$ subset closed under $+$ and $\cdot$ such that

$$s \in I, r \in R \implies rs \in I$$

Main example: the kernel $\ker(\phi)$ are ideals

Point (defining feature of ideal): linear combination of elements in I with coefficients in R are still in I.

Definition 5.21: Principle Ideal

The principle ideal generate by $a \in R$ is: $I = aR = Ra = (a) = \{ra \mid r \in R\}$. We have

- $(1) = 1R = R$
- $a \in R$ unit $\implies (a) = R$
  $(a) = (ra \mid r \in R)$, bust since a is a unit, we have $a^{-1} \in R$. Since $a \in (a), a^{-1} a \in (a) \implies 1 \in (a) \implies (a) = R$
- $(0) = 0R = \{0\}$ which is the trivial ideal (or zero ideal)

Example 5.22. Define

$$\begin{aligned}\phi_2 : \mathbb{R}[x] &\to \mathbb{R}\\ x &\mapsto 2\end{aligned}$$

Then the kernel is $\ker(\phi_2) = \{p(x) \in \mathbb{R}[x] \mid p(2) = 0\}$. Then by fundamental theorem of algebra,

$$\begin{aligned}p(2) = 0 &\Leftrightarrow (x-2) \mid p(x)\\ &\Leftrightarrow p(x) = q(x)(x-2)\end{aligned}$$

So $\ker(\phi_2) = \{q(x)9x-2) \mid q(x) \in \mathbb{R}[x]\} = (x-2) = (x-2)\mathbb{R}[x]$

Example 5.23. Look at the homomorphism

$$\begin{aligned}\Phi : \mathbb{R}[x,y] &\to \mathbb{R}[t]\\ x &\mapsto t^2\\ y &\mapsto t^3\end{aligned}$$

See $f(x,y) = x^3 - y^2 \in \ker(\Phi)$ since $f(t^2,t^3) = t^6 - t^6 = 0 \implies f \in \ker(\Phi)$. Now want to prove another containment: $\ker(\Phi) \subseteq (f)$. Consider $g \in \mathbb{R}[x,y]$ such that $g(t^2,t^3) = 0$. Since $f \in \mathbb{R}[x,y] = \mathbb{R}[x][y]$ is monic, so we can divide g by f:

$$g(x,y) = f(x,y)q(x,y) + r(x,y)$$

Then

$$\begin{aligned}f(x,y) &= y^2 - x^3\\ &= a_2(x)y^2 + a_1(x)y + a_0(x) \in \mathbb{Z}[x][y]\end{aligned}$$

By division algorithm, $deg_y(r(x,y)) < deg_y(f) = 2$, so

$$r(x,y) = r_1(x)y + r_0(x) \in \mathbb{Z}[x][y]$$

Therefore,

$$\begin{aligned}0 = g(t^2,t^3) &= q(t^2,t^3)f(t^2,t^3) + r(t^2,t^3)\\ &= 0 + r(t^2,t^3) \quad (f \in \ker(\Phi) \implies \text{ideal } qf \in \ker(\Phi))\\ \implies r(t^2,t^3) &= 0\\ r_1(t^2)t^3 + r_0(t^2) &= 0\end{aligned}$$

Since odd degree monomial + even degree monomial can't be zero, $r(x,y) = 0 \implies g(x,y) = f(x,y)q(x,y) \implies g \in (f) \implies \ker(\Phi) \subseteq (f)$

NICE FACT: $\mathbb{Q}[x], \mathbb{Z}$ are PID (**Principle ideal domain**) where all ideals are principle

Example 5.24. Look at another homomorphism (find the kernel)

$$\begin{aligned}\phi : \mathbb{Z}[x] &\to \mathbb{F}_p \\ f(x) &\mapsto f(0) (\text{mod } p)\end{aligned}$$

Then,

$$\begin{aligned} f(x) = p \in \mathbb{Z}[x] &\implies f(0) = p = 0 (\text{mod } p) \implies p \in \ker(\phi) \\ f(x) = x \in \mathbb{Z}[x] &\implies f(0) = 0 = 0 (\text{mod } p) \implies x \in \ker(\phi) \\ &\implies (p, x) \subseteq \ker(\phi)\end{aligned}$$

Now we want to show $\ker(\phi) \subseteq (p, x)$

$$\begin{aligned} f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x] &\implies f(0) = a_0 \\ &\implies a_0 \equiv 0 (\text{mod } p) \\ &\implies a_0 = bp \\ f(x) = a_0 + \sum_{k=1}^{n} a_k x^k & \\ = bp + x \sum_{k=1}^{n} a_k x^{k-1} & \\ = g_1(x)p + g_2(x)x &\end{aligned}$$

(p, x) is an ideal of $\mathbb{Z}[x] \implies \ker(\Phi) \subseteq (p, x)$

5.4 Play with Field

Proposition 5.25: 11.3.19

(a) the only two ideals in a field F are $(0) = \{0\}$ and $(1) = F$

(b) R with exactly two ideals, then R is a field

Corollary 5.26

Every homomorphism $F \to R$ is injective.

Proof. $\ker(\phi)$ is an ideal and so $\ker(\phi) = 0$ or 1. Can't be (1), because otherwise $\phi(x) \equiv 0$, then $\phi(1) = 1$ not a ring homomorphism. So only choice is $\ker(\phi) = \{0\} \implies \phi$ □

generator of $\ker(\mathbb{Z} \to R)$ is called characteristic of R

Proposition 5.27: 11.3.22

F is a field $\implies F[x]$ is a PID. And every ideal of $F[x]$ is generated by a unique monic polynomial of lowest degree in I.

Example 5.28. $\Phi : \mathbb{Q}[x] \to \mathbb{C}, x \mapsto 2^{\frac{1}{3}} = \gamma$. $\ker(\Phi) = K \subseteq \mathbb{Q}[x]$ ideal generated by monic polynomial of minimum degree having $f(\gamma) = 0$.
Consider $f(x) = x^3 - 2$ monic, $\in K \subseteq \mathbb{Q}[x]$. Note that $x^3 - 2 \neq g(x)h(x)$ for deg g, deg $h < 3 \implies x^3 - 2$ is minimum degree in $K \implies K = (x^3 - 2)$

Lemma 5.28.1: 11.3.24

If $f(x) \in \mathbb{Z}[x]$ monic and $f \mid g$ in $\mathbb{Q}[x]$, then $f \mid g$ in $\mathbb{Z}[x]$

Proof. Some intuition from an example: $g(x) = x^2 + \frac{1}{2}x + \frac{1}{3} \implies 6g(x) = 6x^2 + 3x + 2 \implies f|6g \in \mathbb{Z}[x]$ □

Corollary 5.29

$R = F[x], F$ is a field, $f, g \in R$. Now define $\gcd(f, g)$ = unique monic polynomial of minimum degree generated by (f, g). Recall, $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$ as subgroups of $(\mathbb{Z}, +)$. Let $d = \gcd(f, g)$,

(a) $Rd = Rf + Rg$

(b) $d \mid f, d \mid g$ in R

(c) $h \mid f, h \mid g \implies h \mid d$

(d) $d = pf + qg$ for some $p, q \in R$

Definition 5.30

The characteristic of a ring R is the minimum n so that $\underbrace{1 + 1 + \ldots + 1}_{n} = 0$

Example 5.31. $\mathbb{F}_p : char(\mathbb{F}_p) = p$
$\mathbb{Z}/n\mathbb{Z} : char = n$
$\mathbb{R}, \mathbb{C}, \mathbb{Z} : char = 0$

5.5 Quotient Rings

Definition 5.32

Let $I \subseteq R$ an ideal, $\implies I^+ \leqslant R+$ (subgroup of the additive group R). Then the cosets of $I+$ are $a+I$. And then we'll see that $R/I :=$ the set of cosets $a+I$ is a ring

Theorem 5.33: 11.4.1

$I \subseteq R$ ideal, there exists unique ring structure on R/I so that the function $\pi : R \to R/I, a \mapsto a+I = \overline{a}$ is a ring homomorphism whose kernel is I.

Proof. (partial proof)
Look at multiplication in R/I. The set

$$P = (a+I)(b+I) = \{rs \mid r \in a+I, s \in b+I\}$$

is not always a coset (!$= c+I$). But $P \subseteq ab+I$. If $r = a+u \in a+I, s = b+v \in b+I (u, v \in I)$. Then

$$\begin{aligned} rs &= (a+u)(b+v) \\ &= ab+av+ub+bv \in ab+I \end{aligned}$$

□

Theorem 5.34: 11.4.2 Mapping(Universal) property of quotient ring

- $f : R \to S$ be a ring homomorphism, $K = \ker(f)$
- $I \subseteq R$ ideal with $\pi : R \to R/I$ (canonical map)

Then

(a) $I \subseteq K$ then exists unique $\overline{f} : R/I$ so that $\overline{f} \circ \pi = f$

(b) **First isomorphism for rings:** f surjective, $I = K \implies \overline{f}$ is isomorphism

Theorem 5.35: 11.4.3 Correspondence theorem

Let $\phi : R \to S$ surjective, $K = \ker(\phi)$. Then we have bijection:

$$\begin{aligned} \{K \subseteq I \subseteq R\} &\longleftrightarrow \{J \subseteq S\} \\ I &\longrightarrow \phi(I) \\ \phi^{-1}(J) &\longleftarrow J \end{aligned}$$

Corollary 5.36

$I \longleftrightarrow J \implies R/I \cong S/J$

Example 5.37. Look at

$$\phi : \mathbb{C}[x,y] \to \mathbb{C}[t]$$
$$x \mapsto t$$
$$y \mapsto t^2$$

Then $\ker(\phi) = (y - x^2) \subseteq \mathbb{C}[x,y] \longleftrightarrow J \subseteq \mathbb{C}[t]$. Now know: $\mathbb{C}[t]$ is a PID $\implies J = (f(t))$. Consider $I_1 = (y - x^2, f(x))$, $K \subseteq I$ and $\phi(I_1) = J$

5.6 Maximal Ideal

Consider a homomorphism $\phi : R \to F$. Then the ideals of ϕ are:

$$I_\phi = \phi^{-1}((0)), \text{ and } \phi^{-1}((1))$$

We know $R = \phi^{-1}((1)) = \phi^{-1}(F)$. Recall that fields only have 2 ideals: (0) and (1) (Notation: $(a) = aR = \{ar \mid r \in R\}$. If we apply correspondence theorem to the homomorphism, the only ideals of R that contain I are I and R. Because of this, I is called a maximal ideal.

Definition 5.38: Maximal Ideal

The maximal ideal M is a proper ideal ($M \neq R$) that is not contained in any other proper ideal.

Proposition 5.39: 11.8.2

(1) Let $\phi : R \to R'$ be a surjective ring homomorphism, with kernel I. The image R' is a field if and only if I is a maximal ideal.

(2) And ideal I of a ring R is maximal if and only if $\overline{R} = R/I$ is a field.

(3) The zero ideal of a ring R is maximal if and only if R is a field.

Proposition 5.40: 11.8.3

The maximal ideal of the ring $\mathbb{Z}$ of integers are the principal ideals generated by prime integers

Proof. We know $\mathbb{Z}$ is a PID. Consider a principle ideal generated by n. If n is a prime, then $\mathbb{Z}/(n) = \mathbb{F}_p$ is a field $\implies (n)$ is a maximal. If n is not prime, then $n = 0, 1,$ or has form of $n = ab$ where $1 < a < n$. It's clear that zero and unit ideal is no maximal. And notice $1 \notin (a), a \notin (n), n \in (a)$, so $(n) < (a) < R$. So (n) is not a maximal. □

Definition 5.41: Irreducible

A polynomial with coefficients in a field is called irreducible if it is not sonstant and if its is not the product of the two non-constant poly

Proposition 5.42: 11.8.4

(a) Let F be a field. The maximal ideals of $F[x]$ are the principal ideals generated by the monic irreducible polynomials.
(b) Let $\phi : F[x] \to R'$ be a homomorphism to an integral domain R' and let P be the kernel of ϕ. P is either a maximal ideal or $P = (0)$.