MATH 541 Lecture Notes

Pongsaphol Pongsawakul

Spring 2023

Contents

- Book: Dujmit Foote "Modern Algebra 3rd ed"
- Midterm 3/23 in class
- Final 5/8
- Homeworks: weekly
- Honors Credit: Extra sections + homeworks

1 Groups

Operations often modeled: $+, \cdot$

composition: space of thing that you are looking at $\leftarrow$ alomst always not commutative

Groups: One operation $\cdot$

Rings: 2 operations: $+, \cdot$ that play nice

1.1 Axioms of Groups

By "operation" on S, I mean a function $\cdot S \times S \to S$

Instead of $\cdot(a, b)$, we write $a \cdot b$

A group is a set G with an operation $\cdot$ satisfying:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. There is an identity element: there is one special element $1 \in G$ so $1 \cdot a = a$ for any $a \in G$ and $a \cdot 1 = a$ for any $a \in G$
3. Inverses: For any $a \in G$, there is a $b \in G$ so $a \cdot b = b \cdot a = 1$

Note: $a \cdot b = b \cdot a$ is <u>not</u> an axiom.

If G satisfies this, we call it an abelian group

Example 1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$

1. 0 is the identity
2. inverses: $-a$ is the inverse of a

Example 2. $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$

1. 1 is the identity
2. Inverses: $\frac{1}{a}$ is the inverse of a

Note: $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a group

$(V, +)$ is a group

Example 3. For n, a natural number, $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group

On $\mathbb{Z}$, we say a, b are (mod n) equivalent (written $a \equiv b(\text{mod } n)$) if n divides $a - b$

$\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes mod n

Example 4. $n = 2$: (odds, evens) which is $\{0_{\text{mod } 2}, 1_{\text{mod } 2}\}$

$17_{\text{mod } 2} + 64_{\text{mod } 2} = 81_{\text{mod } 2} = 1_{\text{mod } 2}$

Example 5. $\mathbb{Z}/3\mathbb{Z} = \{0_{\text{mod } 3}, 1_{\text{mod } 3}, 2_{\text{mod } 3}\}$

Example 6. $(2\mathbb{Z}, +)$ is a group (even numbers)

Example 7. If $(G, \cdot_G)$ and $(H, \cdot_H)$ are groups, then $(G \times H, \cdot_G \times \cdot_H)$ is a group

- $(g_1, h_1) \cdot_{G\times H} (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$
- Identity: $1_{G\times H} = (1_G, 1_H)$
- Inverse of (g, h): (g^{-1}, h^{-1})

1.1.1 Properties

- G has exactly 1 identity
- Each $g \in G$, there is exactly 1 inverse of g we write this g^{-1} (i.e. $^{-1} : G \to G$)
- $(g^{-1})^{-1} = g$
- $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
- $(a_1 \cdot a_2 \cdot \ldots \cdot a_m)^{-1} = a_m^{-1} \cdot a_{m-1}^{-1} \cdot \ldots \cdot a_1^{-1}$

Proof.

- Suppose a, b are both identities in G. Then $a = a \cdot b = b$
- Suppose a, b are both inverses of g. i.e $a \cdot g = g \cdot a = 1$ and $b \cdot g = g \cdot b = 1$ Then $b = 1 \cdot b = (a \cdot g) \cdot b = a \cdot (g \cdot b) = a \cdot 1 = a$

- know $g \cdot g^{-1} = g^{-1} \cdot g = 1$ so $(g^{-1})^{-1} = g$
- $(a \cdot b)^{-1}$ satisfies: $x \cdot (a \cdot b) = (a \cdot b) \cdot x = 1$ we check $b^{-1}a^{-1}$ does this

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

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

□

Theorem 8. In G, there is exactly 1 solution to the equation $ax = b$ for a fixed $a, b \in G$

Corollary 9. Cancellation laws:

$$ax = ay \implies x = y$$

$$xa = ya \implies x = y$$

Proof. If $a \cdot x = b$

$$\begin{aligned} a^{-1} \cdot a \cdot x &= a^{-1} \cdot b \\ (a^{-1} \cdot a) \cdot x &= a^{-1} \cdot b \\ 1x = x &= a^{-1} \cdot b \end{aligned}$$

□

Definition 10. For $x \in G$, the order of x, written $|x|$, is the least $n > 0$ so

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n} = 1_G$$

If there is no such n, x has "infinite order"

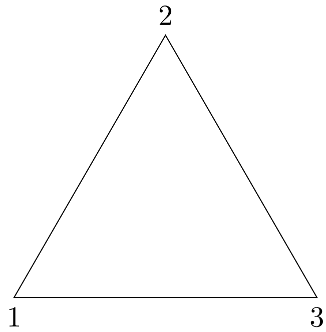
Example 11. In $(\mathbb{R} \setminus \{0\}, \cdot)$, $|5| = \infty$, $|-1| = 2$, $|1| = 1$

Example 12. $(\mathbb{Z}/6\mathbb{Z}, +)$, $|1_{\text{mod } 6}| = 6$, $|2_{\text{mod } 6}| = 3$, $|3_{\text{mod } 6}| = 2$, $|4_{\text{mod } 6}| = 3$, $|5_{\text{mod } 6}| = 2$

1.2 Dihedral Groups

1.2.1 Triangle

Look at the collection of symmetries of an equilateral Triangle



Rotation right

- $1 \to 2$
- $2 \to 3$
- $3 \to 1$

r

Rotation Left

- $1 \to 3$
- $2 \to 1$
- $3 \to 2$

r^2

Reflection around 2

- $1 \to 3$
- $2 \to 2$
- $3 \to 1$

$r^2 \circ s$

Reflection around 1

- $1 \to 1$
- $2 \to 3$
- $3 \to 2$

s

Reflection around 3

- $1 \to 2$
- $2 \to 1$
- $3 \to 3$

$r \circ s = s \circ r^2$

Identity

- $1 \to 1$
- $2 \to 2$
- $3 \to 3$

r^3, s^2

$$\begin{aligned} r^2 s &= r \cdot (r \cdot s) \\ &= (r \cdot s) \cdot r^{-1} \\ &= s \cdot (r^{-1} \cdot r^{-1}) \\ &= s \cdot (r^{-1})^2 \end{aligned}$$

(Symmetry of $\triangle, \circ) = D_6$

1.2.2 n-gon

Rotation right

- $k \to k+1$ (for $k < n$)
- $n \to 1$

$r, |r| = n$

Reflection around 1

- $k \to n+2-k$
- $1 \to 1$

$s, |r| = n$

My Symmetry

- $1 \to k$
- $2 \to k+1$

r^k

So, $\{r, s\}$ generates the group of sym of regular n-gon

(Symmetry of a regular n-gon, $\circ$) $= D_{2n}$

1.2.3 Definition

Rules of dihedral group multiplication in D_{2n} $\{r, s\}$

a) $r^n = 1$

b) $s^2 = 1$

c) $r \cdot s = s \cdot r^{-1}$

When you have generators S for G and can list R_1, R_2, R_3 <u>all</u> the rules you need to know to do multiplication in G Then $\langle S, R_1, R_2, R_3 \rangle$ is a "presentation of the group G"

$D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, rs^{n-1}\}$

Fact: There is a finite set of rule $R_1, \ldots, R_{2000}$ so $\langle a, b | R_1, \ldots, R_{2000} \rangle$ "undecidable word problem"

1.3 Symmetric Group

Given Ω any set, $S_\Omega =$ The permutations of $\Omega =$ The bijections $f : \Omega \to \Omega$

Example 13. $\Omega = \{1, 2, 3\}$

$S_n = S_{\{1,2,\ldots,n\}}$ has $n!$ elements

$|S_3| = 6, |D_6| = 6, D_6 \subseteq S_3$

$|D_{2n}| = 2n$

$|S_n| = n!$

1.3.1 Cycle Decomposition

$1 \to 4, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 5$ can be written as $(1432)(5)$

$(a_1 \ldots a_{m_1})(a_{m_1+1} \ldots a_{m_2})$ with a_i is disjoint represents the function which satisfies

- a_i to a_{i+1} unless $i = m_j$ for some j
- a_{m_j} to $a_{m_{j-1}} + 1$ $j \neq 1$
- a_{m_1} to a_1

$(1)(2)(3)(4)(5)(6)(7) = 1$

$(1442) \circ (3421) = (124)$

$|(123)(45)| = 6$

Order of a product of disjoint cycles is the lcm(lengths of the cycles)

1.4 Homomorphisms and Isomorphisms

Definition 14. A homorphism from $(G, \cdot_G)$ to $(H, \cdot_H)$ is a function $f : G \to H$ such that

$$f(x \cdot_G y) = f(x) \cdot_H f(y)$$

for all $x, y \in G$

- $f(x^{-1}) = f(x)^{-1}$

$$\begin{aligned} f(x) &= f(1_G \cdot_G x) \\ &= f(1_G) \cdot_H f(x) \\ f(x) \cdot_H (f(x))^{-1} &= f(1_G) \cdot_H f(x) \cdot_H (f(x))^{-1} \\ 1_H &= f(1_G) \end{aligned}$$

$$\begin{aligned} 1_H = f(1_G) = f(x \cdot_G x^{-1}) = f(x) \cdot_H f(x^{-1}) \\ 1_H = f(1_G) = f(x^{-1} \cdot_G x) = f(x^{-1}) \cdot_H f(x) \end{aligned}$$

Definition 15. If f is a bijection and a homorphism, then f is an isomorphism

Example 16. $\cdot id : G \to G$

$\cdot^{-1} : G \to G, x \mapsto x^{-1}$

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

is an isomorphism if and only if G is abelian

$xyx^{-1}y^{-1} = 1$

Example 17. $e^x : (\mathbb{R}, +) \to (\mathbb{R}, \cdot), f(x+y) = f(x) \cdot f(y)$ is an isomorphism

Example 18. $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$

- $0 \to 0$
- $1 \to 1$
- $2 \to 2$
- $3 \to 0$
- $4 \to 1$
- $5 \to 2$

is a homorphism NOT an isomorphism

Definition 19. G and H is isomorphic if there is a $f : G \to H$ which is an isomorphism (written $G \cong H$)

If $G \cong H$ then

- G is a belian iff H is abelian

Abelian: For every x, y $x \cdot_G y = y \cdot_G x$

$$f(y) \cdot_H f(x) = f(y \cdot_G x) = f(x \cdot_G y) = f(x) \cdot_H f(y)$$

So, any 2 elements

If f is a $\cong$, $f : G \to H$ and $x \in G$ has order 2 Then $f(x) \in H$ has order 2

$$x^2 = 1_G$$
$$(f(x))^2 = f(x) \cdot f(x) = f(x \cdot x) = f(1_G) = 1_H$$

Recall $D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle$

If $G = \langle g_1, \ldots, g_n \mid R_1, R_2, \ldots \rangle$ and $h_1, \ldots, h_n \in H$ so $R_1(h_1 \ldots h_n) \ldots$ Then $f : g_i \mapsto h_i$ is a homomorphism

1.5 Group Actions

Definition 20. A group action is a function

$$\alpha : G \times A \to A$$

so

$$\alpha(g, \alpha(h, a)) = \alpha(g \cdot h, a)$$

We write $g \cdot a$ for $\alpha(g, a)$

$$g \cdot (h \cdot a) = (g \cdot h) \cdot a$$

- $1_G \cdot a = a$ for any $a \in A$

For any $g \in G$ the function $g\cdot : A \to A$, $a \mapsto g \cdot a$ is a bijection of a.

$$\begin{aligned}(g \cdot (g^{-1} \cdot_G)) &: A \to A \\ &= (g \cdot g^{-1}) \cdot a \\ &= 1_G \cdot a = a \\ g^{-1}(g \cdot a) &= a\end{aligned}$$

Since this function has an inverse (as a funciton) it is bijective

Recall: S_A is the group of all permutations of A

Get a function $\sigma : G \to S_A$ and $\sigma(g) =$ the function $a \mapsto g \cdot a$

Observation: σ is a homomorphism

$$\sigma(g \cdot h) = \sigma(g) \cdot \sigma(h)$$

Example 21. $(\mathbb{R}, +)$ acts on $A = \{1, 2, 3\}$

$g \cdot a = a$

$\sigma : \mathbb{R} \to S_3$, $g \mapsto 1_{S_3}$

2 Subgroups

2.1 Definition and Examples

Definition 22. Let G be a group. The subset H of G is a subgroup of G if

- $1_G \in H$
- $\forall x, y \in H,\ x \cdot y \in H$
- $\forall x \in H,\ x^{-1} \in H$

We write $H \leq G$ to indicate that H is a subgroup of G.

Proposition 23. A subset H of a group G is a subgroup of G if and only if

- $H \neq \emptyset$
- $\forall x, y \in H, xy^{-1} \in H$

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Definition 24 (Centralizer)**.** Let G be a group and A be a subset of G. The centralizer of A in G is

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$$

Moreover, $C_G(A)$ is a subgroup of G.

Definition 25 (Center)**.** Let G be a group. The center of G is

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

Definition 26 (Normalizer)**.** Let G be a group and A be a subset of G. Let

$$gAg^{-1} = \{gag^{-1} \mid a \in A\}$$

The Normalizer of A in G is

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

Definition 27 (Stabilizer)**.** If G is a group acting on a set S and s is some fixed element of S the stabilizer of s is

$$G_s = \{g \in G \mid g \cdot s = s\}$$

2.3 Cyclic groups

Definition 28. A group H is a cyclic if H can be generated by a single element. i.e., $H = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ for some $x \in H$.

Proposition 29. If $H = \langle x \rangle$, then $|x| = n$.

Proof. Let $|x| = n$ then $1, x, x^2, \dots, x^{n-1}$ are distinct

If $x^a = x^b$ for $0 \le a < b < n$ then $x^{b-a} = 1$ but $b - a < n$ contradict □

Proposition 30. Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$.

Proof. By the Euclidean Algorithm, there exists $q, r \in \mathbb{Z}$ such that $d = mr + ns$ where $d = (m, n)$. Thus

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1$$

□

Theorem 31. For any two cyclic groups of the same order are isomorphic.

Proof. Suppose $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n. Let $\varphi : \langle x \rangle \to \langle y \rangle$ be defined by $\varphi(x^k) = y^k$

- φ is well defined, if $x^r = x^s$ then $\varphi(x^r) = \varphi(x^s)$. Because $x^r = x^s$ then from proposition 30, $n \mid r - s$, $r = tn + s$ then

$$\begin{aligned}\varphi(x^r) &= \varphi(x^{tn+s}) \\ &= y^{tn+s} \\ &= (y^n)^t y^s \\ &= y^s \\ &= \varphi(x^s)\end{aligned}$$

- φ is injective
- φ is surjective

□

Theorem 32. If H_1, H_2 is cyclic groups and $|H_1| = |H_2|$ then $H_1 \cong H_2$.

Proposition 33. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

1. If $|x| = \infty$, then $|x^a| = \infty$
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$
3. If $|x| = n < \infty$ and $a \mid n$ then $|x^a| = \frac{n}{a}$

Proof.

1. Proof by contradiction, Suppose $|x| = \infty$ and $|x^a| = m < \infty$ then, $1 = (x^a)^m = x^{am}$ and $x^{-am} = (x^{am})^{-1} = 1^{-1} = 1$. Since either am or $-am$ is greater than 0, then it is contradicts $|x| = \infty$
2. Since $x^n = 1$ so $(x^n)^{\frac{a}{(n,a)}} = (x^a)^{\frac{n}{(n,a)}}$ then $|x^a| = \frac{n}{(n,a)}$.
3. Just a special case of 2.

□

Theorem 34. If $H = \langle x \rangle$ and $|x| = n$ then $x^a = 1$ if and only if $n \mid a$.

Theorem 35. If $H = \langle x \rangle$ and $K \leq H$. Then K is cyclic

Proof. Let a be the least positive integer such that $x^a \in K$, let $y = x^a$

Then we want to show $\langle y \rangle = K$.

- $\langle y \rangle \subseteq K$: Obvious
- $\langle y \rangle \supseteq K$: Given $x^b \in K$ we can write $b = am + r$ with $0 \leq r < a$

$$\begin{aligned} x^b &= x^{am+r} = (x^a)^m x^r \\ &= y^m x^r \ (x^r \in K) \\ x^r &= y^{-m} x^b \ (y^{-m}, x^b \in K) \end{aligned}$$

  So, $x^r \in K$ so $r = 0$, $x^b = y^m$

Therefore $\langle y \rangle = K$ □

3 Quotient Groups and Homomorphisms

3.1 Definition and Examples

Definition 36. If $\varphi : G \to H$ is a homomorphism then $\ker(\varphi) = \{x \in G \mid \varphi(x) = 1_H\}$

Lemma 37. $\ker(\varphi) \leq G$

Proof. Proof eash properties of subgroup

- Closed identity, Since $\varphi(1_G) = 1_H$

$$\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G) \cdot \varphi(1_G) = 1$$

  So, $1_G \in \ker(\varphi)$

- Closed under inverses, if $x \in ker(\varphi)$

$$\varphi(x^{-1}) = (\varphi(x))^{-1} = (1_H)^{-1} = 1_H$$
$$1_H = \varphi(1_G) = \varphi(x^{-1}x) = \varphi(x) \cdot \varphi(x^{-1})$$

  So, $x^{-1} \in \ker(\varphi)$

- Closed under multiplication, if $x, y \in \ker(\varphi)$

$$\begin{aligned} \varphi(xy) &= \varphi(x) \cdot \varphi(y) \\ &= 1_H \cdot 1_H = 1_H \end{aligned}$$

  So, $xy \in \ker(\varphi)$

$\square$

Definition 38. Given $\varphi : G \to H$ a homomorphism and $K = \ker(\varphi)$ For any $a \in H$, let

$$X_a = \{x \in G \mid \varphi(x) = a\}$$

then

$$G/K = (\{X_a \mid a \in H\}, \circ)$$

where

$$X_a \circ X_b = X_{ab}$$

Lemma 39. If $\varphi : G \to H$ is a homomorphism, $K = \ker(\varphi)$, and $\varphi(b) = a$ then $X_a = bK$ where $bK = \{bz \mid z \in K\}$

Proof. The goal is to show $X_a = bK$

- $X_a \supseteq bK$, Given $y \in bK, y = bz$ for some $z \in K$

$$\varphi(y) = \varphi(b \cdot z) = \varphi(b) \cdot \varphi(z) = a \cdot 1_H = a$$

- $X_a \subseteq bK$, Given $\varphi(y) = a$

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

Therefore $X_a = bK$ □

Definition 40. For any $N \leq G$ and for any $g \in G$ let

$$gN = \{gn \mid n \in N\}$$

and

$$Ng = \{ng \mid n \in N\}$$

Theorem 41. Let G be a group and K be the kernel of some homomorphism. Then the set whose elements are the left cosets of K in G with operation defined by

$$uK \circ vK = (uv)K$$

forms a group G/K.

Proof. Let $X, Y \in G/K$ and let $Z = XY$ in G/K. Since K is the kernel of some homomorphism, $\varphi : G \to H$, so $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$ for some $a, b \in H$. By definition of the operation in G/K, $Z = \varphi^{-1}(ab)$.

Let u, v be arbitrary representatives of X, Y ($\varphi(u) = a, \varphi(v) = b$ and $X = uK, Y = vK$)

GOAL: show $uv \in Z$

$$\begin{aligned} uv \in Z &\iff uv \in \varphi^{-1}(a, b) \\ &\iff \varphi(uv) = ab \\ &\iff \varphi(u)\varphi(v) = ab \end{aligned}$$

Therefore Z is the (left) coset $(uv)K$. □

Proposition 42. If $N \leq G$ then for all $u, v \in G, uN = vN$ if and only if $v^{-1}u \in N$

Proof. Since N is a subgroup of G, since $1_G \in N$ then

$$G = \bigcup_{g \in G} gN$$

If $x \in uN \cap vN$ then for some $n_1, n_2 \in N$

$$\begin{aligned} x &= un_1 = vn_2 \\ v^{-1}u &= n_2 n_1^{-1} \in N \end{aligned}$$

For any $n \in N$

$$un = (vv^{-1})un = v(v^{-1}un) \in vN$$

So $uN \subseteq vN$, wlog, $vN \subseteq uN$. Therefore $uN = vN$. □

Definition 43. The element gng^{-1} is called the *conjugate* of $n \in N$ by g. The set gNg^{-1} is called the *conjugate* of N by g. if $gNg^{-1} = N$ then g is said to *normalize* N.

If $N \leq G$ called *normal* if for any $g \in G$ normalizes N. In another word, $gNg^{-1} = N$ for all $g \in G$, written

$$N \trianglelefteq G$$

Theorem 44. For $N \leq G$, the following are equivalent

- $N \trianglelefteq G$
- $N_G(N) = G$
- $gN = Ng$ for all $g \in G$
- $gNg^{-1} \subseteq N$ for all $g \in G$

3.2 More on Cosets and Lagrange's Theorem

Theorem 45 (Lagrange's Theorem)**.** Let G be a finite group and $H \leq G$, then

$$|H| \mid |G|$$

and

$$\frac{|G|}{|H|}$$

is the number of H-cosets in G.

Proof. let $|H| = n$ and k be the number of H-cosets in G. By the definition, the map

$$H \to gH$$
$$h \mapsto gh$$

So

$$|gH| = |H| = n$$

Since G is partitioned into k disjoint subsets each of which has cardinality n, $|G| = kn$. Therefore, $k = \frac{|G|}{|H|}$. □

Definition 46. If $H \leq G$. then the "index of H in G" is the number of left H cosets in G and denoted by $|G : H|$

Corollary 47. If G is a finite group and $x \in G$ then $|x| \mid |G|$, So, $x^{|G|} = 1$

Proof. let $H = \langle x \rangle \leq G$ So $|x| \mid |G|$ Since for $x^a = 1$ if and only if $|x| \mid a$, So $x^{|G|} = 1$ □

Corollary 48. If $|G| = p$ is prime, then $G \cong \mathbb{Z}/p\mathbb{Z}$

Proof. Take any $x \in G \setminus \{1\}$, $|x| \mid |G|$, So, $|x| = p$ Since $\langle x \rangle = H \leq G$ and $p = |x| = |H|$ therefore $H = G$ □

Theorem 49. For any $n \in \mathbb{N}$ either $p \mid n$ or $p \mid n^{p-1} - 1$

Theorem 50 (Sylow)**.** If G is finite of order $p^\alpha \cdot m$ where $p \nmid m$ where p is prime. Then G has a subgroup of size p^α.

Definition 51. If $H, K \leq G$ then

$$HK = \{hk \mid h \in H, k \in K\} = \bigcup_{h \in H} hK$$

Lemma 52. If cK intersects H then $|cK \cap H| = |K \cap H|$

Proof. Let $a \in cK \cap H$ let $f : K \cap H \to cK \cap H$, $x \mapsto ax$

Claim: $x \in K \cap H \implies ax \in cK \cap H$ $ax \in H$ because $a, x \in H \leq G$

$a = cl$ for some $l \in K$ because $a \in cK$ $ax = c\underbrace{(lx)}_{\in K} \in cK$ So, f is now injective

Claim: If $y \in cK \cap H$ then $a^{-1}y \in K \cap H$ $y \in cK$, $y = cl$, $a^{-1}y = (a^{-1}cl \in K$

□

Theorem 53. If H, K are finite subgroups of G then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof. $|HK| = |\bigcup_{h \in H} hK| = |K| \cdot$ number of K-coests of the form hK for $h \in H$. Each $h \in H$ define a coset hK. But $h_1K = h_2K \iff h_2^{-1}h_1 \in K$ Thus

$$h_1K = h_2K \iff h_2^{-1}h_1 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K)$$

The number of distinct K-coset of the form hK for $h \in H$ is the number of distinct $H \cap K$-cosets $h(H \cap K)$ for $h \in H$. By Lagrange Theorem, equal $\frac{|H|}{|H \cap K|}$ □

Proposition 54. For $H, K \leq G$ then $HK \leq G$ if and only if $HK = KH$

Proof. $\Leftarrow$ assume $HK = KH$

- $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$
- $(h_1k_1)(h_2k_2) = (h_1k_1)(k_3h_3) = h_1k_4h_3 = k_4h_5h_3 = k_4h_6 \in KH = HK$

$\Rightarrow$ Assume $HK \leq G$

- $H, K \leq HK$ because $H = H \cdot 1 \subseteq HK, K = 1 \cdot K \subseteq HK$

  So, for $a \in H, b \in K$, $a, b \in HK$ then $ba \in HK$. Therefore $KH \subseteq HK$
- Let $y \in HK, y = hk, y^{-1} = k^{-1}h^{-1} \in KH$

  So $HK \subseteq KH$

□

Corollary 55. If $H, K \leq G$ and $H \leq N_G(K)$. Then $HK \leq G$. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

3.3 The Isomorphism Theorems

Theorem 56 (First Isomorphism Theorem)**.** If $\varphi : G \to H$ is a homomorphism then

- $\ker(\varphi) \trianglelefteq G$
- $G/\ker(\varphi) \cong \varphi(G)$

Definition 57. $\varphi(G) = \operatorname{im}(\varphi) = \{y \in H \mid \exists x \in G, \varphi(x) = y\}$

Proof.

- for any $x \in \ker(\varphi)$, for any $g \in G$

$$\begin{aligned}\varphi(gxg^{-1}) &= \varphi(g)\varphi(x)\varphi(g^{-1}) \\ &= \varphi(g) \cdot 1_H \cdot \varphi(g^{-1}) \\ &= \varphi(g)\varphi(g^{-1}) \\ &= \varphi(g)\varphi(g)^{-1} \\ &= 1_H\end{aligned}$$

  Since $\varphi(gxg^{-1}) = 1_H$, So $gxg^{-1} \in \ker(\varphi)$. Therefore $\ker(\varphi) \trianglelefteq G$

- Let $f : G \to G/\ker(\varphi)$, $a \cdot K \mapsto \varphi(a)$ ($K = \ker(\varphi)$)

  $aK = bK \iff b^{-1}a \in K$

  If $aK = bK$ want $\varphi(a) = \varphi(b)$

$$\begin{aligned}\varphi(a) &= \varphi(b \cdot b^{-1}a) \\ &= \varphi(b) \cdot \varphi(b^{-1}a) \\ &= \varphi(b) \cdot 1 \\ &= \varphi(b)\end{aligned}$$

$$f(aK \cdot bK) = f(ab \cdot K) =$$

□

Corollary 58. Let $\varphi : G \to H$ be a homomorphism

1. φ is injective iff $\ker(\varphi) = \{1_G\}$
2. $|G : \ker(\varphi)| = |\varphi(G)|$

Theorem 59 (2nd or "Diamond" isonorphism theorem)**.** Given G, a group, $A, B \leq G$ and $A \leq N_G(B)$ (i.e., $aBa^{-1} = B$ for every $a \in A$) then

- $AB \leq G$
- $B \trianglelefteq AB$
- $A \cap B \trianglelefteq A$

- $AB/B \cong A/(A \cap B)$

Proof.

- For $B \trianglelefteq AB$. For any $a \in A, b \in B$

$$\begin{aligned} abB(ab)^{-1} &= B \\ abB(ab)^{-1} &= a(bBb^{-1})a^{-1} = aBa^{-1} = B \end{aligned}$$

- For $A \cap B \trianglelefteq A$

  we want for any $a \in A$, $a(A \cap B)a^{-1} = A \cap B$

$$\begin{aligned} a(A \cap B)a^{-1} &\subseteq aAa^{-1} = A \\ a(A \cap B)a^{-1} &\subseteq aBa^{-1} = B \end{aligned}$$

  Given $y \in A \cap B$, for any $a \in A$, WANT $y \in a(A \cap B)a^{-1}$

$$\begin{aligned} a^{-1}ya &\in a^{-1}(A \cap B)A \subseteq A \cap B \\ y = a(a^{-1}ya)a^{-1} &\in a(A \cap B)A^{-1} \end{aligned}$$

  Therefore $a(A \cap B)a^{-1} = A \cap B$, so $A \cap B \trianglelefteq A$

- WANT $\varphi : A \to AB/B$

$$\begin{aligned} x &\in ab \cdot B = aB \\ x &= ab \cdot b' (\text{for some } b' \in B) \\ &= a \cdot (bb') (\text{for some } b' \in B) \end{aligned}$$

  $\varphi(a) = aB$

$$A \to AB \to AB/B$$

$$a \mapsto a \mapsto AB$$

$$\begin{aligned} \varphi(a \cdot a') &= a \cdot a'B \\ \varphi(a) \cdot \varphi(a') &= aB \cdot a'B = aa'B \end{aligned}$$

  φ is onto. For any $ab \in AB$

$\square$

Theorem 60 (The 3rd theorem)**.** Given G, a group, $H, K \trianglelefteq G$ with $H \trianglelefteq K$ Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong (G/K)$

3.4 Transpositions and the Alternating Group

3.4.1 The Alternating Group

Let $x_1, \ldots, x_n$ be independent variables and let Δ be the polynomial

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

For each $\sigma \in S_n$ let σ act on Δ by permuting the variable in the same way as σ

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

For each $\sigma \in S_n$ let

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma(\Delta) = \Delta \\ -1 & \text{if } \sigma(\Delta) = -\Delta \end{cases}$$

Definition 61.

- $\varepsilon(\sigma)$ is call the sign of σ
- if $\varepsilon(\sigma) = 1$, σ is called an even permutation, if -1 it is called an odd permutation

Proposition 62. The map $\varepsilon : S_n \to \{1, -1\}$ is a homomorphism

Proof. Let k_1 be the number of inversions in σ and k_2 be the number of inversions in τ Obviously, $\varepsilon(\sigma) = (-1)^{k_1}$ and $\varepsilon(\tau) = (-1)^{k_2}$. Let k be the number of inverstion in $\sigma \circ \tau$, so, $k = k_1 + k_2 - 2 \cdot$ (number of inversion in the same position). Hence, $\varepsilon(\sigma \circ \tau) = (-1)^k = \varepsilon(\sigma) \cdot \varepsilon(\tau)$ $\square$

Definition 63 (alternating group)**.** The alternating group of degree n, A_n, is the kernel of the homomorphism ε

Proposition 64. The permutation σ is odd $\iff$ the number of cycles of even length if its sycle decomposition is odd.

4 Group Actions

For any $g \in G$ we have

$$\begin{aligned} \sigma_g : A &\to A \\ a &\mapsto g \cdot a \end{aligned}$$

$\varphi : g \mapsto \sigma_g$

- $g \cdot (h \cdot a) = gh \cdot a$
- $1 \cdot a = a$

Example 65. $\varphi : G \to S_A$ is a homomorphism $g \cdot a = \varphi(g)(a)$, then φ is homomorphism then G action on A by $g \cdot a = \varphi(g)(a)$

Proof.

$$\begin{aligned} g \cdot (h \cdot a) &= \varphi(g)(\varphi(h)(a)) \\ &= (\varphi(g) \circ \varphi(h))(a) \\ &= \varphi(gh)(a) \\ &= gh \cdot a \end{aligned}$$

$$\begin{aligned} 1 \cdot a &= \varphi(1)(a) \\ &= 1_{S_A}(a) \\ &= a \end{aligned}$$

□

Example 66. The Kernel of the action G on A is

$$\{g \in G \mid ga = a \ \forall a \in A\} = \{g \mid \sigma_g = id_A = 1_{S_A}\}$$

Example 67. For each $a \in A$, the stabilizer of a is

$$G_a = \{g \in G \mid g \cdot a = a\}$$

Observation 68. If G acts on A, faithfully then

$$G \cong \varphi(G)$$

Proof. $G \cong G/\ker(\varphi) \cong \varphi(G) \subseteq S_A$ □

4.1 Group Actions and Permutation Representations

Definition 69. Let G be a group, $\varphi : G \to S_A$ is a "permutation representation" of G into S_A

Proposition 70 (Orbit Equivalence Relations)**.** Let G acts on A. Define the relation $\sim$ on A by $a \sim b$ if $a = gb$ for some $g \in G$ Then $\sim$ is an equivalence relation

For each $a \in A$, $|[a]|$ is $|G : G_a|$

Proof. Check $\sim$

- (reflexive $a \sim a$) $1_G \cdot a = a$
- (symmetric $a \sim b \implies b \sim a$) $\sigma_(g^{-1}) = (\sigma_g)^{-1}$
- (transitive $a \sim b \wedge b \sim c \implies a \sim c$)

$$\begin{aligned} h \cdot b &= a \\ h \cdot g \cdot c &= a \\ (hg) \cdot c &= a \end{aligned}$$

Every element of G □

Definition 71. Let G acts on A.

- $[a] = \{b \mid a \sim b\}$ is called the orbit of G containing a
- $a \sim b$ is said "a and b are equivalent"
- The action of G on A is **transitive** if there is only 1 orbit (orbit class)

4.1.1 cycle decomposition

Example 72. Every element $\sigma \in S_A$ has a cycle decomposition

$$\sigma = (a_1\ a_2\ \dots)(b_1\ b_2\ \dots)\dots$$

Theorem 73. Cycle decomposition are unique up to permutiting between cycles and rotating the cycles

Theorem 74. If $\sigma \in S_A$, then σ is a product of distinct elements $(n\ x)$ or $(n\ y)$ for $n \in A, x, y \notin A$

4.2 The left-multiplication action()

G acts on G by $g \cdot h = gh$, $g_1(g_2 \cdot h) = g_1 g_2 h = g_1 g_2 \cdot h$

Observation 75. The left-multiplication action is transitive, faithful and $G_a = \{1\}$ for any $a \in G$

Proof. $(ba^{-1}) \cdot a = b$, so ba^{-1} moves a to b so, the action is transitive.

$$x \in G_a \iff x \cdot a = a \iff xaa^{-1} = a^{-1} \iff x = 1$$

□

Theorem 76. $H \leq G$, G act on A by left-multiplication

1. G acts transitively on A
2. $G_{1H} = H$
3. ker of the action $(= \{g \in G \mid g \cdot aH = aH\}) = \bigcap_{x \in G} xHx^{-1}$ =the normal subgroup of G which is contained in H

Proof. 1. $(ba^{-1}) \cdot aH = bH$

2.

$$\begin{aligned} G_{1H} &= \{g \in G \mid g \cdot 1H = 1H\} \\ &= \{g \in G \mid gH = 1H\} \\ &= \{g \in 1^{-1}g \in H\} \\ &= \{g \in g \in H\} \\ &= H \end{aligned}$$

3.

$$\begin{aligned} g \in \ker(\text{action}) &\iff g \cdot xH = xH \quad \text{for every } x \in G \\ &\iff g \in \bigcap_{x \in G} \{a \in G \mid a \cdot xH = xH\} \\ &\iff g \in \bigcap_{x \in G} \{a \in G \mid x^{-1}ax \in H\} \\ &\iff g \in \bigcap_{x \in G} \{a \in G \mid a \in xHx^{-1}\} \\ &\iff g \in \bigcap_{x \in G} xHx^{-1} \end{aligned}$$

□

Corollary 77. If G is a finite group of order n. Let p be the smallest prime dividing n. Suppose $H \leq G$ so $|G : H| = p$ then $H \trianglelefteq G$

Proof. $G \curvearrowright A = \{\text{left } H\text{-cosets}\}$

$\pi : G \to S_A$ be the representation of this action

$k = \ker(\pi)$

Goal: $H = K$, i.e., $|H : K| = 1$ □

4.3 Conjugation action of G on G

$$g \cdot h = ghg^{-1}$$
$$g \cdot S = gSg^{-1} = \{gxg^{-1} \mid x \in S\}$$

Size of an orbit, orbit of a = $|G : G_a|$

Size of orbit of $h \in G = |G : C_G(h)|$, $S \subseteq G = |G : N_G(S)|$

Theorem 78 (the class equation)**.** let G be a finite group and $g_1, g_2, \ldots g_r$ be reoresentatives of all the conjugacy classes then

$$|G| = \sum_{i=1}^{r} |\text{Orbit}(g_i)| = \sum_{i=1}^{r} |G : G_{g_i}| = \sum_{i=1}^{r} |G : C_G(g_i)|$$

let $g_1, \ldots, g_r$ be representative of every conjugate class not contained in $Z(G)$

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

Theorem 79. let p be prime, G a group of order p^α for some $\alpha \in \mathbb{N}$ then $|Z(G)| \neq 1$

Proof. let $g_1, \ldots, g_r$ represents all conjugacy classes of size ≥ 1

$$p^\alpha = |G| = \sum_{i=1}^{r} |g : C_G(g_i)| + |Z(G)|$$
$$|G| = \underbrace{|G : C_G(g_i)|}_{\neq 1} \cdot |C_G(g_i)|$$

So, $p \mid |G : C_G(g_i)|$, so $p \mid |Z(G)| \implies |Z(G)| \geq p$ □

Example 80. Q:What is a conjugacy class in S_n?

Describe when 2 diff, products of disj cycles are conjugate

$\sigma = (1\ 2\ 3)(4\ 5)(6)$, for $\tau = (1\ 2\ 3\ 4\ 5\ 6)$

$$\tau\sigma\tau^{-1} = (1)(2\ 3\ 4)(5\ 6)$$
$$\sigma = (6)(1\ 2\ 3)(4\ 5)$$
$$\tau\sigma\tau^{-1} = (\tau(6))(\tau(1)\ \tau(2)\ \tau(3))(\tau(4)\ \tau(5))$$

Observation 81. If $\sigma = (a_1\ \ldots a_{r_1})(a_{r_1+1}\ \ldots\ a_{r_2})\ldots$ then

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \ldots \tau(a_{r_1})\ldots$$

Proof.

$$\tau\sigma\tau^{-1}(\tau(a_j)) = \tau\sigma(a_j) = \tau(a_{j_1})$$
$$\tau\sigma\tau^{-1}(\tau(a_{r_n})) = \tau\sigma(a_{r_n}) = \tau(a_{r_{n-1}} + 1)$$

□

If $\sigma =$ a product of disj cycles of lengths $n_1, \ldots, n_r$ (including 1-cycles) and $n_1 \leq \ldots \leq n_r$ then $(n_1\ \ldots\ n_r)$ is the cycle-type of σ

Observation 82. p is conj to $\sigma \iff$ they have the same cycle-type.

Example 83. The conj classes in S_5