PMATH 336 Notes

velo.x.

Contents

1 Group

1.1 Isometry - Jan 9

Group theory is the mathematical study of symmetry.

Symmetry is vaguely speaking, undetectable changes.

Definition 1.1.1.
Let X, Y be sets, a function $f : X \to Y$ is called

- injective: if $f(x) = f(x')$ implies $x = x'$ in X.
- surjective: if for all $y \in Y$, exists $x \in X$, $f(x) = y$.
- bijective: f is injective and surjective.

Definition 1.1.2 — isometry.
An **isometry** is a bijection that preserves distance, $\text{dist}(x, x') = \text{dist}(f(x), f'(x'))$ for all $x, x' \in X$.

Example 1.1.1. Consider $\mathbb{R}^n$ with euclidean distance d which $d(\vec{s}, \vec{t}) = ((x_i - y_i)^2 + \cdots + (x_n - y_n)^2)^{1/2}$. Then some isometires include translations $f(\vec{x}) = \vec{x} + \vec{a}$ for all $\vec{x}$, rotations, reflections.

Definition 1.1.3.
A **symmetry** of a set $X \subseteq \mathbb{R}^n$ is an isometry $f : \mathbb{R}^n \to \mathbb{R}^n$ s.t. $f(X) = X$ and $f^{-1}(X) = \{\vec{v} \in \mathbb{R}^n : f(\vec{v}) \in X\} = X$.

Remark 1.1.4. Each geometric object determines its own collection of symmetries.

Definition 1.1.5.
A nonempty collection of isometries is called a group of isometries if it is closed under fucntion composition and taking inverses.

Remark 1.1.6. The symmetry of any subset $X \subseteq \mathbb{R}^n$ form a group of symmetries.

Definition 1.1.7 — order.
A isometry f has order n if $f^n = 1$ but $f^k \neq 1$ for all $1 \leq k < n$. (order is unique)

1.2 Cayley Table - Jan 11

DEFINITION 1.2.1 — CAYLEY TABLE.
Composition of elements of a symmetry group can be organized into a multiplication table.

Example 1.2.1. (For 'H' .)

	1	A	B	C
1	$1 \circ 1 = 1$			
A	A	1	C	B
B	B	C	1	A
C	C	B	A	1

Example 1.2.2.

Remark 1.2.2. So far, our discussion is a bit misleading as our shapes have symmetrys that "commute" (i.e. $fg = gf$), however that is not the case in general.

For exammple

Example 1.2.3.

DEFINITION 1.2.3 — COMPLEX NUMBER.
$\mathbb{C} = \{a + bi \mid ab \in \mathbb{R}, i = \sqrt{-1}\}$

Example 1.2.4. $S = \{1, -1, i, -i\}$, then $\forall s, s' \in S$, $ss' \in S$. Again, we form a table:

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

This is structurally similar to symmetries of "rotation". For each $s \in S$, there is a unqiue $s' \in S$ such that $ss' = s's = 1$.

THEOREM 1.2.4 — WELL-ORDERING PRINCIPLE.
Each nonempty set of positive integers has a smallest element. (this is equivalent to mathematical induction)

DEFINITION 1.2.5.
a **divides** b if there is a **quotient** q such that $b = aq$, $a, b, q \in \mathbb{Z}$. Some properties: for all $u, v, a, b, c \in \mathbb{Z}$

1. $uv = 1 \iff (u = v = 1$ or $u = v = -1)$
2. $a|b, b|a \Rightarrow a = \pm b$

3. $a|b$, $b|c \Rightarrow a|c$.

4. $a|b$, $a|c \Rightarrow a|sb+tc, s,t \in \mathbb{Z}$

Proposition 1.2.1 (Division with remainders)**.** For any integers a, d with $d > 0$, there exist unique integers q, r such that $a = qd + r$ with $0 \leq r < d$.

Proof. Existence: let $S = \{a - kd \,|\, k \in \mathbb{Z}, a - kd \geq 0\}$.

Claim: $S \neq \varnothing$.

Proof of Claim:

- Say $a > 0 \Rightarrow a - 0 \cdot d = a \in S$
- Say $a < 0 \Rightarrow a - (2a)d = a(1-2d) \in S$.

If $0 \in S$, then $a = qd + r$ for $r = 0$ and some q. (so assume all $s \in S$ are positive). Well-ordering principle tells us S has a smallest element r.

Because $r = a - qd$, i.e. $a = qd + r$. Assume for contradiction that $r \geq d$, then $a - (q+1)d = a - qd - d = r - d \geq 0$, but $a - (q+1)d < a - qd$. Contradiction. So $r < d$ must hold.

Now to prove uniquenss. Assume $qd + r = a = q'd + r'$, $r' \geq r$. □

1.3 Jan 13

Definition 1.3.1.
A positive integer d is the **greatest common divisor**(gcd) of given nonzero integers m, n, denoted $\gcd(m, n) = d$, if

(a) $d|m$ and $d|n$

(b) if $x \in \mathbb{Z}_{>0}$ divides m and n, then $x|d$.

(2) implies that the gcd of two integers must be unique. Therefore, we can also analogously define $\gcd(n_1, n_2, \ldots, n_r)$ for $r \geq 2$.

Proposition 1.3.1 (Existence of gcd)**.** For all $m, n \in \mathbb{Z} \setminus \{0\}$, there exist $s, t \in \mathbb{Z}$ s.t.

$$\gcd(m, n) = sm + tn\ .$$

moreover, $\gcd(m, n)$ is the <u>smallest such positive integer</u>.

Proof. "smallest" and "positive" should remind of well-ordering principle

Let $S = \{km + ln \,|\, k, l \in \mathbb{Z}, km + ln > 0\} \neq \varnothing$. Apply well-ordering principle, exists $d = sm + tn > 0 \in S$, which $\forall s \in S, d \geq s$.

Now by Proposition 1.1.1 (Division with remainders), $m = qd + r$, $0 \leq r < d$. But $r = m - qd = m - q(sm + tn) = (1 - qs)m + (-qt)n$. This forces $r = 0$, by definition of d. Therefore, $d|m$. And by symmetry $d|n$.

Now suppose $x \in \mathbb{Z}_{>0}$, $x|m$ and $x|n$, then $m = q'x$, $n = q''x$, then $d = sm + tn = s(q'x) + t(q''x) = (sq' + tq'')x \Rightarrow x|d$. Therefore, $\gcd(m, n) = d$. □

Remark 1.3.2. Let $\langle m, n\rangle = \{km + ln \,|\, k, l \in \mathbb{Z}\}$. Then $d \in \langle m, n\rangle$ and every element of $\langle m, n\rangle$ is divisible by d. In fact, $\langle m, n\rangle = \langle d\rangle = \{k, d|k \in \mathbb{Z}\}$.

Definition 1.3.3.
Nonzero integers m, n are relatively prime if $\gcd(m, n) = 1$. i.e. $sm + tn = 1$ for some $s, t \in \mathbb{Z}$. Similarly, nonzero integers $n_1, n_2, \ldots n_r$, $r \geq 2$ are relatively prime $\iff$ $\gcd(n_1, \ldots, n_r) = 1$.

Example 1.3.1. $1 = (-3) \cdot 21 + 4 \cdot 16 \Rightarrow 21$ and 16 are relatively prime.

Lemma 1.3.1 (Euclid)**.** If p is prime, and $p|ab$, then $p|a$ or $p|b$.

Proof. $p \not| a \Rightarrow \gcd(p, a) = 1 \iff 1 = sp + ta \Rightarrow b = spb + tab \Rightarrow p|b$. □

Definition 1.3.4.
Given $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, a is congruent to b modulo n if $n|a - b$, denoted $a \equiv b \mod n$.

Properties: $\forall a, b \in \mathbb{Z}$,

1. reflexive: $a \equiv a \mod n$
2. symmetry: $a \equiv b \mod n \iff b \equiv a \mod n$
3. transitive: $a \equiv b \mod n, b \equiv c \mod n \Rightarrow a \equiv c \mod n$.

Remark 1.3.5. We can work with $+$ and $\times$ modulo n, this is well-defined and satisfies **MOST** usual rules of arithmetic but there are exceptions. For example $4 \cdot 2 \equiv 4 \cdot 5 \mod 12$ but cancellation does not work because $2 \not\equiv 5 \mod 12$.

Proposition 1.3.2 (Chinese Remainder Theorem)**.** Suppose $\gcd(m, n) = 1$, for $m, n \in \mathbb{Z} \setminus \{0\}$, and let $a, b \in \mathbb{Z}$, then there exists $x \in \mathbb{Z}$ s.t.

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \tag{1}$$

x is unique modulo mn.

Proof. There exists $s, t \in \mathbb{Z}$ such that $sm + tn = 1$. Let $x_1 = 1 - sm = tn$ so $x_1 \equiv 1 \mod m$ and $x_1 \equiv 0 \mod n$; and let $x_2 = 1 - tn = sm$ so $x_2 \equiv 0 \mod m$ and $x_2 \equiv 1 \mod n$. Then $x = ax_1 + bx_2$ satisfies (1).

If also $x' \equiv a \mod m$ and $x' \equiv b \mod n$. Then $x - x' = a - a \equiv 0 \mod n$ and similarly $x - x -' \equiv 0 \mod n$. Therefore, $m, n | x - x'$, since $\gcd(m, n) = 1$, $mn | x - x'$. $x \equiv x' \mod mn$. $\square$

1.4 Groups - Jan 16 Mon & Jan 18 Wed

DEFINITION 1.4.1 — BINARY OPERATION.
Let G be a set. A **binary operation** on G is a function $* : G \times G \to G$, $(a, b) \to a * b$.

Example 1.4.1. In $\mathbb{Z}$,

- $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(m, n) \mapsto m + n$.
- $\min : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(m, n) \mapsto \min(m, n)$.

Example 1.4.2. $\mathbb{Z}/n$ denote the set $\{0, 1, 2, ..., n - 1\}$. (other notations $\mathbb{Z}/_{<n>}$ or $\mathbb{Z}_n$ or $\mathbb{Z}/_n\mathbb{Z}$)

- $(a, b) \mapsto$ the unique r, $0 \leq r < n$ such that $a + b = qn + r$
- $(a, b) \mapsto$ the unique r, $0 \leq r < n$ such that $ab = qn + r$

*** IMPORTANT ***

DEFINITION 1.4.2 — GROUP.
A **group** is a set G with a binary operator $* : G \times G \to G$ that satisfies

- identity: exists $e \in G$, for all $a \in G$, $e * a = a = a * e$.
- associativity: $(a * b) * c = a * (b * c)$
- inverse: for all $a \in G$ there is an inverse $a' \in G$ s.t. $a * a' = a' * a = e$.

DEFINITION 1.4.3 — ABELIAN.
If $(G * n)$ is a group staisfying $a * b = b * a$ for all $a, b \in G$, then G is **abelian**.

Remark 1.4.4. We usually omit $*$: G is a group.

Example 1.4.3. Examples and nonexamples of groups:

- $(\mathbb{Z}, +)$ yes, $(\mathbb{Z}, \times)$ no, $(\mathbb{Q}_{>0}, \times)$ yes, $(\mathbb{Z}_{>0}, +)$ no.
- $(\{1\} \cup (\mathbb{R} \setminus \mathbb{Q})_{>0}, \times)$ NO!.
- $(\mathbb{Z}/n, +)$ yes; $(\mathbb{Z}/n, \times)$ it depends
- $GL_n(\mathbb{R})$ = set of invertible elements in $Mat_{n \times n}(\mathbb{R})$ with matrix multiplication is a group. $(AB)^{-1} = A^{-1}B^{-1}$.

THEOREM 1.4.5 — UNIQUENESS OF THE IDENTITY.
In any group G, the identity is unique.

Proof. Suppose e, e' are both identities, then $e = ee' = e'$. □

Theorem 1.4.6 — Cancellation.
In any group G, both right and left cancellation hold. i.e. $ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$.

Proof.

$$ba = ca \quad \Rightarrow \quad (ba)a^{-1} = (ca)a^{-1} \quad \Rightarrow \quad b(aa^{-1}) = c(aa^{-1}) \quad \Rightarrow \quad b = c\ .$$

□

Theorem 1.4.7 — Uniqueness of Inverses.
For any group G, for any element a in G, there is a unique element $b \in G$, $ab = ba = e$.

Proof. Suppose a', a'' are both inverses of a, then cancellation law gives

$$aa' = e = aa'' \quad \Rightarrow \quad a' = a''$$

□

Theorem 1.4.8 — Socks-Shoes Property.
For any group G, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

$$\begin{aligned}(ab)(b^{-1}a^{-1}) =& a(b(b^{-1}a^{-1})) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e\\ \Rightarrow (ab)^{-1} = b^{-1}a^{-1}\ .\end{aligned}$$

□

Remark 1.4.9. Associativity of the group operation ensures that triple-products are unambiguous: $(ab)c = a(bc)$. Ways to mltiply four elements in G.:

$$a(b(cd)), a((bc)d), (ab)(cd), (a(bc))d, ((ab)c)d\ ,$$

and we can reduce to $a(bcd), (ab)(cd), (abc)d$. Therefore, $abcd$ is unambiguous. By induction, $a_1a_2...a_n$ is unambiguous.

Remark 1.4.10. $(ab)^n \neq a^nb^n$ because groups do not necessarily commute.

Lemma 1.4.1. In any group G, the equations $ax = b$ and $xa = b$ each have a unique solution.

Proof. $ax = b \Rightarrow x = a^{-1}b$. □

Example 1.4.4. Let $(\mathbb{Z}/n)^\times$ denote the set of elements in $\mathbb{Z}/n$ which have multiplicative inverses. Then $(ex.)$ $a \in (\mathbb{Z}/n)^\times \iff \gcd(a,b) = 1$. Also, exists $(\mathbb{Z}/n)^\times$ forms a group with respect to multiplication mod n, called **the group of units modulo** n.

For example, $(\mathbb{Z}/6)^\times = \{1,5\} = \{\pm 1\}$, $(\mathbb{Z}/10)^\times = \{1,3,7,9\} = \{\pm 1, \pm 3\}$, $(\mathbb{Z}/7)^\times = \{1,2,3,4,5,6\}$, $(\mathbb{Z})^\times = \{\pm 1\}$.

Definition 1.4.11.
The number of elements of a group G is the **order** of G; denoted $|G|$; $|G|$ can be finite or infinite.

The **order of** $g \in G$ is the minimal $n \in \mathbb{Z}_{>0}$ such that $g^n \in e$, denoted $|g|$; if no such n exists, then g has **infinite order**.

Example 1.4.5. $1 \in (\mathbb{Z}/n, +)$ has $1 = n$. $1 \in \mathbb{Z}$ has $|1| = \infty$.

Example 1.4.6. In a finite group, each element has finite order.

1.5 Subgroup - Jan 18, 20, 23

Definition 1.5.1 — Subgroup.
Let G be group and $H \subseteq G$. Then H is a **subgroup** of G if H is a group under $*$. Denoted $H \leq G$.

Example 1.5.1. Examples of subgroups:

- $\{1\} \subseteq (\mathbb{Z}/7)^{\times}$
- $\{e\} \subseteq G$ is a subgroup, so is $G \subseteq G$.

Example 1.5.2. Recall, $GL_n(\mathbb{R})$ is a group under matrix multiplication. The general linear group. So is $GL_n(\mathbb{F})$ is a group where say $\mathbb{F}$ is $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p$ prime.

$$GL_n(\mathbb{F}) = \{[a_{i,j}]_{1 \leq i,j \leq n} \mid a_{i,j} \in \mathbb{F} \text{ and } \det[a_{i,j}] \neq 0\}$$

is a group because $\det(AB) = \det(A)\det(B)$.

The special linear group of $n \times n$ matrices with entries in $\mathbb{F}$ is

$$SL_n(\mathbb{F}) = \{[a_{i,j}]_{1 \leq i,j \leq n} \mid \text{each } a_{i,j} \in \mathbb{F}, \det[a_{i,j}] = 1\}$$

with matrix multiplication. It is also a group and it's a subset of $GL_n(\mathbb{F})$, in fact it is a subgroup.

Example 1.5.3. Let $A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$. $A \notin SL_2(\mathbb{R})$ but in $SL_2(\mathbb{Z}/5)$.

Theorem 1.5.2 — Subgroup Test.
Let G be a group, let $\varnothing \neq H \subseteq G$, if the properties

1. for all $h, k \in H$, have $hk \in H$.
2. for all $h \in H$, we have $h^{-1} \in H$.

Both hold, then we have $H \leq G$.

Proof. Lets check that H is a group under

- Consider $G \times G \to G$,
- associativity: guaranteed because G is a group
- inverses: every element in H has an inverse in H
- identity: for any $h \in H$, $h^{-1} \in H$, then $e = hh^{-1}$.

□

Example 1.5.4. To verify $H = SL_n(\mathbb{F}) \leq GL_n(\mathbb{F}) = G$, note,

- $H \neq vanothin$ becasue $I \in H$

- if $A, B \in H$, then $\det(AB) = \det(A)\det(B) = 11 = 1$.
- if $A \in H$, then $1 = \det(I) = \det(A^{-1})(\det A)^{-1}(\det(A^{-1})) = \det(A^{-1})$

Hence, indeed $SL_n(\mathbb{F}) \le GL_n(\mathbb{F})$.

Theorem 1.5.3 — One-step Subgroup Test.
Let G be a group, $\varnothing \neq H \subseteq G$. Then $H \le G$ if for all $h, k \in H$, have $hk^{-1} \in H$.

Example 1.5.5. Let $O_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid A^{-1} = A^t\}$. Is this a group?

- $O_n(\mathbb{F}) \neq \varnothing$, because $I^{-1} = I = I^t$.
- Let $A, B \in O_n(\mathbb{F})$, want $AB^{-1} \in O_n(\mathbb{F})$.

$$(AB^{-1})^t = (B^{-1})^t A^t = (B^t)^t A^t = (B^t)^t A^{-1} = BA^{-1} = (B^{-1})^{-1} A^{-1} = (AB^{-1})^{-1} \, .$$

So $O_n(\mathbb{F})$ is a subgroup of $GL_n(\mathbb{F})$, called the **orthogonal group**.

Example 1.5.6. A group can have various subgroups of different orders and satisfying various inclusions: X =square in $\mathbb{R}^2$. Then $G = Sym(X) > \{1, r, r^2, r^3\} = H$. And $G > \{1, R_1\}$

Example 1.5.7. Let G be abelian, $H = \{a \in G \mid |a| < \infty\}$. Then $H \le G$:

- $H \neq \varnothing$: $|e| = 1 \Rightarrow e \in H$.
- let $a, b \in H$, say $|a| = m$, $|b| = n$.
- if $a \in H$ and $|a| = m$, then $a^m = e$ so $(a^{-1})^m = (a^{-1})^m a^m = e$. Hence, $|a^{-1}| = m < \infty$ so $a^{-1} \in H$.

Theorem 1.5.4 — Finite Subgroup Test.
Let G be a group, $\varnothing \neq H \subseteq G$, $\#H < \infty$ (number of elements in H is finite). Then $H \le G$ holds, if for all $h, k \in H$, $hk \in H$.

Remark 1.5.5. To show $H \subseteq G$ is not a subgroup, exhibit a counter-example to any of the properties:

- $e \notin H$
- give $h, k \in H$ with $hk \notin H$
- give $h \in H$ with $h^{-1} \notin H$

Definition 1.5.6 — Cyclic Subgroup Generated by a.
Let G group, $a \in G$, the set $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = \{a^0, a, a^1, a^{-1}, a^2, a^{-2}, \ldots\}$ is a subsgroup of G, called the **cyclic subgroup generated by** a.

Proof.
- $a \in \langle a \rangle \Rightarrow \langle a \rangle \neq \varnothing$.

- for all $k, l \in \mathbb{Z}$, $a^k a^l = a^{k+l} \in \langle a \rangle$.
- for all $k \in bZ$, $a^k \cdots a^{-k} = e$ and $a^{-k} \in \langle a \rangle$.

$\square$

Remark 1.5.7. Even though the list $e, a, a^{-1}, a^2, \ldots$ is infinite, $\langle a \rangle$ can be finite.

Example 1.5.8. In $\mathbb{Z} = (\mathbb{Z}, +)$, $\langle 1 \rangle = \{0, 1, -1, 2, -2, \ldots\} = \mathbb{Z} = \langle -1 \rangle$.

In $\mathbb{Z}/10$, $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$.

In $(\mathbb{Z}/15)^\times$, $\langle 7 \rangle = \{1, 7, 4, 13\}$.

Definition 1.5.8.
Let $\varnothing \neq S \subseteq G$. The **subgroup of** G **generated by** S is the smallest subgroup of G that contain S, denoted $\langle S \rangle$. The subgroup $\langle S \rangle$ can be characterized in the following ways:

1. the subgroup of G satisfying: $S \subseteq \langle S \rangle$ and if $S \subseteq H \leq G$ holds, then $\langle S \rangle \subseteq H$ holds.
2. $\langle S \rangle = \bigcap_{H \leq G, S \subseteq H} H$; or
3. $\langle S \rangle = \{a_1 a_2 \cdots a_r \,|\, r \in Z_{>0},\ \text{each} a_i \in S \text{ or } a_i^{-1} \in S\}$

Example 1.5.9. Recall for $m, n \in \mathbb{Z}$, $\langle m, n \rangle = \{km + ln \,|\, k, l \in \mathbb{Z}\}$ e.g. $\langle 8, 14 \rangle = \langle 2 = 2\mathbb{Z} \rangle$.

Definition 1.5.9.
In $\mathbb{C}$,

$$\langle 1, i \rangle = \{k + li \,|\, k, l \in \mathbb{Z}\} = \mathbb{Z}[i]$$

is called the Gaussian integers

Example 1.5.10. Cyclic subgroups are abelian.

Definition 1.5.10 — Centralizer.
Let $a \in G$, G is a group. The **centralizer of** a **in** G is the set

$$C(a) = \{g \in G \,|\, ga = ag\}\ .$$

Theorem 1.5.11 .
For any $a \in G$, $C(a)$ is a group.

Proof.
- $C(a) \neq \varnothing$, because $ea = ae = a \Rightarrow$
- Let $g, h \in C(a)$, does $(gh)a = a(gh)$ hold? $(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$.

- For all $g \in C(a)$,

$$\begin{aligned} ga = ag \iff g^{-1}(ga) =& g^{-1}(ag) \\ a =& g^{-1}ag \\ ag^{-1} =& g^{-1}agg^{-1} = g^{-1}a \ . \end{aligned}$$

  $g^{-1} \in C(a)$.

Therefore, $C(a) \leq G$ holds. □

Example 1.5.11. $X =$ square. $G = Sym(X)$.

Example 1.5.12. Also $C(R_2) = \{id, R_2, r^2, R_4\}$. $R_2R_4 = r^2 = R_4R_2$.

Note 1.5.12. $\forall a \in G$, $\langle a \rangle \leq C(a) \leq G$.

2 Cyclic Groups

2.1 Properties of Cyclic Groups - Jan 25, 27

Definition 2.1.1.
A group is **cyclic** if there is $a \in G$ s.t. $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, in this case a generates G.

Example 2.1.1. 1 and -1 are both generators of $(bZ, +)$.

Example 2.1.2. $\mathbb{Z}/8$ is generated by 1, but also $3, 5, 7$.

Theorem 2.1.2 — Criterion of $a^i = a^j$.
Let G be a group and $a \in G$. Let $i, j \in \mathbb{Z}$. Then

- if $|a| = \infty$, then $a^i = a^j \iff i = j$.
- if $|a| < \infty$, then $n = |a| \in \mathbb{Z}$, we have $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and moreover, $a^i = a^j \iff n \big| i - j$.

Proof. $\underline{\text{Case } |a| = \infty}$: Know $a^k \neq e$ for all $k \in \mathbb{Z} \setminus \{0\}$. Then, $a^i = a^j \iff a^{i-j} = e \iff i - j = 0 \iff i = j$.

$\underline{\text{Case } |a| < \infty}$: Division algorithm tells that $k = qn+r$ with $0 \leq r < n$, then $a^k = a^{qn+r} = a^{qn}a^r = a^r \in \{e, a, a^2, \ldots, a^{n-1}\}$. THus $\langle a \rangle \subseteq \{e, a, \ldots, a^{n-1}\}$ and so $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$. Now let $a^i = a^j \iff a^{i-j} = e$; write $i - j = qn + r$ with $0 \leq r < n$. Then $e = a^{i-j} = a^{qn+r} = a^r$ which forces $r = 0$, by definition of n so $n|i - j$.

Conversely, $n|i - j$ then $i - j = qn$ hence $a^i = a^{j+qn} = a^j$. $\square$

Corollary 2.1.1. We have

- $|a| = |\langle a \rangle|$
- $a^k = e$ for some $k \in \mathbb{Z} \iff n = |a| \mid k$.

Remark 2.1.3.

Remark 2.1.4. The theorem says $\mathbb{Z}$ and

Example 2.1.3. Let $a \in G$ have $|a| = 30$, what is $|a^{26}|$?

Observe $\gcd(26, 30) = 2$. Hence, $a^{26} \in \langle a^2 \rangle$.

Theorem 2.1.5 — ($\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$).
Let $a \in G$, G is a group. $|a| = n$ and $k \in \mathbb{Z}_{>0}$. Letting $d = \gcd(n, k)$, we have $\langle a^k \rangle = \langle a^d \rangle$ and $|a^k| = n/d$.

Proof. Write $k = dq$.

$$a^k = (a^d)^q \quad \Rightarrow \quad a^k \in \langle a^d \rangle \quad \Rightarrow \quad \langle a^k \rangle \subseteq \langle a^d \rangle \ .$$

On the other hand, $d = sn + tk$ for some $s, t \in \mathbb{Z}$, so

$$a^d = (a^n)^s (a^k)^t = e^s (a^k)^t = (a^k)^t \in \langle a^k \rangle \quad \Rightarrow \quad \langle a^d \rangle \subseteq \langle a^k \rangle \ .$$

Therefore, $\langle a^d \rangle = \langle a^k \rangle$. Now write $n = dq'$, we want $|a^d|$. We have that

$$(a^d)^{q'} = a^{dq'} = a^n = e \ ,$$

so $|a^d| \leq q'$, But if $|a^d| < q'$, say $|a^d| = l < q'$, then $(a^d)^l = e = a^{dl}$ with $dl < dq' = n$, contradiction as $|a| = n$.

Therefore, $|a^d| = q' = n/d$. □

Example 2.1.4. Let $a \in G$ and $|a| = 30$, what is $|a^{14}|$?

gcd$(30, 14) = 2$, so $\langle 14 \rangle = \langle a^2 \rangle = \langle 26 \rangle = 15$.

Example 2.1.5. What are all the generators of $\mathbb{Z}/30$? a^j means that $j \cdot 1$ so $\langle j \rangle = G = \mathbb{Z}/30$ exactly when $j \in \{1, \}$

Corollary 2.1.2 ($|a^i| = |a^k|$). Let $n = |a| < \infty$, then

$$\langle a^i \rangle = \langle a^j \rangle \quad \iff \quad \text{gcd}(n, i) = \text{gcd}(n, j) \quad \iff \quad |a^i| = |a^j| \ .$$

Proof. INCOMPLETE □

Remark 2.1.6. In a finite cyclic subgroup, we cannot have two distinct (cyclic) subgroups of the same order.

Start of Jan 27 Wed Notes ============================

Remark 2.1.7. Question: What are all possible subgroups of $\mathbb{Z}$.

- Have cyclic subgroups: $\langle m \rangle = m\mathbb{Z}$
- More generally $\langle m, n, r \rangle = \langle \{m, n, r\} \rangle = \{km + ln + sr \,|\, k, l, r \in \mathbb{Z}\} = \langle d \rangle, d =$ gcd(m, n, r).

Therefore, these subgroups are always cyclic and we can reduce modulo on integer to see the same.

Theorem 2.1.8 — Fundamental Theorem of Cyclic Groups.
Every subgroup of a cycli group is cyclic. Further, $G = \langle a \rangle$ has order $n < \infty$ and $H \leq G$, then $|H| \,\big|\, n$, also, for all $k \in \mathbb{Z}_{>0}$ dividing n, there is a unique subgroup of G of order k, the subgroup generated by $\langle a^{n/k} \rangle$.

Proof. Let $G = \langle a \rangle \geq H$. Want H is cyclic.

If $H = \{e\}$, then we are done. Assume H is not trivial, then exists some $a \in H$, $a \neq e$.

Let $S = \{t \in \mathbb{Z}_{>0} \mid a^t \in H\}$. We claim that $S \neq \varnothing$.

Since $H \neq \{e\}$, exists $s \in \mathbb{Z} \setminus \{0\}$, $a^s \in H$, hence, if $s > 0$, $s \in S$, otherwise $s < 0$, then $a^{-s} \in H$ as H is a subgroup, hence $-s > 0 \in S$. Then, by well-ordering principle, S has a smallest element m.

Now, we want to prove that $\langle a^m \rangle = H$. Let $h \in H$ be arbitrary, so $h = a^k$ for some k, as $G = \langle a \rangle$. By division algorithm, $k = qm + r$ with $0 \leq r < m$. Then, $a^k = a^{qm}a^r$, hence, $a^r = a^{-qm}a^k \in H$. Now by definition of m, this forces $r = 0$, therefore, $a^k = a^{qm} \in \langle a^m \rangle$. Thus $H = \langle a^m \rangle$ is cyclic.

Next, let $|G| = n < \infty$. First part $H = \langle a^m \rangle$ for some $m \in \mathbb{N}$ and WLOG $m|n$ and $|H| = n/m$ by $\langle a^k \rangle$.

If $k|n$, then it's clear now that $|a^{n/k}| = k$, and so G has subgroup $\langle a^{n/k} \rangle$ of order kl by our earlier remark it is unique. □

Example 2.1.6. Let $G = \langle a \rangle$ with $|a| = 36$. What are all the generators of the subgroup of G of order 9?

First, $9|36$, so $\langle a^{36/9} \rangle = \langle a^4 \rangle$, then ${}^{4^j}$ generates $\langle a^4 \rangle \iff 1 = \gcd(9, j)$.

Example 2.1.7. What are all thes subgroups of $\mathbb{Z}/12$?

There are $\mathbb{Z}/12 = \langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 6 \rangle$, $\langle 12 \rangle = \langle 0 \rangle$.

Start of Jan 30 Mon Notes ============================

Example 2.1.8. Consider $(\mathbb{Z}/2^n)^\times$ for $n \geq 1$.

- $n = 1$, $(\mathbb{Z}/2)^\times = \{1\}$ which is cyclic
- $n = 2$, $(\mathbb{Z}/4)^\times = \{1, 3\}$ which is cyclic $\langle 3 \rangle$.
- $n \geq 3$, Claim: $(\mathbb{Z}/2^n)^\times$ is not cyclic.

  Observation: $\forall m \in \mathbb{Z}_{>0}$, $m - 1 \in (\mathbb{Z}/m)^\times$, $m - (m-1) = 1$ and $(n-1)^2 = (-1)^2 \equiv 1 \mod m$ i.e. $|m - 1| = 2$. Therefore, $(2^n - 1)^2$ must be the unique element which has order 2 by Fundamental Theorem of Cyclic Group. But $(2^{n-1} + 1) \in (\mathbb{Z}/2^n)^\times$ and

  $$(2^{n-1} + 1)^2 = 2^{n-2} + 2 \cdot 2^{n-1} + 1 = 2^n \cdot 2^{n-1} + 2^n + 1 \equiv 1 \mod 2^n .$$

  this gives at least two order 2 elements, hence $(\mathbb{Z}/2^n)^\times$ is not cyclic.

Definition 2.1.9 — Euler's totient function.

$$\varphi(n) = \begin{cases} 1 \text{ if } n = 1 \\ \text{\# of positive integers } < n \text{ and relatively prime to } n \text{ if } n \geq 2 \end{cases} .$$

Example 2.1.9. $\varphi(3) = 2$, $\varphi(10) = 4$, $\varphi(n) = |(\mathbb{Z}/n)^{\times}|$.

THEOREM 2.1.10 .
If G is a cyclic group of order n and $k|n$, then the number of elements of order k in G is $\varphi(n)$.

Proof. By FToCC, G has a unqiue subgroup of order k, say $\langle b\rangle$, then $\langle b\rangle = \langle a^j\rangle \iff \gcd(k, j) = 1$. The number of such j with $0 \leq j < k$ is $\varphi(k)$. □

Example 2.1.10.

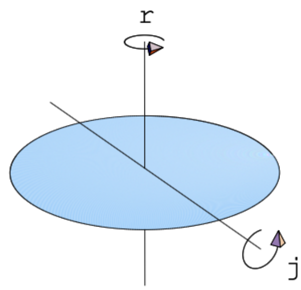
- $\varphi(p^n) = p^n = p^{n-1}$ for p prime, $n \in \mathbb{Z}_{>0}$.
- $\varphi(p_1^{n_1}, p_2^{n_2}, ..., p_m^{n_m}) = \varphi(p_1^{n_1})\varphi(p_2^{n_2})\cdots\varphi(p_m^{n_m})$ for p_i prime and $n_i \in \mathbb{Z}_{>0)}$ for all i.

2.2 Dihedral Groups

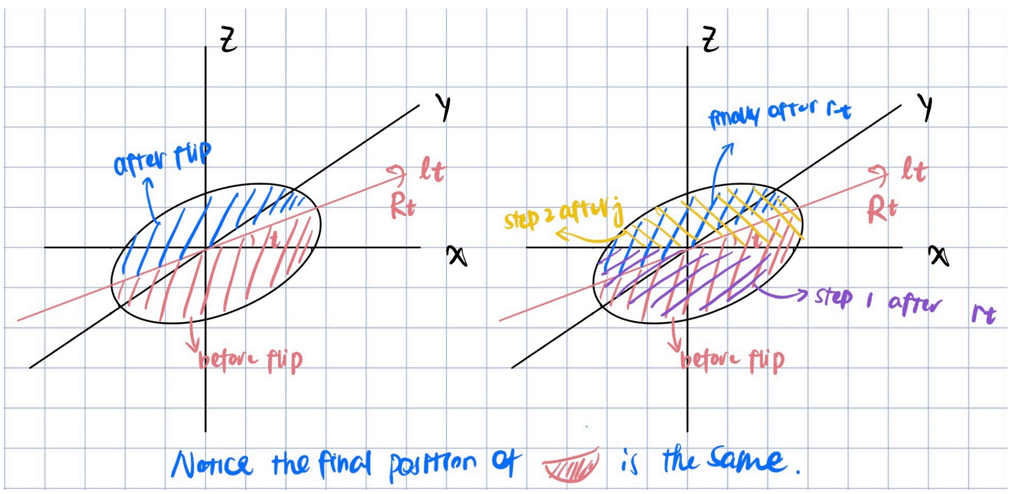
Consider the disk $\{(x, 0, 0) : x^2 + y^2 \leq 1\}$, whose symmetry group we denote by D.

Let r_t be the rotation of the disk by degree t rad around the z-axis. r_t is a symmetry of the disk. $r_s r_t = r_{t+s}$ and $r_t r_{-t} = r_0 = e$, so $H = \{r_t : t \in \mathbb{R}\}$ is a subgroup of D.

Let R_t be the flip over line $l_t = \{(x, y, 0) : y = \frac{\cos t}{\sin t} x\}$ which is line through origin and the point $(\cos t, \sin t, 0)$. Each j_t generates a subgroup of order 2 of D. Let $R = R_0$ denote the flip over x-axis.



Now, each $R_t = r_t R r_{-t}$. As illustrated below:



Now, let's turn to the symmetries of the regular polygons.

Definition 2.2.1.
A regular n-gon is a subset of $\mathbb{R}^2$ enclosed by n line segments of equal length that form equal angles.

Theorem 2.2.2 .
The symmetries of a regular n-gon are

- rotation by $\frac{2\pi k}{n}$ radians $k \in \mathbb{Z}$
- reflection across line through (centroid and vertex) or (centroid and midpoint of an edge)

Proof. EXERCISE $\square$

Definition 2.2.3.
The **dihedral group** D_n is the symmetry group of a (chosen) $n-$gon. So

$$D_n = (\{id, r_1, r_2, \cdots, r_{n-1}, R_1, R_2, ..., R_n\}, \circ)$$

where r_k= rotation by $\frac{2\pi k}{n}$ rad and R_i reflections across n-axes.

Proposition 2.2.1. Let P_n be regular n-gon with vertices $(\cos(2\pi k/n), \sin(\frac{2\pi k}{n}), 0)$ for $0 \leq k \leq n-1$, denote the symmetry group of it by D_n. Then

$$D_n = \{r^k, r^l R \,|\, 0 \leq k, l < n\}$$

where $r = r_{2\pi/n}$, $R = j_0$.

Remark 2.2.4.

- r_k = rotation by $\frac{2\pi k}{n}$ about z-axis
- R_1= rotation by π about x-axis. (flip)
- R_i= rotation by π about i-th line of reflection in xy-plane.

Lemma 2.2.1.

1. $Rr_\alpha = r_{-\alpha}R$, $j_\alpha = Rr_{2\alpha} = r_{2\alpha}R$.
2. $\langle\{r_\alpha, j_\beta\}\rangle \subseteq I_{sim}(\mathbb{R}^3)$. Then $\langle\{r_\alpha, j_\beta\}\rangle = Sym(D^2) = \{r_\alpha, r_\beta R | \alpha, \beta \in \mathbb{R}\}$.

Proposition 2.2.2. Let P_n be regular n-gon with verticies, $(\cos\frac{2\pi k}{n}, \sin\frac{2pik}{n}, 0)$ in $\mathbb{R}^3$, for $k = 0, 1, ..., n-1$, then $D_n = \{r^k, r^l R \,\big|\, 0 \leq k < n, 0 \leq l < n\}$, where $r = r_{2\pi/n}, R = j_0$.

Start of Feb 1 Wed Notes ============================

Observations: we have all rotational symmetry is cleanl $\langle r_n\rangle < D_n$ of order n.

3 Permutation Groups

3.1 Introduction - L11

Definition 3.1.1.
Let X be a set, a **permutation** of X is a bijective function $\sigma : X \to X$.

Note 3.1.2. For this course, we will focus on the case $|X| < \infty$, usually $X = \{1, 2, ..., n\}$.

Example 3.1.1. $X = \{1, 2, 3, 4\}$, $\alpha : X \to X$, $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$ and $\alpha(4) = 4$.

Array form: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, Cycle form: $\alpha = (1, 2, 3)(4)$.

Example 3.1.2. Permutations are functions, so can be composed.

For example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \quad \Rightarrow \quad \gamma\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$$

Definition 3.1.3 — Symmetric Group.
The **symmetric group** S_n(or σ_X) of degree n is the set of all permutations of $X = \{1, 2, ..., n\}$ considered as a group under composition. Its elements are $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \in S_n$.

Proposition 3.1.1 (Order of Symmetric Group S_n)**.** $|S_n| = n!$.

Example 3.1.3. $S_3 = \{\sigma : \{1, 2, 3\} \to \{1, 2, 3\} \big| \sigma \text{ is a bijection}\}$. $|S_3| = 3! = 3 \cdot 2 \cdot 1 = 6$.

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Example 3.1.4 (Cyclic Notation)**.** Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 2 & 6 & 5 & 7 \end{pmatrix} \in S_7$. We can write $\sigma = (1423)(56)(7) = (3142)(65)$. The ways you can rewrite each cycle must preserve the cyclic ordering.

Definition 3.1.4.
An m-cycle, $m \in \mathbb{Z}_{>0}$ is a sequence $(a_1, a_2, \ldots, a_m)$ of distinct integers between $1 \leq a_i \leq n$.

We want to write permutations as product of **disjoint** cycles (no elements in common).

Example 3.1.5. $\alpha = (13)(27)(456)(8)$, $\beta = (1237)(648)(5)$, then $\alpha, \beta \in S_8$. Then α, β are products of disjoint cycles.

$$\alpha\beta = (1732)(48)(56) \ .$$

Remark 3.1.5. The order we calculate composition is from RIGHT to LEFT!!!

3.2 Properties of Permutations - L12

Theorem 3.2.1 — Products of Disjoint Cycles.
Every permutation of $X = \{1, 2, ..., n\}$ is either a cycle or a product of disjoint cycles.

Proof. $n = 1$ then $\sigma = (1) = \varepsilon$.

$n = 2$, then $\sigma = (1)(2) = \varepsilon$ or $\sigma = (12)$

Let $n \geq 3$. Let $\sigma \in S_n$ and $a_1 \in X$. Let $a_2 = \sigma(a_1)$, $a_2 = \sigma(\sigma(a_1)) = \sigma^2(a_1)$, then eventually, we will arrive at some $a_1 = \sigma^m(a_1)$. This is because since X is finite, the sequence must be finite, hence there must eventually be a repetition, say $\sigma^i(a_1) = \sigma^j(a_1)$ with $i < j$. Then $a_1 = a^m(a_1)$, where $m = j - i$. Hence, we can express this relationship among $a_1, a_2, ..., a_m$ as

$$\sigma = (a_1, a_2, ..., a_m)...$$

If $X \backslash \{a_1, ..., a_m\} = \varnothing$, we are done. Otherwise, choose $b_1 \in X \backslash \{a_1, ..., a_m\}$. Then, let $b_2 = \sigma(b_1)$, $b_3 = \sigma^2(b_1)$, etc, until we have $b_1 = \sigma^k(b_1)$ for some k. Then this new cycle will have no elements in common with the previously constructed cycle because if so $\sigma^i(a_1) = \sigma^j(b_1)$ for some i and j, but then $\sigma^{i-j}(a_1) = b_1$ hence there is some t which $a_t = b_1$, this contradicts the way b_1 is chosen. Therefore, we can continue this process until there is no element left in A. And our permutation will be

$$\sigma = (a_1, a_2, ..., a_m)(b_1, .., b_k)....(c_1, ...c_?)$$

□

Theorem 3.2.2 — Disjoint Cycles Commute.
If the pair of cycles $\alpha = (a_1, ..., a_m)$, $\beta = (b_1, ..., b_r) \in S_n$ and $a_i \neq b_j$ for all i, j, then $\alpha\beta = \beta\alpha$.

Proof. Let's say that α and β are permutations of the set $S_n = \{a_1, a_2, ..., a_m, b_1, ..., b_r, c_1, ..., c_k\}$ where c are the members of S_n left fixed by both α and β, and there may not be any cs.

Choose x in S, if x is a_i for some i, then

$$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1} \ ,$$

and similarly

$$(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1} \ .$$

Therefore, $\beta\alpha$ and $\alpha\beta$ agree on a elements, and similarly on c elements. And because $\alpha\beta$ has nothing to do with c,

$$\alpha\beta(c_i) = c_i = \beta\alpha(c_i) \ .$$

This completes the proof $\square$

Example 3.2.1.

$$\begin{aligned}\alpha\beta =&(13)(27)(456)(8)\ (1237)(648)(5)\\ =&(13)(27)(1237)\ (456)(648) = (1732)\ (48)(56)\ .\end{aligned}$$

Anyway of solving this quickly?

THEOREM 3.2.3 — RUFFIM'S THEOREM.
The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles. Let $\#X < \infty$, $\sigma \in S_X$, writing σ as a product of disjoint cycles, $|\sigma| = lcm\{\text{lengths of the cycles}\}$.

Proof. Intuition: $\sigma = (1234)(678)(5)$, then $\sigma^4(a) = a$ for $a \in \{1234\}$ and $sigma^3(b) = b$ for $b \in \{678\}$. Therefore, $\sigma^{12} = \varepsilon$. $\square$

Example 3.2.2. What are al possible orders of elements of S_7?

$|S_7| = 7! = 5040$. Then

$$\begin{aligned}
&(7) && lcm(7) = 7\\
&(6)(1) && lcm(6) = 6\\
&(5)(2) && lcm(5,2) = 10\\
&(5)(1)(1) && lcm(5,1) = 5\\
&(4)(3) && lcm(4,3) = 12\\
&(4)(2)(1) && lcm(4,2) = 4\\
&(4)(1)(1)(1) && lcm(4,1) = 4\\
&\dots\\
&(3)(1)(1)(1)(1) && lcm(3,1) = 3\\
&\dots\\
&(2)(1)(1)(1)(1)(1) && lcm(2,1) = 2\\
&(1)(1)(1)(1)(1)(1)(1) && lcm(1) = 1\ .
\end{aligned}$$

Therefore, all possible orders are $\{1, 2, 3, 4, 5, 6, 7, 10, 12\}$.

And all elements of S_7 which have order 7 is all $(a_1, a_2, a_3, a_4)(b_1, b_2, b_3)$. Therefore, $(7 \cdot 6 \cdot 5 \cdot 4) \cdot (3 \cdot 2 \cdot 1) = 420$.

Note 3.2.4. If we want to count number of elements with structure $(a_1, a_2, a_3)(b_1, b_2, b_3)$ we need to divide by 2!!!!!!!

3.3 Properties of Permutations Continued - L13

Theorem 3.3.1 — Products of 2-cycles.
Every permutation in S_n, $n > 1$ is a product of 2-cycles.

Proof. Every permutation can be written in the form $(a_1 a_2 ... a_k)(b_1 b_2 ... b_t) \cdots (c_1 c_2 ... c_s)$ by Theorem. And

$$(a_1 a_2 ... a_k) = (a_1 a_2)(a_1 a_3)(a_1 a_4) ... (a_1 a_m) \ .$$

Therefore, every σ is a product of disjoint cycles. □

Example 3.3.1. $(1\ 2\ 3\ 4\ 5) = (15)(14)(13)(12) = (54)(53)(52)(51) = (54)(52)(21)(25)(23)(13)$.

is a product in many ways, and not even the number of transpositions is unique; but all products here have even numbers of transpositions.

Notation 3.3.2. For any polynomial P in variables $x_1, x_2, ..., x_n$ and $\sigma \in S_n$ denote by σP the polynomial obtained by changing x_i to $x_{\sigma(i)}$ for all $1 \leq i \leq n$.

Example 3.3.2. Let $n = 3, \sigma = (132) = (12)(13)$. Consider the polynomial $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

$$\sigma P = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = P = (12)\big((13)P\big) \ .$$

OTOH, $(12)P = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -P$.

Remark 3.3.3. We always have $\sigma = P$ or $\sigma = -P$ for any $\sigma \in S_n$.

Theorem 3.3.4 — Even vs Odd.
Let $\sigma \in S_n$, if $\sigma = \tau_1 \tau_2 ... \tau_r = \rho_1 \rho_2 ... \rho_s$ where all τ_i's and $\rho_j' s$ are transpositions, then r and s are either both even or both odd.

Proof. Let $P = (x_1 - x_2)(x_1 - x_3) \cdots (x_{n-1} - x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$. Then

$$\sigma P = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}) = \text{sign}(\sigma) P$$

, where $sgn(\sigma) = \pm 1$, this follows because σ is a bijection, so all the same linear factors appear, but they might be permuted and have sign changes. Consider any transposition $\tau = (ab)$ with $a < b$.

- τ changes the factor $x_a - x_b$ to $x_b - x_a$ (-)
- for $k < a$, τ changes $x_k - x_a \to x_k - x_b$ (+) and $x_k - x_b \to x_k - x_a$ (+).
- for $k > b$, τ changes $x_a - x_k \to x_b - x_k$ (+) and $x_k - x_a \to x_k - x_b$ (+)
- for $a < k < b$, τ changes $x_a - x_k \to x_b - x_k$ (-) and $x_k - x_b \to x_k - x_a$ (-)

Therefore, $\tau P = -P$, i.e. $\operatorname{sign}(\tau) = -1$. This implies that

$$\sigma P = \tau_1 \cdots \tau_r P = (-1)^r P = \rho_1 \cdots \rho_s P = (-1)^s P = \operatorname{sign}(\sigma) P \ .$$

Therefore, r and s are both odd or both even. $\square$

Definition 3.3.5 — Even and Odd Permutation.
A permutation σ is **even** if $\operatorname{sign}(\sigma) = 1$ and **odd** if $\operatorname{sign}(\sigma) = -1$.

Definition 3.3.6 — Alternating group.
The set A_n of all **even** permutations in S_n is a subgroup called the **alternating group of degree** n**.**

Theorem 3.3.7 .
$|A_n| = \frac{n!}{2}$, for $n > 1$.

Proof. Let $f : \{\text{even permutations}\} \to \{\text{odd permutations}\}$ which $\sigma \mapsto (12)\sigma$, then f is a bijection. Therefore, $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2} \cdot n!$. $\square$

4 Isomorphism

4.1 Homomorphism and Isomorphism - L13, L14

Definition 4.1.1 — Homomorphism & Isomorphism.
A **homomorphism** φ from a group G to a group G' is a function $\varphi : G \to G'$ s.t. for all $g, h \in G$,

$$\varphi(gh) = \varphi(g)\varphi(h) \ .$$

A **ismorphism** is a bijective homomorphism $\varphi : G \mapsto G'$.

Example 4.1.1. The map $\varphi = \det : GL_n(\mathbb{R}) \to \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ is a homomorphism because for all $A, B \in GL_n(\mathbb{R})$ have

$$\det(AB) = \det(A)\det(B) \ .$$

Therefore, det is an isomorphism iff $n = 1$.

Example 4.1.2. There is a unique homomorphism $\varphi : D_3 \to S_3$ with $\varphi(r) = (1\ 2\ 3)$ and $\varphi(R) = (2\ 3)$; in fact, φ is ismorphism.

Remark 4.1.2. If there is an isomorphism from G to G', then write $G \cong G'$ or $G \simeq G'$.

Example 4.1.3. Let $a \in G$, then there is a homomorphism $\varphi : \mathbb{Z} \to G$, $k \to a^k$. Why is it a homomorphism?

$$\varphi(k + l) = a^{k+l} = a^k a^l = \varphi(k)\varphi(l) \ .$$

Proposition 4.1.1 (5 Properties of Homomorphism)**.** Let $\varphi : G \to G'$ be a homomorphism.

1. If $\psi : G' \to G''$ is also a homomorphism, then the composition $\psi \circ \varphi : G \to G''$ is a homomorphism.
2. $\varphi(e) = e'$ where e =id of G, e'= id of G'.
3. $\varphi(g^n) = (\varphi(g))^n$ for all $n \in \mathbb{Z}$.
4. For any $H \leq G$, we have $\varphi(H) \leq G'$.
5. For any $H' \leq G'$, we have $\varphi^{-1}(H') \leq G$.

Proof.
1. $\psi \circ \varphi(gh) = \psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h)) = \psi \circ \varphi(g)\, \psi \circ \varphi(h)$.
2. $\varphi(e)\varphi(g) = \varphi(eg) = \varphi(g)$, right cancellation in G' gives $\varphi(e) = e'$.
3. - $n = 0$: follows by (2);
   - $n > 0$: $\varphi(g^n) = \varphi(gg^{n-1}) = \varphi(g)(\varphi(g))^{n-1}$ by induction
   - $n < 0$: $e' = \varphi(e) = \varphi(g^n g^{-n}) = \varphi(g^n)\varphi(g^{-n})$.

□

Definition 4.1.3 — kernel.
Let $\varphi : G' \to G'$ be a homomorphism. The **kernel** of φ is

$$\ker(\varphi) = \varphi^{-1}(\{e'\}) = \{g \in G \,|\, \varphi(g) = e'\}$$

Remark 4.1.4. By (5), $\ker(\varphi) \le G$.

Example 4.1.4. Prove that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$. Recall that $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homormorphism, so $\ker(\det) = \{A \in GL_n \,\big|\, \det(A) = 1\} = SL_n$. Must be a subgroup of the domain.

Proposition 4.1.2. A homomorphism $\varphi : G \to G'$ is injective $\iff$ $\ker(\varphi) = \{e\}$.

Proof. ($\Rightarrow$): Know $e \in \ker\varphi$, if $g \neq e$, then $\varphi(g) \neq \varphi(e) = e'$.

($\Leftarrow$): Suppose $g_1, g_2 \mapsto g'$, then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = g' g'^{-1} = e'$. Therefore, $g_1 g_2^{-1} \in \ker(\varphi) = \{e\}$, then $g_1 = g_2$. $\square$

Example 4.1.5. Consider $\pi : \mathbb{Z} \to \mathbb{Z}/n$, $k \mapsto k \mod n$, then $\ker\pi = \{k \in \mathbb{Z} \,\big|\, k \equiv 0 \mod n\} = n\mathbb{Z} \neq \{0\}$, so π is not injective.

Example 4.1.6. Let $\varphi : (\mathbb{R}, +), (\mathbb{R}_{>0}, \times), t \mapsto 2^t$, then φ is an isomorphism because it is both homomorphism and bijective. Hence, $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \times)$.

Example 4.1.7 (A3Q5). We showed $(\mathbb{Z}/98)^\times \cong \mathbb{Z}/42$, here an explicit isomorphism is $\varphi : \mathbb{Z}/42 \to (\mathbb{Z}/98)^\times$, $k \to 3^k \mod 98$.

Proposition 4.1.3. If $\varphi : G \simeq G'$ is isomporhism then so is $\varphi^{-1} : G' \simeq G$.

Remark 4.1.5. having an isomophism m means that all group-theoretic properties of G and G' are identical: orders of elements, number of elements of various orders, kinds of subgroups, etc.

Example 4.1.8. Consider the groups $\mathbb{Z}/12$, D_6, A_4, they all have order of 12.

Are those groups isomorphism to each other? NO. $\mathbb{Z}/12$ has 1 order-2 element, D_6 has $1 + 6 = 7$ order-2 elements, A_4 has 3 order 2 elements ((12)(34), (13)(24), (14),(23)).

Remark 4.1.6. Arbitrary homomorphism still preserve some structure, just not as much.

4.2 Isomorphism, automorphism, inner automorphism - L15

DEFINITION 4.2.1 — AUTOMORPHISM.
An **automorphism** is an **isomorphism** from a group to itself. For a group G, we denote all automorphism of G to be $\text{Aut}(G) = \{\varphi : G \to G \,|\, \varphi \text{ is an isomorphism}\}$.

Example 4.2.1 $((\mathbb{C}, +))$**.** Then $\mathbb{C} \to \mathbb{C}$, $a + bi \mapsto a - bi$ complex conjugation is an automorphism, which we can check

(i) codomain = domain

(ii) Is this a homomorphism with respect to $+$?

(iii) Is this injective?

(iv) Is this surjective?

THEOREM 4.2.2 .
$\text{Aut}(G)$ is a group.

Proof. Given $\varphi, \chi \in \text{Aut}(G)$, have that $\varphi \circ \chi : G \to G$ is a homomorphism by properties of homomorphisms(1), and it is not hard to show that $\varphi \circ \chi$ is a bijection.

And you can check the associativity, identity and inverses properties of a group holds. □

Remark 4.2.3. $\text{Aut}(G)$ is a group but it can be difficult to describe for some groups. Forturnately, there are always some automophism we can describe.

DEFINITION 4.2.4 — INNER AUTOMORPHISM INDUCED BY ELEMENT.
Let G be a group, $a \in G$, the **inner automorphism of** G **induced by** a is the map

$$\varphi_a : G \to G, \quad g \mapsto aga^{-1} \ .$$

Note: the a^{-1} is on the right.

Notation 4.2.5. We denote all inner automorphism of G to be $\text{Inn}(G) = \{\varphi \in \text{Aut}(G) \,|\, \varphi = \varphi_a \text{ for some } a \in G\}$.

Example 4.2.2. Inner automorphisms can be useful for finding "other copies" of a given $H \leq G$. $\varphi_a(H) \leq G$, in fact, $H \cong \varphi_a(H) = aHa^{-1}$.

Given $G = S_4 > H = \{(1234), (13)(24), (1432), (12)(34), (24), (14)(23), (13)\}$,

Notation 4.2.6. G is a group, $\text{Inn}(G) = \{\varphi \in \text{Aut}(G) \,|\, \varphi \text{ is inner automorphism}, i.e. \varphi = \varphi_a, \text{ for some } a \in G\}$.

Theorem 4.2.7 .
For any group G, $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Proof. Define a map $\Phi : G \to \mathrm{Aut}(G)$, $a \to \varphi_a$.

Let $a, b \in G$, $\Phi(ab) = \varphi_{ab}$ is the homomophism $G \to G$ s.t. $\varphi_{ab}(g) = (ab)g(ab)^{-1} = abgb^{-1}a^{-1} = \varphi_a(bgb^{-1}) = \varphi_a\varphi_b(g) = \varphi_a\varphi_b(g)$, for all $g \in G$. Therefore, $\Phi(ab) = \Phi(a)\Phi(b)$. Then Φ is a homomorphism and the image of Φ is exactly $\mathrm{Inn}(G)$ and $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ by Property (4). □

Definition 4.2.8.
The **centre** of a group G is $Z(G) = \ker \Phi \leq G$ (The image of Φ was $\mathrm{Inn}(G)$).

Remark 4.2.9. $a \in Z(G) \iff a \in \ker \Phi \iff \Phi(G) = (id : G \to G) \iff \varphi_a = id \iff \forall g \in G, aga^{-1} = g \iff \forall g \in G, ag = ga.$

So an eleemnt a belongs to the centre of G iff a commutes with every element of G.

Theorem 4.2.10 .
$\mathrm{Aut}(\mathbb{Z}/n) \cong (\mathbb{Z}/n)^\times$.

Proof. Define a map $\zeta : \mathrm{Aut}(\mathbb{Z}/n) \to (\mathbb{Z}/n)^\times$, which for $\alpha \in \mathrm{Aut}(\mathbb{Z}/n)$, $\zeta(\alpha) = \alpha(1)$.

Then $\alpha(1) \in (\mathbb{Z}/n)^\times$ because 1 generates $\mathbb{Z}/n$ and so $\alpha(1)$ must also generate $\mathbb{Z}/n$ as $\alpha : \mathbb{Z}/n \to \mathbb{Z}/n$ is an automorphism.

Is ζ an isomorphism?

- Homomorphism: let $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}/n)$,

$$\zeta(\alpha\beta) = (\alpha\beta)(1) = (\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1)\text{ times}}) = \alpha(1)\beta(1) = \zeta(\alpha)\zeta(\beta)\ .$$

- Bijective: exercise

□

Example 4.2.3. $\mathrm{Aut}(\mathbb{Z}/10) \cong (\mathbb{Z}/10)^\times = \{1, 3, 7, 9\}$, so $\mathrm{Aut}(\mathbb{Z}/10)$ has four elements, call them $\alpha_1, \alpha_3, \alpha_7, \alpha_9$, where $\alpha_i(1) = i$.

How to multiply these? Composition $\alpha_1\alpha_3 =?$

$$(\alpha_1\alpha_3)(1) = \alpha_1(1)\alpha_3(1) = 3\ .$$

Therefore $\alpha_1\alpha_3 = \alpha_3$. In fact, α_1 is the identity automorphism on $\mathbb{Z}/10$.

We can work out the entire multiplication table of $\mathrm{Aut}(\mathbb{Z}/10)$ in the same way, it is identitcal to that of $(\mathbb{Z}/10)^\times$.

THEOREM 4.2.11 — CAYLEY'S THEOREM.
Every group is isomorphic to a permutation group.

Proof. Let G be a group, we need a set to permute. Let $X = G$ be the underlying set. For each $g \in G$, define $\sigma_g : X \to X$, where $\sigma_g(x) = gx$.

Is $\sigma_g \in S_X$, i.e. is σ_g a permutation?

σ_g is injective:

σ_g is surjective: □

THEOREM 4.2.12 .

1. $\mathbb{Z}/1 = \{0\}$ is the unique group of order 1, up to isomorphism.
2. $\mathbb{Z}/2$ is the unique group of order 2, up to isomorphism.
3. $\mathbb{Z}/3$ is the unique group of order 3, up to isomorphism.
4. $\mathbb{Z}/4$, $K_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$(the klein 4 group) the only groups of order 4 up to isomorphism .
5. ... can continue ... $n = 5, group\# : 1$, $n = 6, group\# : 2$, $n = 7 \to 1$, $n = 8 \to 5$, $n = 9 \to 2$.

Idea of Proof. Try to write a Cayley table, e.g. order 4, □

5 Cosets

5.1 Cosets - L17

Our first goal will be to understand an extremely important result on finite groups.

Theorem 5.1.1 — Lagrange's THeorem.
If G is a finite group, and $H \leq G$, then $|H|\big||G|$. Further H has $|G|/|H|$ diestinct left cosets in G.

Definition 5.1.2.
Let G be a group and $H \subseteq G$ a subset. For $a \in G$, denote $aH = \{ah \big| h \in H\}$; $Ha = \{ha \big| h \in H\}$, write $|aH| = \#aH$, and $|Ha| = \#Ha$.

When $H \leq G$, aH is the **left coset of** H **in** G **containing** a and Ha is the **right coset of** H **in** G **containing** a. The element a is a **coset representation** of aH or Ha.

Example 5.1.1. Let $H = \{\varepsilon, (12)\} \leq S_3$, the left cosets of H are

- $H = \varepsilon H = (12)H = \{(12)\varepsilon, (12)(12)\}$
- $(13)H = (123)H = \{(13), (123)\}$

Proposition 5.1.1 (Properties of Cosets)**.** Let $H \leq G$ be groups, $a, b \in G$,

0) $a \in aH$
1) $(ab)H = a(bH)$ and $H(ab) = (H)ab$
2) $aH = bH \iff a \in bH \iff b^{-1}a \in H \iff b \in aH \iff a^{-1}b \in H$
3) Either $aH = bH$ or $aH \cup bH = \varnothing$
4) $|aH| = |bH|$
5) $aH = Ha \iff aHa^{-1} = H$
6) $aH \leq G \iff a \in H$

Proof. 0) $a = ae$ where $e \in H$

1) trivial by associativity
2) If $aH = bH$, for any $h \in H$, exists $g \in H$ which $ah = bg$, then $a = bgh^{-1}$. Therefore, $a \in bH$ as $gh^{-1} \in H$.
3) If $aH \cup bH \neq \varnothing$, then $\exists c \in aH \cup bH$, then by (2), $aH = cH = bH$.
4) $aH = Ha \iff (aH)a^{-1} = Haa^{-1} \iff aHa^{-1} = H$.
5) $aH \leq G \iff e \in aH \Rightarrow a^{-1} \in H \Rightarrow a \in H$. Conversely, $a \in H \Rightarrow aH = H \leq G$.

□

Example 5.1.2. For $H = \{\varepsilon, (1, 2)\} \leq S_3$, note $(1\ 3)H \neq H(1\ 3)$.

5.2 Lagrange's Theorem

Theorem 5.2.1 .
If G is a finite group, $H \leq G$, then $|H|\big||G|$, further, H has $|G|/|H|$ distinct left cosets in G.

Proof. Let $a_1H, a_2H, \ldots, a_rH$ be the distinct left cosets of H in G. Then $\forall a \in G$, have $a \in aH = a_iH$ for some $i \in \{1, 2, ..., r\}$. $\Rightarrow G = a_1H \cup a_2H \cup \cdots \cup a_rH = \bigcup_{i=1}^{r} a_iH$.

But these cosets are pairwise disjoint (3), i.e. $G = \bigcup a_iH$, and this implies $|G| = \sum_i |a_iH| = r|H|$. Hence, $r = |G|/|H|$. □

Example 5.2.1. For $H = \{\varepsilon, (1\ 2)\} \leq S_3$, we have $|H| = 2|6 = |S_3|$, and H has $6/2 = 3$ left cosets: $H, (1\ 3)H, (2\ 3)H$.

Example 5.2.2. In L_9, we claimed without proof that $\langle 3 \rangle = (\mathbb{Z}/50)^{\times}$. To prove this, recall that $|(\mathbb{Z}/50)^{\times}| = \varphi(50) = \varphi(2 \cdot 5^2) = 20$. Lagrange's Theorem $\Rightarrow |3| \in \{2, 4, 5, 10, 20\}$. Now calculate 3^k can get $\langle 3 \rangle = (\mathbb{Z}/50)^{\times}$.

Remark 5.2.2. Lagrange's Theorem allows/prohibits certain orders for subgroups, but it does not imply there is a subgroup of order k for each $k\big||G|$. In fact, this is false: $|A_4| = 12$ but A_4 has no subgroup of order 6.

Definition 5.2.3.
For $H \leq G$ a group, the **index of H in G** is the number of distinct left(or right) cosets of H in G, denoted $[G : H]$.

Corollary 5.2.1. $[G : H] = |G|/|H|$, if $|G| < \infty$ and $H \leq G$.

Corollary 5.2.2. $|a|\big||G|$ if $|G| < \infty$ and $a \in G$.

Corollary 5.2.3. If $|G| = p$ prime, then $G \cong \mathbb{Z}/p$.

Proof. Pick any $a \in G \setminus \{e\}$. Then $\langle a \rangle \leq G$ is a subgroup of order > 1; but $|a|\big||G| \Rightarrow |a| = p$, i.e. $G = \langle a \rangle$. □

Corollary 5.2.4 ($a^{|G|} = e$)**.** If $|G| < \infty$ and $a \in G$, then $a^{|G|} = e$.

Proof. $|a|\big||G|$. $\square$

Theorem 5.2.4 .
For all $a \in \mathbb{Z}$ and p prime, we have $a^p \equiv a \mod p$.

Proof. If $p|a$, then $a^p \equiv 0^p \equiv 0 \equiv a \mod p$.

If $p \not| a$, then $a = qp + r$ for $0 < r < p$. Then $r \in (\mathbb{Z}/p)^\times = F$ and so $r^{|G|} = r^{p-1} \equiv 1 \mod p$. That is $a^p = aa^{p-1} = \equiv rr^{p-1} \equiv r \cdot 1 \equiv a \mod p$. $\square$

Theorem 5.2.5 .
For subgroups H, K of some group, let $HK := \{hk\big|h \in H, k \in K\}$. Suppose $|H|, |K| < \infty$. Then $|HK| = |H|\,|K|/|H \cup K|$.

Proof. Each pair $(h, k) \in H \times K$ determines a product $hk \in HK$. When is $hk = h'k'$? How to count when this happens?

Observer: there is an equivalence relation on $H \times K$ defined by $(h, k) \sim (h', k') \iff hk = h'k'$.

The equivalence relation partitions $H \times K$ into a disjoint union of equivalent classes

$$[(h, k)] = \{(h', k')\big|(h', k') \sim (h, k)\}.$$

Let's see how many elements are in each class. Claim: $hk = h;k; \iff h' = hg$ and $k' = g^{-1}k$ for some $g \in G \cap K$. Proof for Claim: exercise.

In other words, each equivalence class has $|H \cap K|$ elements. $|H \times K| = |HK||H \cap K|$. $\square$

Example 5.2.3. Suppose G is a group of order 75, then one can show that G must have a subgroup of order 25.

Suppose $H, K < G$ of order 25, $H \cap K \leq H, K \Rightarrow |H \cap K|$

5.3 Normal Subgroup - L19

Definition 5.3.1.
If $H \leq G$, G is a group, then H is **normal**, if for all $g \in G$, $gH = Hg$. Denoted $H \lhd G(H \trianglelefteq G)$.

Remark 5.3.2. Normal subgroups are an important class of subgroups. Elements of $H \lhd G$ almost commute with any $g \in G$, given $h \in H$, $g \in G$, you can find $h', h'' \in H$ such that $gh = gh'$ and $gh = h''g$.

Remark 5.3.3. Any subgroup of an abelian group is normal.

Remark 5.3.4. $Z(G) \trianglelefteq G$ because for every $z \in Z(G)$ and all $g \in G$ $zg = gz \Rightarrow gZ(G) = Z(G)g$.

Remark 5.3.5. The alternating group $A_n \trianglelefteq S_n$.

Theorem 5.3.6 — Normal Subgroup Test.
Let G be a subgroup then $H \trianglelefteq G \iff$ for all $g \in G$, $gHg^{-1} \subseteq H$.

Proof. $(\Leftarrow)$: We saw in A2Q5b that $gHg^{-1} \subseteq H$ for all $g \in G$ implies $gHg^{-1} = H$ for all $g \in G$. Therefore, then property of cosets (5) shows that $gH = Hg$ for all $g \in G$. Thus $H \trianglelefteq G$.

$(\Rightarrow)$: Property of cosets $(5) \Rightarrow gHg^{-1} = H \forall g \in G \Rightarrow gHg^{-1} \subseteq H \forall g \in G$. $\square$

Example 5.3.1. Suppose G has a unique subgroup H of some particular finite order. Then $H \trianglelefteq G$. Note $gHg^{-1} = \varphi_g(H) \leq G$. To see this, let $g \in G$, consider the inner automorphism $\varphi_g : G \cong G$, $b \to gbg^{-1}$. Then $\varphi_g(H) \leq G$ is isomorphic to H, so $|\varphi_g(H)| = |H|$. Therefore, $gHg^{-1} = \varphi - g(H) = H$ for any $g \in G$. Therefore, $H \trianglelefteq G$.

Proposition 5.3.1. Let $\varphi : G \to H$ be a homomorphism then $\ker \varphi \trianglelefteq G$.

Proof. Normal subgroup test, $g(\ker \varphi)g^{-1} \subseteq \ker \varphi$ for all $g \in G$. Let $h \in \ker \varphi$, $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1})$.. $\square$

Example 5.3.2. Consider the map $sgn : S_n \to \{\pm 1\}$. Ex. sgn is a homomorphism. The ker $sgn = \{\sigma \in S_n \,|sgn(a_n) = 1\} = A_n$. Therefore, $A_n \lhd S_n$.

Example 5.3.3. Let $H = \{\varepsilon, (12)\} < S_3$. Then $(13)H \neq H(13)$ as you can verify. Therefore, H is not a normal subgroup.

Proposition 5.3.2. Let $H \trianglelefteq G$ and $K \leq G$, then $HK \leq G$.

Proof. Subgroup Test. $HK \neq \varnothing$ as $ee \in HK$.

HK closed under multiplication: Let $hk, h'k' \in HK$. Then H is normal so $kH = Hk \Rightarrow \exists h'' \in H$ s.t. $kh' = h''k$. Then

$$(hk)(h'k') = h(kh')k' = h(h''k)k' = (hh'')(kk') \in HK \ .$$

HK is closed under inverses $(hk)^{-1} \in k^{-1}h^{-1} \in k^{-1}H = Hk^{-1} \subseteq HK$. $\square$

6 Quotient (Factor) Group - L20

Theorem 6.0.1 .
Let G be a group and let H be a normal subgroup of G, the set $G/H = \{aH | a \in G\}$ is a group under the operation $(aH)(bH) = abH$

Theorem 6.0.2 .
Let G be a group, and $N \trianglelefteq G$ be a normal subgroup. The set $G/N := \{gN | g \in G\}$ (G mod N) has a unique product that makes G/N into a group and makes the **quotient map** $\pi : G \to G/N$, $g \mapsto gN$ into a group homomorphism.

Proof. We want to define $(aN)(bN) := (ab)N$. This is well defined as N is a normal subgroup.

Now to show G/N is a group,

- Identity: $\varepsilon N = N$ is the identity as for all $N(aN) = (\varepsilon aN) = aN$.
- Associativity:

$$\begin{aligned}\big((aN)(bN)\big)(cN) =&(abN)(cN) = (abc)N \\ =&(a(bc))N = (aN)(bcN) = (aN)((bN)(cN))\end{aligned}$$

- Inverse: $(aN)(a^{-1}N) = (aa^{-1})N = N$.

Therefore, G/N is a group. Now for π is homomorphism, for $a, b \in G$, $\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b)$. Finally π being a homomorphism forces $(aN)(bN) = abN$. $\square$

Example 6.0.1. $\langle n \rangle = n\mathbb{Z} \trianglelefteq \mathbb{Z}$ as $\mathbb{Z}$ is abelian.

Remark 6.0.3. In G/N, all elements of N collapse together to become the identity.

Remark 6.0.4. For G/H, H must be a normal subgroup.

Example 6.0.2. Consider $N = \mathbb{Z} \triangleleft G = \mathbb{R}$.

Properties of Cosets: $r + \mathbb{Z} = s + \mathbb{Z} \iff \mathbb{Z} = -r + s + \mathbb{Z} \iff s - r \in \mathbb{Z}$. Therefore, we can uniquely represent any coset as $r + \mathbb{Z}$ where $0 \leq r < 1$.

Geometric Idea: $\mathbb{R}/\mathbb{Z} \mapsto U = \{\mathbb{Z} \in \mathbb{C} \big| |z| = 1\} = \{e^{i\theta} \big| 0 \leq \theta < 2\pi\}$.

Then $r + \mathbb{Z} \to e^{2\pi i r}$.

Example 6.0.3. Let G be a finite group and suppose some quotient G/N contains an order m element say aN. Let $k = |a| \Rightarrow (aN)^k = a^k N = eN = N \Rightarrow m|k$, say $k = qm$. Then a^q must have order m, i.e. G also contains an order m element.

THEOREM 6.0.5 — CAUCHY'S THEOREM (ABELIAN CASE).
Let G be a finite abelian group and suppose $p\big||G|$, p prime, then G contains an order p element.

Proof. Strong induction. Base case $|G| = 2$, $G \cong \mathbb{Z}/2$ and $|1| = 2$.

Now suppose the theorem holds for all groups of order less than $|G|$.

let $x \in G$, $|x| = m$, if m is not prime, then write $m = qn$ with q prime, so $|x^n| = q$ has prime order. Thus, we can find an element of G of some prime order: say $y \in G$, $|y| = q$ prime.

If $q = p$, then done. Otherwise, $q \neq p$ and we form the quotient $G/\langle y\rangle$(G is abelian so $\langle y\rangle$ is normal) of order $|G|/q$, which is less than $|G|$ and still divisible by p. Then by induction, $G/\langle y\rangle$ has an order p element, then so does G. $\square$

Remark 6.0.6.
- $N = \mathbb{Z} \lhd G = \mathbb{R}$
- $R/\mathbb{Z} \cong U = \{e^{i\theta}\big|0 \leq \theta < 2\pi\}, t = e^{2\pi it}$.
- $\mathbb{R} \to U, t \to e^{2\pi it}$

THEOREM 6.0.7 — FIRST ISOMORPHISM THEOREM.
Let $\varphi : G \to H$ be a surjective homomorphism and $N = \ker\varphi$. Then there is an isomorphism $\bar{\varphi} : G/N \to H$ s.t. $\bar{\varphi} \circ \pi = \varphi$, where π is the quotient map. i.e. the diagram $\ker\varphi = N \subset G$ commutes.

Proof. To get $\varphi = \bar{\varphi}\pi$, we need $\bar{\varphi}(gN) := \varphi(g)$. But is this well-defined?

$$\begin{aligned} gN = aN \iff g^{-1}aN = N &\iff g^{-1}a \in N = \ker\varphi \\ &\iff \varphi(g^{-1}a) = e_H \\ &\iff \varphi(g^{-1})\varphi(a) = e_H \iff \varphi(a) = \varphi(g)\ . \end{aligned}$$

Therefore, $\bar{\varphi}$ is well defined. Now

- $\bar{\varphi}$ is a homomorphism: $\bar{\varphi}(aNbN) = \bar{\varphi}(abN) = ab = \bar{\varphi}(aN)\bar{\varphi}(bN)$.
- $\bar{\varphi}$ is surjective: for $h \in H$, $\exists g \in G$ with $\bar{\varphi}(gN) = \varphi(g) = h$.
- $\bar{\varphi}$ is injective: $\bar{\varphi}(aN) = e_H \iff \varphi(a) = e_H \iff a \in N \iff aN = N$.

$\square$

Remark 6.0.8. Given any homomorphism $\varphi : G \to G'$, we have $G/\ker\varphi \cong \sqsupset\!\!>\!\varphi$.

Remark 6.0.9. This is often applied to non-surjective homomorphism, i.e. let $\varphi : G \to G'$ arbitrary homomorphisml then setting $H = \varphi = \varphi(G) < G'$, we get a surjective homomorphism $\varphi : G \to H$.

Begin of Lec 22

Corollary 6.0.1. If $\varphi : G \to H$ is a homomorphism and $|G| < \infty$, then $|G|/|\ker\varphi| = |\operatorname{img}\varphi|$; in fact, $|\operatorname{img}\varphi|$ divides $|G|$ and $|H|$.

Proof. First, we have an isomorphism $G/\ker\varphi \cong \operatorname{img}\varphi$, now, $\operatorname{img}\varphi \le H$, then $|\operatorname{img}\varphi|\big||H|$. Also, $G/\ker\varphi|\big||G|$, $\square$

Theorem 6.0.10 — G/Z.
If G is non-abelian group, then $G/Z(G)$ is not cyclic.

Proof. We will prove the contrapositive. If $G/Z(G)$ is cyclic that $G/Z(G) = \langle gZ(G)\rangle$. Let $a \in G$, $\exists i$ s.t. $aZ(G) = (gZ(G))^i = g^iZ(G)$. Therefore, $a = g^iz$ for some $z \in Z(G)$. But then g commutes with a, for any $a \in G$, therefore $g \in Z(G)$. Hence $G/Z(G) = \{Z(G)\}$, i.e. $G = Z(G)$, i.e. G is abelian. $\square$

7 Group Actions

7.1 L23

Definition 7.1.1 — Action.
An **action** of group G acting on a set X, written $G \circlearrowleft X$ is a homomophism $G \to \mathrm{Sym}X$.

- i.e. $\forall g_1, g_2 \in G$, $\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2)$.
- i.e. $\forall g_1, g_2 \in G, \forall x \in X$, $(\alpha(g_1 g_2))(x) = \alpha(g_1)((\alpha(g_2))(x))$.

This is often written suppressing α as $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

Remark 7.1.2. Let φ be an action of G on X. Each $g \in G$ corresponds to a bijection $\varphi(g)$ of X.

Definition 7.1.3 — Normalizer.
Let $H \leq G$ a group, the **normalizer** of H in G is

$$N(H) := \{g \in G \big| gH = Hg\} = \{g \in G \big| gHg^{-1} = H\} \ ,$$

$H \leq N(H) \leq G$.

Example 7.1.1. Recall $\Phi : G \to \mathrm{Aut}(G)$, $g \mapsto \varphi_g$. Let $x \in N(H)$. Then $\forall h \in H$, get $\varphi_x(h) = xhx^{-1} \in xHx^{-1} = H \Rightarrow \varphi_x \in \mathrm{Aut}(H)$.

So we get a homomorphism $\Phi|_{N(H)} : N(H) \to \mathrm{Aut}(H)$, $x \to \varphi_x$. What is its kernel?

$$\begin{aligned} x \in \ker \Phi|_{N(H)} &\iff \varphi_x = id_H \\ &\iff \forall h \in H, xhx^{-1} = h \\ &\iff \forall h \in H, xh = hx \\ &\iff \forall h \in H, x \in C(h) \leftarrow \text{centralizerofh} \\ &\iff x \in C(H) := \{y \in G | yhy^{-1} = h, \forall h \in H\} \end{aligned}$$

which is called the centralizer of H in G.

Hence the first isomorphism theorem, $N(H)/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Example 7.1.2. Take $\alpha : D_n \to S_X$, where X is the regular $n-$gon to be the inclusion map (i.e. every symmetry of X is a bijection of X). Then $D_n \circlearrowleft X$ is the obvious geometric action of these symmetries on the points of X.

Definition 7.1.4 — Orbit.
Given an action of G on X, there is an **equivalence relation on** X defined by $x \sim y \iff \exists g \in G, g \cdot x = y$.

The **orbit** of $x \in X$ is the equivalence class of x, denoted $O(x) = \mathrm{Orb}(x) = \mathrm{Orb}_G(x) = G \cdot x$.

$$\mathrm{Orb}(x) = \{y \in X \,|\, \exists g \in G, g \cdot x = y\} \ .$$

Example 7.1.3. Any group G acts on itself by left multiplication, that is, for $g \in G$ and $x \in G$, $g \circ x = gx$.

Definition 7.1.5 — Stabilizer.
Let $G \circlearrowright X$, the **stabilizer** of $x \in X$ is the set

$$\text{Stab}(x) := \{g \in G \,|\, g \cdot x = x\} = \text{Stab}_G(x) = G_x \ .$$

Lemma 7.1.1 (Stabilizer is a subgroup)**.** If $G \circlearrowright X$ and $x \in X$, then $\text{Stab}(x) \leq G$.

Proof. For all $g, h \in \text{Stab}(x)$, since $h \in \text{Stab}(x)$, then $\alpha(h^{-1}h) = e \in SymX$. Then for all $x \in X$, $h^{-1}h \circ x = h^{-1} \circ x = x$. Therefore, $h^{-1} \in \text{Stab}(x)$. Now, for all gh^{-1},

$$gh^{-1} \circ x = g \circ (h^{-1} \circ x) = g \circ x = x \ .$$

Therefore, $gh^{-1} \in \text{Stab}(x)$, hence by One-Step Subgroup Test, $\text{Stab}(x) \leq G$. $\square$

Definition 7.1.6 — Transitive.
An action $G \circlearrowright X$ is **transitive** if it has only one orbit. That is, for any two elements $x, x' \in X$, there is a $g \in G$ such that $gx = x'$. A subgroup of $\text{Sym}(X)$ is transitive if it acts transitively on X.

Example 7.1.4. $D_3 = \text{Sym}(X) \to S_X$ where X=equilateral triangle. Let $x \in X$ be a vertex. $\text{Orb}(x) = \{$ vertices of $X\}$. Also $\text{Stab}(x) = \{id, R\}$ where R is reflection through x and the centroid.

Example 7.1.5. Let X=regular tetrahedron. Define an action of A_4 on X as follows $\alpha : A_4 \to Sym(X) \to S_X$ given by

- for each $\sigma \in A_4$, then exists a unique symmetry of X that realizes the premutation σ on vetices

7.2 L24

Last Time: groups actions

- Group actions: each $g \in G$ a group, acts on a set X as a permutation of X.
- tend to say action in two ways: the action = the G action on X, what anything in G does to anything in X.
- the action of g

Example 7.2.1. Let $H \leq G$, then G acts transitively on the set G/H of left cosets of H in G via the action $g \circ (aH) := (ga)H$. (Often drop the "$\circ$": $g(aH) = (ga)H = gaH$)

Example 7.2.2. The homomorphism $\Phi : G \to \text{Aut}(G) \subseteq S_G$ where $\Phi(a) = \varphi_a$ determines the conjugation action of G on itself.

$$\begin{aligned} y \in \text{Orb}(x) &\iff \exists g \in G, g \circ x = y, \varphi_g(x) = y \\ &\iff \exists g \in G, gxg^{-1} = y \\ &\iff y \text{ is a conjugate of } x \end{aligned}$$

So the orbits of the conjugation action are **conjugacy classes**.

$\text{Stab}(x) = \{g \in G \big| g \circ x = x\} = \{g \in G \big| gxg^{-1} = x\} = C(x)$,

Example 7.2.3. Let $X = \{H \big| H \leq G\}$, the set of all subgroups of G.

Then Φ induces an action $G \circlearrowright X$ via

$$g \circ H = gHg^{-1} = \varphi_g(H) \in X \ .$$

Then we have

$$\begin{aligned} \text{Orb}(H) =& \{\text{conjugates of } H\} \\ \text{Stab}(H) =& \{g \in G \big| gHg^{-1} = H\} = N(H) \end{aligned}$$

Theorem 7.2.1 — Orbit-Stabilizer.
Let G be a group, X a set, $G \circlearrowright X$, $x \in X$, then there is a bijection which $\psi : G/\text{Stab}(x) \to \text{Orb}(x)$, $a\text{Stab}(x) \mapsto a \cdot x$ which satisfies $\psi(g(a\text{Stab}(x)))) = g\dot{\psi}(a\text{Stab}(x)$.

Proof. Is ψ well-defined?

$$\begin{aligned} a\text{Stab}(x) = b\text{Stab}(x) &\iff \text{Stab}(x) = a^{-1}b\text{Stab}(x) \\ &\iff a^{-1}b \in \text{Stab}(x) \\ &\iff (a^{-1}b) \cdot x = x \\ &\iff a^{-1} \cdot (b \cdot x) = x \\ &\iff a \cdot (a^{-1} \cdot (b \cdot x)) = a \cdot x \\ &\iff (aa^{-1}) \cdot (b \cdot x) = a \cdot x \\ &\iff b = a \ . \end{aligned}$$

Therefore, ψ is well-defined.

Injectivity: $\psi(a\text{Stab}(x)) = \psi(b\text{Stab}(x)) \iff a \cdot x = b \cdot x = a\text{Stab}(x) = b\text{Stab}(x)$.

Surjectivity: Given $g \in \text{Orb}(x) \iff \exists g \in G, g \cdot x = y$.

The final claim follows from $(ga) \cdot x = g \cdot (a \cdot x)$. $\square$

7.3 L25

Example 7.3.1. $D_3 \circlearrowleft \triangle \Rightarrow D_3 \circlearrowleft \{\text{vertices of } \triangle\} = \text{Orb}(vertex)$.

Corollary 7.3.1 (Counting Theorem)**.** If G is a finite group acting on a set X, then

$$|G| = |\text{Orb}(x)|\,|\text{Stab}(x)|$$

for all $x \in X$. In particular, $|\text{Orb}(x)| = [G : \text{Stab}(x)] \,\big|\, |G|$.

Proof. The Orbit-Stabilizer Theorem $\Rightarrow |\text{Orb}(x)| = |G/\text{Stab}(x)| = \frac{|G|}{\text{Stab}(x)}$ by Lagrange. □

Remark 7.3.1. This is like Lagrange's Theorem but for group actions, orbits and stabilizers.

Example 7.3.2. Let $G = D_3 \circlearrowleft Y = \{1, 2\}$, where r acts as the identity, R acts as $(1\ 2) \in S_y = S_2$. Then, $\text{Orb}(1) = \{1, 2\}$, and $\text{Stab}(1) = \{id, r, r^2, r^3\}$. Then $|\text{Orb}(1)|\,|\text{Stab}(1)| = 2 \times 4 = 8 = |D_4|$.

Example 7.3.3. Recall the action of A_4 on X=regular tetradefron, where each permutation was realized as a rotational symmetry.

$|\text{Orb}(1)| = 4$, $\text{Stab}(1)| = 3$; $|A_4| = \frac{4!}{2} = \frac{24}{2} = 12$, for 1 a vertex of X.

$|\text{Orb}(x)| = 12$, $|\text{Stab}(x)| = 1$, for random $x \in X$ inside a facet of X.

$|\text{Orb}(m)| = 6$, $|\text{Stab}(m)| = 2$, for m the midpoint of an edge.

$|\text{Orb}(c)| = 4$, $|\text{Stab}(x)| = 3$ for c the centroid of a face.

Example 7.3.4. What is the order of the group G of all rotational symmetries of the cube?

Let $X = \{1, 2, ..., 6\}$ where we think of each number as labelling a face. $\text{Orb}(1) = \{1, 2, ..., 6\} = X$ and $\text{Stab}(10 = \{id, r, r^2, r^3\}$ where r is rotational by $\frac{\pi}{2}$ about vertical axis.

In face, $G \cong S_4$, where we think of $1, 2, 3, 4$ as corresponding to the four diagonals of the cube.

Example 7.3.5. Let $|G| < \infty$, how many conjugates does a chosen $g \in G$ have?

Know $G \circlearrowleft X = G$ by conjugation$\Rightarrow \text{Orb}(g) = \{conjugatesofg\}$ The number of conjugates of g is $|\text{Orb}(g)| = [G : C(g)] = \frac{|G|}{|C(g)|}$.

For instance, $g = (1\ 2\ 3) \in S_3$.

7.4 Applications to Counting - L26

Example 7.4.1. Let $\binom{n}{k}$ denote the \$ of k-element subsets of $\{1, 2, ..., n\}$. THen

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \ .$$

To see this, let $X = \{Y \big| Y \subseteq X, \#Y = k\}$. Then there is a transitive action of S_n on X via

$$\sigma \cdot \{a_1, a_2, ..., a_k\} := \{\sigma(a_1), \sigma(a_2), ..., \sigma(a_k)\} \ .$$

Example 7.4.2. How many distinct arrangements are there of the letters in "MISSISSIPPI"?

4S, 4I, 2P, 1M = 11 letters. Then $S_{11} \circlearrowright X = \{$ rearrangements of MISSISSIPPI$\}$ acts transitively by sending the letter in the i-th position to the $\sigma(i)$-th position.

Let $x = MPPIIIISSSS \in X$. Like last example, let Stab$(x) \cong S_1 \times S_2 \times S_4 \times S_4$.

THerefore, by Counting Theorem,

$$|\text{Orb}(x)| = \frac{|S_{11}|}{|S_1 \times S_2 \times S_4 \times S_4|} = \frac{11!}{1!2!4!4!} = 34650 \ .$$

Definition 7.4.1 — Fixed point.
Let $G \circlearrowright X$, for any $g \in G$, the **fixed-point** set of g is

$$\text{Fix}(g) = \{x \in S \big| g \circ x = x\} = X^g \ .$$

Lemma 7.4.1 (Burnside's Lemma)**.** Let G be a finite group acting on a finite set X. The # of orbits of $G \circlearrowright X$ equals

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| \ .$$

Proof. Idea: To count elements of $F := \{(g, x) \in G \times X, g \circ x = x\}$ in two ways.

First way:

$$\sum_{g \in G} (\text{\# of } x \in X \text{ fixed by } g) = \sum_{g \in G} |\text{Fix}(g)|$$

Second way:

$$\sum_{x \in G} (\text{\# of } g \in G \text{ that stabilizes } x) = \sum_{x \in X} |\text{Stab}(x)| \ .$$

Therefore,

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}|\text{Fix}(g)| &= \sum_{x\in X}\frac{1}{|\text{Orb}(x)|}\\ &= \sum_{i=1}^{r}\sum_{x\in O_i}\frac{1}{|O_i|}\\ &= \sum_{i=1}^{r}|O_i|\frac{1}{|O_i|}\\ &= \sum_{i=1}^{r}1 = r = \text{\# of orbits of } Ga \circlearrowleft X\ .\end{aligned}$$

□

Example 7.4.3. Hwo many necklaces can be made from 4 red, 3 white, 2 yellow beads?

The # of sequences of 4Rs, 3Ws, 2Ys are

$$\frac{9!}{4!3!2!} = 1260\ .$$

Think of these as labelling vertices of an enneagon 9-gon.

Use the action $D_9 \circlearrowleft X\ X = \{all\ such\ labellings\ of\ 9gon\}$

Then need to find $|\text{Fix}(g)|$ for all $g \in D_9$.

1. $g = r^k$ for some $k \in \mathbb{Z}$, where $r = rot_{2\pi/9}$. We know $\langle r\rangle$ has order 9.

Example 7.4.4. How many ways are there to color the edges using 3 colors?

Colourings are equivalent if we can rotate the tetrahedron to get from one colouring to another.

Remark 7.4.2. For each element $g \in A_4$, we figured out the orbits of edges when $A_4 \circlearrowleft \{edges\}$, then each orbit has one color. Example:

8 Classification of Finite Abelian Groups

8.1 L28

THEOREM 8.1.1 — FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS.
Every finite abelian group G is a(n internal) direct product of cyclic groups of prime-power products.

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}} .$$

Moreover, the number of and orders of the cyclic groups are uniquely determined by G.

Example 8.1.1. Let $G = \mathbb{Z}/12$, know $12 = 4 \cdot 3$, with $\gcd(4, 3) = 1 \Rightarrow G \cong \mathbb{Z}/2^2 \times \mathbb{Z}/3$.

DEFINITION 8.1.2 — INTERNAL DIRECT PRODUCT.
A group G is an **internal direct product** of its subgroups H and K if $HK = G$, $H, K \trianglelefteq G$, and $H \cap K = \{e\}$. In this case, $G \cong H \times K$, where we say $H \times K$ is the external direct/cartesian product.

Remark 8.1.3. If $G \cong H' \times K'$, then G is the internal direct product of $H := \varphi^{-1}(H' \times \{e_{K'}\})$ and $K := \varphi^{-1}(\{e_{H;}\} \times K')$, where $\varphi : G \to H' \times K'$ is an isomorphism.

Remark 8.1.4. We can generalize to more factors i.e. if

- $G = H_1 H_2 \cdot H_n$
- $H_1, H_2, ..., H_n \trianglelefteq G$
- $(H_1 H_2 \cdots H_k) \cap H_{k+1} = \{e\}$ for all k

then $G = H_1 \times H_2 \times \cdots \times H_n$

Example 8.1.2. Let $G = \mathbb{Z}/12$, $H = \{g \in G \mid 4g = 0\} = \{0, 3, 6, 9\}$, and $K = \{g \in G \mid 3g = 0\} = \{0, 4, 8\}$. Then $H \cap K = \{0\}$ and $H, K \trianglelefteq G$ as $H = \langle 3 \rangle$ and $K = \langle 4 \rangle$. Finally, notice that $G = H + K$. Therefore, $G \cong H \times K \cong \mathbb{Z}/4 \times \mathbb{Z}/3$.

8.2 Applications of the Theorem Lec 29 - Mar 24

Lemma 8.2.1. If G, H, H' are groups and $|G| < \infty$, then if $G \times H \cong G \times H'$, then $H \cong H'$.

Example 8.2.1. $\mathbb{Z}/4 \times \mathbb{Z}/4 \ncong \mathbb{Z}/4 \times \mathbb{Z}/2 \times /2$.

Example 8.2.2. $G = \mathbb{Z}/30 \times \mathbb{Z}/24 \cong \mathbb{Z}/2^3 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/5$. Elementary divisor decomposition. (Goodman)

Remark 8.2.1. Suppose G is an abelian group, $|G| = p^n$, p prime, and say $G \cong H_1 \times H_2 \times \cdots \times H_k$. Then

- $p^n = |G| = |H_1|\,|H_2|\, \cdots |H_n| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$.
- $p = p_1 = p_2 = \cdots = p_k$, and $n = n_1 + n_2 + \cdots + n_k$.

Putting the n_i's in decreasing order wlog, we see that partitions of n is bijective to (isomorphism classes of abelian groups of order p^n).

Example 8.2.3. List all isomorphism classes of order 32.

$32 = 2^5 = p^n = |G|$. Then

partitions of $n = 5$	representative
(5)	$\mathbb{Z}/32$
$(4,1)$	$\mathbb{Z}/16 \times \mathbb{Z}/2$
$(3,2)$	$\mathbb{Z}/8 \times \mathbb{Z}/4$
$(3,1,1)$	$\mathbb{Z}/8 \times \mathbb{Z}/2 \times \mathbb{Z}/2$
$(2,2,1)$	$\mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/2$
$(2,1,1,1)$	$\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$
$(1,1,1,1,1)$	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$
$\vdots$	$\vdots$

Remark 8.2.2. Contrast this with the full classification of groups of order 8, then

- G is abelian $\Rightarrow 8 = 2^3 \Rightarrow (3), (2,1), (1,1,1) \Rightarrow G \cong \mathbb{Z}/8, \mathbb{Z}/4 \times \mathbb{Z}/2, \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.
- G is not abelian? $D_4, Q(quaterniongroup)$,

Remark 8.2.3. To find isomorphism classes of abelian group of any order n,

- write $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, where p_i's are distinct.
- describe all possible factors for each p_i
- pick one factor from each list and form the product

Example 8.2.4. How many isomorphism classes are there of abelian groups of order 4200?

Let $|G| = 4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$. Then we have $3 \times 1 \times 2 \times 1 = 6$ isomorphism classes of abelian groups of order 4200.

Proposition 8.2.1 (Converse to Lagrange's Theorem for Abelian Groups)**.** If G is finite abelian group and $m \,\big|\, |G|$, then $\exists H \leq G$ with $m = |H|$.

Proof. Induction on $|G|$.

When $n = 1 \Rightarrow m = 1 \Rightarrow H = G$.

Suppose $n > 1$, $m|n$ and let $p|m$ for p prime. Then by Cauchy's Theorem, $\exists K \leq G$ with $|K| = p$. Then $|G/K| = \frac{n}{p}$ is divisible by m/p, and G/K is an abelian group. Hence, by induction hypthesis, G/K has a subgroup $\bar{H}$ with $|\bar{H}|$ = m/p.

Let $H := \pi^{-1}(\bar{H})$, where $\pi : G \to G/K$ is the quotient map, then

$$|H| = |\bar{H}|\,|K| = (m/p)p = m\ .$$

□

8.3 Proof of the FToFAG - L30, Mar 27

Lemma 8.3.1 (Primary Components)**.** Let G be an abelian group, then $|G| = p^n m$, p prime, $p \not| m$, define $G(p) := \{g \in G \,\big|\, g^{p^n} = e\}$, and let $K = \{g \in G | g^m = e\}$. Then G is the internal direct product of $G(p)$ and K, i.e. $G \cong G(p) \times K$, and $|G(p)| = p^n$.

Proof. For all $h, g \in G(p)$, since $gg^{-1} = e$, $(gg^{-1})^{g^n} = e$, then $g^{g^n}(g^{-1})^{g^n} = e \Rightarrow (g^{-1})^{g^n} = e$. Then, $(hg^{-1})^{g^n} = e$. Hence, $hg^{-1} \in G(p)$. Hence, $G(p) \leq G$. Similarly, $K \leq G$. Then, since G is abelian, we have $G(p) \trianglelefteq G, K \trianglelefteq G$.

So want: $G = G(p)K$ and $G(p) \cap K = \{e\}$.

We know that $\exists s, t \in \mathbb{Z}$ with $sm + tp^n = 1$, as gcd$(p^n, m) = 1$. Then for all $x \in G$, $x = x^1 = x^{sm}x^{tp^n} \in G(p)K$, as $x^{|G|} = x^{p^n m} = e$.

Finally, $p^n m = |G| = |G(p)K| = \frac{|G(p)|\,|K|}{|G(p)\cap K|} = |G(p)|\,|K|$. Then by Cauchy's Theorem, if $p||K|$, then K has an order p element, then $K \cap G(p)$ has this order p element. Contradiction. Similarly, no factor of m divide $G(p)$. Therefore, $|G(p)| = p^n$. □

Remark 8.3.1. By induction, we reduce further if $|G| = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ with all p_i's distinct, then define

$$G(p_i) = \{g \in G \,\big|\, g^{p_i^{n_i}} = e\} = \{g \in G \,\big|\, |g| \text{ is a power of } p_i\}\ ,$$

we get G is the internal direct product of $G(p_i)$'s, $G = G(p_1) \times G(p_2) \times \cdots \times G(p_k)$.

Example 8.3.1. We saw $G = \mathbb{Z}/12$ is the internal product of $G(2) = \{g \in G \,\big|\, 4g = 0\}$ and $G(3) = \{g \in G \,\big|\, 3g = 0\}$.

DEFINITION 8.3.2 — P-GROUP.
A group G of order p^n, p prime and $n \in \mathbb{Z}_{>0}$ is a **p-group**. When G is abelian we also say **p-primary group**.

Lemma 8.3.2 (Factoring p-primary groups)**.** Let p prime, G be p-primary with $|G| = p^n$ and G abelian. Let $a \in G$ have a maximal order in G, say $|a| = p^m$, $m \in n$. Then G is the internal direct product of $\langle a \rangle$ and K for some $K \leq G$.

Proof. Induction on n. $n = 1 \Rightarrow G = \langle a \rangle \cong \langle a \rangle \times \{e\}$. Suppose $n > 1$. If $m = n$, then $G = \langle a \rangle \cong \langle a \rangle \times \{e\}$ done.

So assume $m < n$. Also, $\forall x \in G$, $x^{p^m} = e$. Let $b \in G \setminus \langle a \rangle$ if minimal possible order. $\square$

8.4 L31 - Mar 29

Remark 8.4.1. Combining the two lemmas and using induction, we can see that every finite abelian group G is a product $G(p_1) \times G(p_2) \times \cdots \times G(p_k)$ where each $G(p_i)$ is a product of cyclic p_i groups. The only missing ingredient is uniqueness of the cyclic factors.

Lemma 8.4.1 (Uniqueness of the Cyclic Factors)**.** Let G be an abelian $p-$group. Suppose $G \cong H_1 \times H_2 \times \cdots \times H_m \cong K_1 \times K_2 \times K_n$, where every K_i and K_j is a nontrivial cyclic subgroup of G and $|H_1| \geq |H_2| \geq \cdots \geq |H_n|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$ then $m = n$ and $H_i \cong K_i$ for all $1 \leq i \leq n$.

Remark 8.4.2. Proof of Fundamental Theorem is just the combination of three lemmas.

Remark 8.4.3. The fundamental theorem generalizes to finitely generated abelian groups i.e. abelian groups G such that $\exists$ finite set $S \subseteq G$ with $\langle S \rangle = G$.

Every finitely generated abelian group is isomorphic to some $\mathbb{Z}^r \times \mathbb{Z}/p_1^{m_1} \times \mathbb{Z}_2^{m_2} \times \cdots \times \mathbb{Z}/p_k^{m_k}$.

Example 8.4.1. $G = \mathbb{Z}, S = \{1\} \Rightarrow \langle S \rangle = G$.

9 Sylow Theory

For a finite abelian group G, much information is in the prime factorization of the order $|G|$. Partly due to Lagrange's Theorem, which is a consequence of using a kind of partition of G.

Question: what are other useful ways to partition G?

Recall $G \circlearrowright X = G$ by congugation $g \circ x = gxg^{-1}$. Then orbits = conjugacy classes

$$\text{Orb}(x) =: Cl(x) = \{h = gxg^{-1} | g \in G\} \ .$$

9.1 L32 - March 31

Lemma 9.1.1. For a group G and $x \in G$, we have $|Cl(x)| = [G : C(x)]$, where $C(x)$ is the centralizer $C(x) = \{g \in G | gx = xg\}$.

Remark 9.1.1. $|Cl(x)| = 1 \iff Cl(x) = \{x\} \iff \forall g \in G, gxg^{-1} = x \iff \forall g \in G, gx = xg \iff x \in Z(G)$.

Theorem 9.1.2 — The Conjugacy Class Equation.
For a finite group G,

$$|G| = |Z(G)| + \sum_{\text{one x from each conjugacy class of size > 1}} [G : C(x)] \ .$$

Proof. Let $C_1, C_2, ..., C_k$ be all the distinct conjugacy classes. THen $|G| = \sum_{i=1}^{k} |C_i|$ because $G = \cup_{i=1}^{k} C_i$. □

Example 9.1.1. Let $G := S_3$. Two elements $\sigma, \rho \in S_3$ are conjugates if and only if σ, ρ have the same cycle structure.

Cycle structure: (3), $(2,1)$, $(1,1,1)$
Number of elements: $2, 3, 1$.

Then, the class equations says $|S_3| = 1 + 3 + 2$. Can see here that $Z(G) = \{\varepsilon\}$.

Proposition 9.1.1 (p-groups have nontrivial centres)**.** Let G be a nontrivial p-group. Then $Z(G)$ is nontrivial.

Proof. By class equation, we know that

$$RHS = |Z(G)| = |G| - \sum_{\text{one x from each conjugacy class of size > 1} = LHS} \ .$$

Then, for any x from conjugacy class of size > 1, by Lagrange's Theorem, $1 < [G : C(x)] = |G|/|C(x)|$ divides $|G|$ which is a power of p. Then, $p | RHS$, hence, $p||Z(G)|$. Therefore, $|Z(G)| \neq 1$. □

Corollary 9.1.1. If $|G| = p^2$, p prime, then $G \cong \mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$.

Theorem 9.1.3 — Sylow's First Theorem.
Let G be a finite group, p prime, and suppose $p^k \big| |G|$ for $k \in \mathbb{Z}_{\geq 0}$. Then G has an order p^k subgroup.

Proof. If G be abelian, then we are done, so assume G is non-abelian.

We prove by induction on size $|G|$.

Base case when $|G| = 1$, then obviously true.

Now suppose $|G| > 1$ and statement of theorem holds for all groups of smaller order. If $\exists H < G$ s.t. $p^k \big| |H|$, then by induction H has an order subgroup which is a subgroup of G so done.

So suppose for all $H < G$, $p^k \not| |H|$. If G is abelian, then we are done. So we can assume G is not abelian.

For all $x \in G$, by Lagrange's Theorem, $|G| = [G : C(x)] \cdot |C(x)|$. Now $p^k \big| |G|$ but $p^k \not| |C(x)|$ for any $x \notin Z(G)$. Therefore, $p | [G : C(x)]$ for all $x \notin Z(G)$.

$\square$

9.2 L33

Theorem 9.2.1 — Cauchy's Theorem(General Case).
Let G be a finite group, p prime, $p \big| |G|$, then G has an element of order p.

Proof. By Sylow's first theorem, we have that there exists $H \leq G$ with $|H| = p$. So H must be cyclic, by $a^k = e \iff |a| \big| k$ and $a^{|H|} = a^p = e$. $\square$

Definition 9.2.2 — Sylow p-subgroup.
Let G be a finite group, p prime. If p^n is the largest power of p dividing $|G|$, then any subgroup of G of order p^n is called **Sylow p-subgroup**.

Example 9.2.1. Say G is a group of order $|G| = 2^3 \cdot 3^2 \cdot 5^4 \cdot 7$, then Sylow's 1st: G has subgroups of orders $2, 4, 8, 3, 9, 5, 25, 125, 625, 7$; then

- Any subgroup of order 8 is a Sylow 2-subgroup.
- Any subgroup of order 9 is a Sylow 3-subgroup.
- Any subgroup of order 625 is a Sylow 5-subgroup.
- Any subgroup of order 7 is a Sylow 7-subgroup.

Remark 9.2.3. Recall the actions

1. $G \circlearrowright G, g \circ x = gxg^{-1}$
2. $G \circlearrowright \{H \big| H \leq G\}, g \circ H = gHg^{-1}$.

THEOREM 9.2.4 — SYLOW'S SECOND THEOREM.
Let G be a finite group, $H \leq G$, $|H| \leq G$, $|H| = p^k$ for some p prime and $k \in \mathbb{N}$. Then H is contained in a Sylow p-subgroup.

Proof. Suppose K is a some Sylow p-subgroup, say $|K| = p^n$. Let $X = \{K_1, K_2, ..., K_r\}$ be the set of conjugates of K; this is an orbit of action (2). Then action 2 restricts to X, i.e. $gK \in X$ for all $i, \forall g \in G$.

In fact, $g \circ K_i = gK_ig^{-1} \cong K_i$ as φ_g is an automorphism. So every K_i is a Sylow p-subgroup.

Moreover, as $H \leq G$, we can also restrict action (2) to H, i.e. $h \circ K_i := hK_ih^{-1} \in X$ for all $h \in H$. Then by Counting Theorem, $p^k = |H| = |\text{Orb}_H(K_i)| \cdot |Stab_H(K_i)|$ for all i, this gives $|\text{Orb}_H(K_i)| = p^j$ for some $0 \leq j \leq k$ depending on i.

Cosnider the condition $|\text{Orb}_H(K_i)| = 1 \iff \text{Orb}_H(K_i) = \{K_i\} \iff \forall h \in H, hK_ih^{-1} = K_i \iff \forall h \in H, hK_i = K_ih \iff H \leq N(K_i)$.

Claim: If $g \in N(K_i)$ and $|g| = p^l$ for some $0 \leq l \leq n$, then $g \in K_i$.

Proof of Claim. $K_i \trianglelefteq N(K_i)$ so $\langle K_i \rangle \leq N(k_i)$ is a subgroup, Also $|\langle g \rangle \cap K_i| = p^m$ for some $0 \leq m \leq l$. Then $|\langle g \rangle K_i| = \frac{|g| \cdot |K_i|}{\langle g \rangle \cap K_i} = \frac{p^l p^n}{p^m} < p^n$ if $l > m$.

Therefore, $l = m \langle g \rangle \cap K_i = \langle g \rangle \Rightarrow g \in K_i$. □

So we will be done if we knwo $\exists i$ with $|\text{Orb}_H(K_i)| = 1$.

Note $[G : K_i] = [G : N(K_i)][N(K_i) : K_i]$ is not divisible by p, so $[G : N(K_i)]$ is not divisible by p.

Orbit-Stabilizer Theorem tells

[] □

9.3 L34 - April 5

THEOREM 9.3.1 — SYLOW'S THIRD THEOREM.
Let G be a group, $|G| = p^n m$ with p prime, $p \not| m$, and $n > 0$. Then the number n_p of Sylow p-subgroups of G satisfies

$$n_p | m \quad \text{and} \quad n_p \equiv 1 \mod p \ .$$

Moreover, any two Sylow p-subgroups of G are conjugate.

Remark 9.3.2. Often this is called Sylow's Second Theorem, and the first is some combination of the two we've already proved.

Remark 9.3.3. We proved $n_p = [G : N(K)]$ for any Sylow p-subgroup K.

Corollary 9.3.1. If K is a Sylow p-subgroup of G,

THEOREM 9.3.4 .
Let $p < q$ be primes, G is a group of order pq. If $p \not| q-1$, then G is cyclic.

Proof. ☐

Let H, H' be distinct Sylow 3-subgroups. Note H, H' are both abelian, then as $|H| = |H'| = 3^2$, Consider $|HH'| = \frac{9 \cdot 9}{H \cap H'} \leq 72$,