1 Chapter 1: Matrices (Review)

Proposition 1.0.1

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 1.0.2

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 1.0.3

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

Definition 1.0.4: Symmetric group

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

Proposition 1.0.5

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

Proposition 1.0.6

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 1.0.7: 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 3.0.1: 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 3.0.2

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

Definition 3.0.3: 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 3.0.4

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

Definition 3.0.5: 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 3.0.6: Subspace

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

(1) closed under $+$,

(2) closed under scalar multiplication $\cdot$

Definition 3.0.7: Direct Sum

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

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

(2) $W_1, W_2, \ldots, W_k$ 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 2.2.1: 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 2.2.2

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

Example 2.2.3.

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

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

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

(4) S_n symmetric group of n letters

Note: NOT ALL GROUPS ARE ABELIAN

Proposition 2.2.4: 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 2.2.5: 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 2.2.6. $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) : |A| = 1\}$,$SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

Proposition 2.2.7

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

Definition 2.2.9: 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 2.3.1: 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 2.3.2

The group $\mathbb{Z}a + \mathbb{Z}b = \langle a, b\rangle = \{\text{all possible products of a and b under group operation}\}$ 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 2.3.3

$a, b \in \mathbb{Z}$ 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 2.3.4. $a = 321, b = 123$. 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 2.3.5: 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 2.3.6

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

2.4 Cyclic Group

Definition 2.4.1: Cyclic groups

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

Proposition 2.4.2

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

(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 2.4.3: 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 2.4.4: 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 2.4.5. $S_3 = \langle (123), (12) \rangle$.
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 2.4.6. $GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0 \right\}$:
$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order. $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ has order 6.

Proposition 2.4.7

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 2.4.8: 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 2.4.9. 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 2.4.10

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 2.5.1: 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 2.5.2.

(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: $H \subseteq G, H \leftrightarrow G, h \to h$

Proposition 2.5.3

$\phi : G_1 \to G_2$ 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 2.5.4: Subgroups associated to how $G_1 \to G_2$

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

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

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

Proof. **Closure:** $g, h \in \text{im}(e)$, so $g = \phi(x), h = \phi(y)$ for some $x, y \in G$. So $gh = \phi(x)\phi(y) = \phi(xy) \implies \text{im}(\phi)$ because $xy \in G_1$. **Inverse:** $g \in \text{im}(\phi) \implies g = \phi(x)$ for some $x \implies g^{-1} = \phi^{-1}(x) = \phi(x^{-1}) \implies g^{-1} \in \text{im}(\phi)$ 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 2.5.5.

(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 2.5.6

$\phi : G_1 \to G_2$ 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 2.5.7

(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 2.5.8: 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 2.5.9

Equivalent:

(1) $gN = Ng$

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

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

Proposition 2.5.10

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 2.5.11: 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 2.5.12

$Z(G)$ 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 2.6.1: 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 2.6.2.

(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 2.6.2.1

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

Definition 2.6.3: 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 2.6.4

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 2.6.5: 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 2.6.6: Commutator subgroup

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

2.7 Equivalence relation

Definition 2.7.1: 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 2.7.2. Conjugacy on a group. Because $a \sim b \Leftrightarrow$ exists g s.t. $a = gbg^{-1}$

Definition 2.7.3: Partition of S

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

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

Example 2.7.4.

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

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

Proposition 2.7.5

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 2.7.5.1

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 2.7.6: 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 2.7.7.
$\mathbb{Z} =$ Even $\sqcup$ Odd.
Even $= C_0 = C_2 = C_4 = \ldots \to$ [Even] $= \overline{0}$
Odd $= C_1 = C_3 = C_4 = \ldots \to$ [Odd] $= \overline{1}$
So group $\overline{\mathbb{Z}} = \{\overline{1}, \overline{0}\}$

Definition 2.7.8: 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 2.7.9.

(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 2.7.10

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

(1) $aK = bK$

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

(3) $b \in aK$

Proposition 2.7.11

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 2.8.1: 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 2.8.2

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

Example 2.8.3. $G = S_3$, $H = \langle y \rangle$. Let $x = (123), y = (12)$. $H = \{e, y\} = yH$. And $xH = \{x, xy\} = xyH$. And $x^2H = \{x^2, x^2y\} = x^2yH$.

Proposition 2.8.4

$a, b \in G$ 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 2.8.5

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 2.8.5.1

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 2.8.6: I

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

Theorem 2.8.7: Lagrange's Theorem

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

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

Corollary 2.8.8

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

Corollary 2.8.9

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

Corollary 2.8.10

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 2.8.11: 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 2.9.1: 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: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ □

Proposition 2.9.2

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

Lemma 2.9.2.1

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

Definition 2.9.3: 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: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ □

Proposition 2.9.4

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

Lemma 2.9.4.1

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

Example 2.9.5. 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 2.9.6: 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 2.10.1: Restriction

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

$$\phi\mid_H = H \to G$$

We have:

$$\begin{aligned} \ker(\phi\mid_H) &= \ker(\phi) \cap H \\ \operatorname{im}(\phi\mid_H) &= \phi(H) \end{aligned}$$

Corollary 2.10.2

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 2.10.3. $H \leqslant$ 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 2.10.4

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

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

Theorem 2.10.6: 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 $\phi^{-1}(\phi(H)) \subseteq H \implies H = \phi^{-1}(\phi(H))$

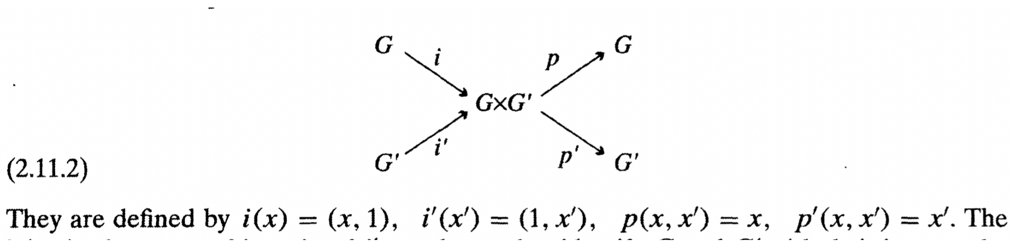
(5) $|\phi^{-1}(H')| = |H'| \cdot |K|$.

□

2.11 Product groups

Definition 2.11.1

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: $(g_1 g_1')(g_2 g_2') = (g_1 g_2, g_1' g_2')$



Product group example in book

Theorem 2.11.2

$\gcd(r,s) = 1$ then $C_{rs} = C_r \times C_s$.

Notation: C_n = cyclic group of order n.

Example 2.11.3.

(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 2.11.4

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 $f(h_1,k_1) = f(h_2,k_2) \implies h_1k_1 = h_2k_2 \implies h_2^{-1}h_1 = k_2k_1^{-1}$. So because $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$, $h_2 = h_1$ and $k_2 = k_1 \implies$ f injective

(2) (Left to right) f homomorphism, $(h_1,k_1),(h_2,k_2) \in H \times K \implies (h_1h_2, k_1k_2) \in H \times K$ and $f(h_1h_2,k_1k_2) = h_1h_2k_1k_2 = f(h_1,k_1) \times f(h_2,k_2) = h_1k_2h_2k_2 \implies h_2k_1 = k_1h_2$. 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 2.11.5: 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 2.12.1

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 2.12.1.1

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

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

Lemma 2.12.1.2

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

□

Corollary 2.12.2

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

Example 2.12.3. $H = \langle(12)\rangle \in S_3$ 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 2.12.4: First Isomorphism Theorem

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

Proposition 2.12.5

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. □