PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 1: September 8

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

1.1 Motivation

Let's say we have a square (four vertices connected together, each vertex with a unique label), how could we "act" on this shape to preserve its shape/symmetry?

We may use different labels to represent how many 90 degrees has been rotated, how the square is flipped, etc. Use these labels, put it on the left side, would mean that some operations are "acted" on the square.

Can these actions be undone? Yes.

What do we need to make the above arguments valid (put (multiple) operators on the left to represent operation)?

- Operation between symmetries (Composition)
- Do nothing
- All actions could be undone
- Associativity: we need $H \cdot V \cdot R = (HV)R = H(VR)$

Definition 1.1. a **group** is a set G equipped with an operation

$$\cdot : G \times G \to G$$

such that:

- **Associativity** For all $a, b, c \in G$, $(ab)c = a(bc)$
- **Identity** There exists $e \in G$ such that $ge = eg = g$ for all $g \in G$
- **Inverses** For all $g \in G$, there exists $h \in G$ such that $gh = hg = e$

Remark:

- We call e the identity of the group
- If $gh = hg = e$, we write $h = g^{-1}$ and call g^{-1} the inverse of g in G.
- In an abstract group, we often call $\cdot$ multiplication.

Group are the math obejects of change. We use them to act on or transform objects.

Notation: we need the set G, and the dot operation $\cdot$. We often write $(G, \cdot)$. Note that we do not require $ab = ba$ for a, b in a group.

1.2 Examples

Example 1.2. We will see some examples for the above definition

- For the group $(\mathbb{Z}, +)$, $e = 0, 2^{-1} = -2$, since $2 + (-2) = (-2) + 2 = 0$.
- For $(\mathbb{Z}, \times)$, this is not a group, since we do not have $2^{-1} \in \mathbb{Z}$.
- $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$ are all groups
- $(\mathbb{R}, \cdot)$ is not a group, since 0 does not have an inverse: there does not exists an element $g \in \mathbb{R}$ such that $0g = g0 = 1$
- $(\mathbb{R}^\times, \cdot)$ is a group, where $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
- $(\mathbb{Q}^\times, \cdot)$ $(\mathbb{C}^\times, \cdot)$ are groups.
- for $n \in \mathbb{Z}$, $n > 1$, $(\mathbb{Z}_n, +)$ is a group. Let's say $n = 5$, $Z_5 = \{0, 1, 2, 3, 4\}$, and we have $-2 = 3 (3 + 2 = 2 + 3 = 0)$
- for $n \in \mathbb{Z}$, $n > 1$, $(\mathbb{Z}_n, \cdot)$ is not a group, since 0 does not have an inverse
- for $n \in \mathbb{Z}$, $n > 1$, $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is not a group. For example, $n = 4$, we have $e = 1$, $2 \cdot 0 = 0, 2 \cdot 1 = 2, 2 \cdot 2 = 0, 2 \cdot 3 = 2$, 2^{-1} does not exist

Remark: If G is a group under addition $(+)$, we write $-g$ instead of g^{-1}

Recall that, from MATH135, for $n > 1$, $n \in \mathbb{Z}$:

$$\{x \in \mathbb{Z}_n : \exists y \in \mathbb{Z}_n, xy = 1\} = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$$

i.e. the elements with inverses are precisely the elements coprime with n. We define such group as $\mathbb{Z}_n^\times$:

Definition 1.3.

$$\begin{aligned} \mathbb{Z}_n^\times &= \{x \in \mathbb{Z}_n : \exists y \in \mathbb{Z}_n, xy = 1\} \\ &= \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\} \end{aligned}$$

And then we can say $(\mathbb{Z}_n^\times, \cdot)$ is a group. For example, $\mathbb{Z}_6^\times = \{1, 5\}$.

Let p be a prime, then

$$\begin{aligned}\mathbb{Z}_p^\times &= \{1, 2, 3, ..., p-1\} \\ &= \mathbb{Z}_p \setminus \{0\}\end{aligned}$$

1.2.1 Matrix Groups

Notation:

$M_n(\mathbb{R})$ would be the set of $n \times n$ real matrices

Simialrly, we have $M_n(\mathbb{Q}), M_n(\mathbb{Z})$.

Example 1.4. Let $+$ be the matrix addition, $\cdot$ be the matrix multiplication

- $(M_n(\mathbb{R}), +)$ is a group. e is the zero matrix. For matrices $A \in M_n(\mathbb{R})$, we have $-A$.
- Similarly, we have $(M_n(\mathbb{Q}), +), (M_n(\mathbb{Z}), +), (M_n(\mathbb{C}), +)$ as groups.
- $(M_n(\mathbb{R}), \cdot)$ is not a group. If we have $A \in M_n(\mathbb{R})$ with $\det A = 0$, then A^{-1} does not exists.
- Let $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$. This is called Real General Linear Group, and then we can see that $(GL_n(\mathbb{R}), \cdot)$ is a group
- However $(GL_n(\mathbb{Z}), \cdot)$ is not a group, since taking inverses might not preserve integrality. For example, $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} \notin GL_2(\mathbb{Z})$

1.2.2 Function Groups

Example 1.5. Denote $F(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} : f \text{ is a function }\}$

- $(F(\mathbb{R}), +)$ where $+$ denotes the operation that $(f+g)(x) = f(x) + g(x)$ is a group.
- $(F(\mathbb{R}), \cdot)$ where $\cdot$ denotes the operation that $(f \cdot g)(x) = f(x)g(x)$ is not a group. Since $f = 0$ is not invertible.
- $(F(\mathbb{R}), \circ)$ where $\circ$ denotes the operation that $(f \circ g)(x) = f(g(x))$ is not a group. For example, $f(x) = x^2$ is not invertible.
- Let X be a set

  $$\begin{aligned}S_X &= \{f \text{ as a function such that } X \to X : f \text{ is invertible}\} \\ &= \{f \text{ as a function such that } X \to X : f \text{ is bijective}\}\end{aligned}$$

  Then we would have $(S_X, \circ)$ as a group
- Notation-wise, if $X = \{1, 2, ..., n\}$, then $S_X = S_n$. We call S_X as the **symmetric group** on X

Definition 1.6. The **symmetric group** on a set X is defined as

$$\begin{aligned} S_X &= \{f \text{ as a function such that } X \to X : f \text{ is invertible}\} \\ &= \{f \text{ as a function such that } X \to X : f \text{ is bijective}\} \end{aligned}$$

Definition 1.7. The **Dihedral group** (operations with rotation, flip, etc.):

Let's say we have $D_4 = \{e, r, r^2, r^3, s_1, s_2, V, H\}$. We have $(D_4, \circ)$ is a group.

1.2.3 Basic Properties

If for a group G, the operation $\cdot$ is understood, then we can just write G instead of $(G, \cdot)$. For example, $\mathbb{Z} = (\mathbb{Z}, +)$, $\mathbb{R}^\times = (\mathbb{R}^\times, +)$

Theorem 1.8. Let G be a group, we have the following properties

1. The identity of G is unique
2. For all $g \in G$, g^{-1} is unique
3. For all $g \in G$, $(g^{-1})^{-1} = g$
4. For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

Proof 1.9. We wish to prove the above properties for a group G

1. Let e_1, e_2 be identities of G. Then, $e_1 e_2 = e_2$ since e_1 is an identity, and we have $e_1 e_2 = e_1$ since e_2 is an identity. So we can conclude that $e_1 = e_2$.
2. Let $g \in G$, suppose $a, b \in G$ are inverses of g, then $ga = ag = e$ and $gb = bg = e$. Hence we have $ga = gb$, and so we can multiply the inverse of g:

$$\begin{aligned} & g^{-1}(ga) = g^{-1}(gb) \\ \Rightarrow\ & (g^{-1}g)a = (g^{-1}g)b \\ \Rightarrow\ & ea = eb \\ \Rightarrow\ & a = b \end{aligned}$$

3. Let $g \in G$ and consider g^{-1}. Then $gg^{-1} = g^{-1}g = e$, and this means that $(g^{-1})^{-1} = g$

4. Consider $a, b \in G$, we claim that $(ab)^{-1} = b^{-1}a^{-1}$. Since

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

and

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}eb \\ &= b^{-1}b \\ &= e\end{aligned}$$

We can conclude that $(ab)^{-1} = b^{-1}a^{-1}$

□

Theorem 1.10. Let G be a group, and let $a, b, c \in G$, we have the following properties

1. if $ab = ac$ then $b = c$ since we can multiply a^{-1} to left on both sides
2. if $ba = ca$ then $b = c$ since we can multiply b^{-1} to right on both sides

Notation: Let G be a group:

1. By associativity, if $a_1, a_2, ..., a_n \in G$, then $a_1a_2...a_n$ is well-defined, and we do not need to write brackets there.
2. let $g \in G, n \in \mathbb{N}$, then $g^n = gg \cdots g$ for n times. And $g^{-n} = g^{-1}g^{-1} \cdots g^{-1}$ for n times.
3. If G is a group under $+$, then we write $ng = g + g + \cdots g$ for n times.

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 2: September 15

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

2.3 Special Types

Definition 2.11. We say G is **finite** if the set G has finitely many elements. We denote the **order (cardinality/size)** of G by $|G|$. If G is not finite, we say G is **infinite**, and write $|G| = \infty$

Example 2.12. Example of finite/infinite groups:

- $\mathbb{Z}_n$ is finite. $|\mathbb{Z}_n| = n$
- $\mathbb{Z}_n^\times$ is finite. $|\mathbb{Z}_n^\times| = |\{a \in \mathbb{Z}_n | \gcd(a, n) = 1\}| = \varphi(n)$, which is the Euler phi-function.
- let p be a prime. $GL_2(\mathbb{Z}_p)$ is finite. To compute $|GL_2(\mathbb{Z}_p)|$, recall that a matrix is invertible if and only if its columns are linearly independent. So, we need to count how many linearly independent columns there can be. For the first column, it just has to be non-zero. So we have $p^2 - 1$ of them. For the second column, there are p^2 of possible columns, and p of them are linearly dependent to the first column, so there are $p^2 - p$ choices for the second column. Hence, $|GL_2(\mathbb{Z}_p)| = (p^2 - 1)(p^2 - p) = (p + 1)(p - 1)p(p - 1) = p(p + 1)(p - 1)^2$

Definition 2.13. We say G is **abelian** if $ab = ba$ for all $a, b \in G$.

Example 2.14. Example of abelian groups:

- $\mathbb{Z}, \mathbb{R}^\times, \mathbb{Q}^\times, \mathbb{C}^\times, \mathbb{Z}_n, \mathbb{Z}_n^\times, M_n(\mathbb{R})$ are all abelian groups with addition.
- $GL_n(\mathbb{R}), GL_n(\mathbb{Z}_p), GL_n(\mathbb{C}), GL_n(\mathbb{Q})$ are all non-abelian groups with addition for $n > 1$.
- D_4 is not abelian.
- S_3 is not abelian.

2.4 Direct Products

Definition 2.15. Let G, H be groups. The **direct product** of G and H is the group with the underlying set

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

and the operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

Note that $g_1 g_2$ uses the operation with G, and $h_1 h_2$ uses the operation with H.

Example 2.16. Example of direct product

- Let $G = \mathbb{R}^\times \times \mathbb{Z}_{12}$. For this group, $e = (1, 0)$. Consider $(4, 8) \cdot (3, 5) = (12, 1)$

Definition 2.17. More generally, if $G_1, G_2, ..., G_n$ are groups, then we may define the **direct product**

$$G_1 \times G_2 \times ... \times G_n = \{(g_1, g_2, ..., g_n) : g_i \in G_i\}$$

similarly.

For **Infinite Direct Products**: Suppose $G_1, G_2, ...$ is an infinite collection of groups. What do elements of $\Pi_{i=1}^{\infty} G_i = G_1 \times G_2 \times ...$ look like? They would be $(g_1, g_2, ...)$ where $g_i \in G_i$. If the groups cannot be indexed by $\mathbb{N}$, then we can design an index set I. For all $i \in I$, G_i is a group. Take $i \in I$, but we can think of putting groups into a spot, which is indexed by i, so we can design a function of i such that $f(i) \in G_i$.

Definition 2.18. Let I be an index set. For each $i \in I$, let G_i be a group. The **direct product** of the G_i's is the set of functions

$$\Pi_{i \in I} G_i = \{f : I \to \cup_{i \in I} G_i \mid \forall i \in I, f(i) \in G_i\}$$

equipped with the operation $(f \cdot g)(i) = f(i) \cdot g(i)$ for all $i \in I$.

The above definition means that, for a $f \in \Pi_{i \in I} G_i$, then f is the function that fills in the blanks.

2.5 Subgroups

Let G be a group, and let $H \subseteq G$. Which group axioms does H inherit from G?

1. **Associativity** $\forall a, b, c \in H, (ab)c = a(bc)$

2. **Identity** $e \in H$? No. Consider $\mathbb{N} \subseteq \mathbb{Z}$
3. **Inverses** $g \in H \Rightarrow g^{-1} \in H$? No. Consider $\mathbb{N} \cup \{0\} \subseteq \mathbb{Z}$
4. **Closure** $\forall a, b \in H, ab \in H$? Consider $\{\text{odd numbers}\} \subseteq \mathbb{Z}$

Definition 2.19. Let G be a group, and let $H \subseteq G$. We say H is a **subgroup** of G if H forms a group via the operation of G. If H is subgroup of G, we say $H \leq G$.

Theorem 2.20. Subgroup Test

Let G be a group, and let $H \subseteq G$. If

1. $e \in H$
2. $a, b \in H \Rightarrow ab \in H$
3. $a \in H \Rightarrow a^{-1} \in H$

Then $H \leq G$

The trick to verify the second and the third point together is to check that $\forall a, b \in H$, $ab^{-1} \in H$.

2.6 Examples

Example 2.21. Example of Subgroups

- $H = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a = 0\} \subseteq GL_2(\mathbb{R})$? No. Since $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin H$
- $H = \{A : \det(A) \in \mathbb{Z}\} \subseteq GL_2(\mathbb{R})$ No since the inverse of A does not guarantee to have integer entries.
- $H = \{x : x \text{ is irrational}\} \cup \{1\} \subseteq \mathbb{R}^\times$. It is not closed. Consider $\sqrt{2} \in H$, but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$
- $H = \{x : |x| = 1\} \subseteq \mathbb{C}^\times$. We claim that $H \leq \mathbb{C}^\times$. $e = 1$ is trivial. Take $x, y \in H$, then $|xy^{-1}| = |x| \cdot \frac{1}{|y|} = 1 \cdot \frac{1}{1} = 1$, and so $xy^{-1} \in H$. By the subgroup test, we have $H \leq \mathbb{C}^\times$

Definition 2.22. Special Linear Group: $SL_n(\mathbb{R}) = \{A : \det(A) = 1\} \subseteq GL_n(\mathbb{R})$

Theorem 2.23. $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

Proof 2.24. Since $\det(I) = 1, I \in SL_n(\mathbb{R})$. Let $A, B \in SL_n(\mathbb{R})$. Then

$$\det(AB^{-1}) = \det(A) \cdot \frac{1}{\det(B)} = 1$$

and so $AB^{-1} \in SL_n(\mathbb{R})$. By the subgroup test, $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ □

Definition 2.25. Let G be a group. We define the **center** of G by

$$Z(G) = \{x \in G : \forall y \in G, xy = yx\}$$

Theorem 2.26. Let G be a group. $Z(G) \leq G$

Proof 2.27. since for all $g \in G$,

$$eg = ge = g$$

. $e \in Z(G)$. Let $a, b \in Z(G)$, then, let $g \in G$ be arbitrary. Note that $bg = gb \Rightarrow g = b^{-1}gb \Rightarrow gb^{-1} = b^{-1}g$. Finally,

$$\begin{aligned}(ab^{-1})g &= a(b^{-1}g) \\ &= a(gb^{-1}) \\ &= (ag)b^{-1} \\ &= (ga)b^{-1} \\ &= g(ab^{-1})\end{aligned}$$

and so $ab^{-1} \in Z(G)$. By the subgroup test, $Z(G) \leq G$. □

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 3: September 22

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

3.7 Order

Definition 3.28. Let G be a group, and let $g \in G$. The **order** of g, $|g|$, is the least positive integer such that $g^{|g|} = e$. If no such positive integer exists, then we say g has infinite order and write $|g| = \infty$.

Theorem 3.29. Properties of Order:

1. Let G be a group, and let $g \in G$. If there is $m, n \in \mathbb{Z}$ such that $g^m = e, g^n = e$, then $g^d = e$ where $d = \gcd(m, n)$.
2. Recall the division algorithm from MATH135: Let $a, b \in \mathbb{Z}$ with $b \neq 0$, there exists unique $q, r \in \mathbb{Z}$ such that
   (a) $a = bq + r$
   (b) $0 \leq r < |b|$

   So, let G be a group, and let $g \in G$. If $m \in \mathbb{N}$ such that $g^m = e$, then $|g| < \infty$ and $|g|$ divides m.
3. Let G be a group, and let $g \in G$, $|g| = n < \infty$. For $m \in \mathbb{N}$,
$$|g^m| = \frac{n}{\gcd(m, n)}$$

Proof 3.30. For (1), this is because there exists $x, y \in \mathbb{Z}, d = mx + ny$, so $g^d = g^{mx+ny} = (g^m)^x (g^n)^y = ee = e$

For (2), suppose $m \in \mathbb{N}$ such that $g^m = e$. By the division algorithm, there eixsts $q, r \in \mathbb{Z}$ such that $m = |g|q + r$ and $0 \leq r < |g|$, and we want to show $r = 0$. Note that $g^r = g^{m-|g|q} = g^m (g^{|g|})^{-q} = ee = e$. Since $|g|$ is the **smallest positive** integer such that $g^{|g|} = e$, we have $r = 0$.

For (3), suppose $h = g^m \in G$, and $d = \gcd(m, n)$. We show $|h| = \frac{n}{d}$. Let $a, b \in \mathbb{Z}$ such that $n = da$ and $m = db$. Thus, we must show that
$$|h| = a$$

. We have

$$\begin{aligned} h^a &= g^{ma} = g^{dba} \\ &= g^{nb} = g^e \end{aligned}$$

By the previous result, $|h|$ divides a. Secondly, let $k = |h|$, so that $g^{mk} = h^k = e$, and so

$$\begin{aligned} &|g| \mid mk \\ \Rightarrow\ &n \mid mk \\ \Rightarrow\ &da \mid dbk \end{aligned}$$

Now, $d = \gcd(m, n)$, and so $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$, i.e. $\gcd(b, a) = 1$.

Finally, we have

$$\begin{aligned} &da \mid dbk \\ \Rightarrow\ &a \mid bk \\ \Rightarrow\ &a \mid k \text{ because } \gcd(a, b) = 1 \\ \Rightarrow\ &a \mid |h| \end{aligned}$$

Since $a, |h| \in \mathbb{N}$, $a = |h|$ □

3.8 Cyclic Group

Definition 3.31. Let G be a group, $S \subseteq G$ be a subset. Then, the subgroup generated by S is defined as

$$\langle S \rangle = \bigcap \{H \leq G : S \subseteq H\}$$

is the smallest subgroup of G which contains S.

The special case for the above definition is that $g \in G$, $S = \{g\}$, we write that

$$\langle g \rangle := \langle S \rangle$$

which lead us to the following definition

Definition 3.32. Let G be a group, $g \in G$, we call $\langle g \rangle$ the **cyclic subgroup** of G **generated by** g

Theorem 3.33. **Properties of cyclic group**: Let G be a group, $g \in G$, then $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$

Proof 3.34. Let $H = \{g^n : n \in \mathbb{Z}\}$. In assignment 1, we show that $H \leq G$. Now, we have $g \in H$, $\langle g \rangle \subseteq H$. Moreover, $g \in \langle g \rangle$ and so $g^n \in \langle g \rangle, \forall n \in \mathbb{Z}$. Hence, $H \subseteq \langle g \rangle$ □

Remark: if the operation of G is plus (addition), then $\langle g \rangle = \{ng : n \in \mathbb{Z}\}$.

Also, remark that if G is a group, $g \in G$, $|g| = n < \infty$, then $\langle g \rangle = \{g^m : m \in \mathbb{Z}\} = \{e, g, g^2, ..., g^{n-1}\}$. In particular, $|\langle g \rangle| = |g|$.

Example 3.35. If $G = \mathbb{Z}$, then $\langle 2 \rangle = \{2n : n \in \mathbb{Z}\}$. $\langle k \rangle = \{kn : n \in \mathbb{Z}\}$.

If $G = \mathbb{R}^\times \times \mathbb{R}^\times$, then $\langle (1,2) \rangle = \{(1,2)^n : n \in \mathbb{Z}\} = \{(1, 2^n) : n \in \mathbb{Z}\}$.

If $G = D_4$, then $\langle r \rangle = \{e, r, r^2, r^3\}$, $\langle s_1 \rangle = \{e, s_1\}$

If $G = \mathbb{Z}_n$, then $\langle 1 \rangle = \{0, 1, 2, ..., n-1\} = \mathbb{Z}_n$.

Definition 3.36. Let G be a group. We say G is **cyclic** if there exists $g \in G$ such that

$$G = \langle g \rangle$$

, we call g a generator of G.

Example 3.37. For example, $\mathbb{Z}_n = \langle 1 \rangle$, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

If $G = \mathbb{Z}_4$, then $\langle 1 \rangle = \mathbb{Z}_4, \langle 2 \rangle = \{0, 2\}, \langle 3 \rangle = \{0, 3, 2, 1\} = \mathbb{Z}_4$.

S_3, D_4 are not cyclic.

Theorem 3.38. If a group G is cyclic, then G is abelian.

Example 3.39. Prove that $(\mathbb{Q}, +)$ is not cyclic.

Proof: For contradiction, suppose $\mathbb{Q} = \langle q \rangle, q \in \mathbb{Q}$. Then there exists $n \in \mathbb{Z}$ such that $\frac{1}{2}q = nq \Rightarrow q = 0$ or $\frac{1}{2} = n$. Thus, $q = 0$, and so $\mathbb{Q} = \langle 0 \rangle = \{0\}$. Contradiction □

3.9 Properties of Cyclic Groups

Theorem 3.40. Let $G = \langle x \rangle$ be a cyclic group:

1. If $|x| = \infty$, then $G = \langle x^k \rangle$ if and only if $k = \pm 1$.
2. If $|x| = n < \infty$, then $G = \langle x^k \rangle$ if and only if $\gcd(n, k) = 1$.
3. Every Subgroup of a cyclic group is cyclic.

Proof 3.41. For (1), Suppose $|x| = \infty$. Easily, $G = \langle x \rangle = \langle x^{-1} \rangle$. Assume $G = \langle x^k \rangle$. Since $x \in G$, there exists $n \in \mathbb{Z}$ such that $x = (x^k)^n$, so $x = x^{kn}$. So $e = x^{kn-1}$.

Since $|x| = \infty$, $kn - 1 = 0$. Thus $kn = 1$, and so $k = \pm 1$

For (2). Suppose $|x| = n < \infty$. For $k \in \mathbb{Z}$, $\langle x^k \rangle \subseteq \langle x \rangle = G$, and so

$$\begin{aligned} & \langle x^k \rangle = \langle x \rangle \\ \Leftrightarrow\ & |x^k| = |x| \\ \Leftrightarrow\ & \frac{n}{\gcd(n,k)} = n \\ \Leftrightarrow\ & \gcd(n,k) = 1 \end{aligned}$$

For (3), Let $G = \langle x \rangle$ be a cyclic group. Let $H \leq G$. If $H = \{e\} = \langle e \rangle$, we are done.

Suppose $H \neq \{e\}$, choose $k \in \mathbb{N}$ minimal such that $x^k \in H$. We claim that $H = \langle x^k \rangle$. To see that, take $x^m \in H$, $m \in \mathbb{Z}$. By the division algorithm, there exists $q, r \in \mathbb{Z}$ such that $m = kq + r$, $0 \leq r < k$. Now, $x^r = x^{m-kq} = x^m (x^k)^{-q} \in H$.

Since $r < k$, by minimality of k, we have $r = 0$. So $x^m = x^{kq} \in \langle x^k \rangle$. So, $H \subseteq \langle x^k \rangle$. However, $\langle x^k \rangle \subseteq H$. So $H = \langle x^k \rangle$ □

Definition 3.42. For $n \in \mathbb{N}$,

$$\varphi(n) = |\{1 \leq k \leq n : \gcd(n, k) = 1\}|$$

is called the **Euler φ-function**.

Theorem 3.43. If $n, m \in \mathbb{N}$ with $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Corollary 3.44. If $G = \langle x \rangle$, $|x| = n < \infty$, then the number of generators of G is $\varphi(n)$.

Theorem 3.45. Let $G = \langle x \rangle$ be a cyclic group of order $n < \infty$. For every $d \in \mathbb{N}$ with $d \mid n$, there is a unique subgroup of G of order d. Moreover, these are all subgroups of G.

Proof 3.46. Proof of the above theorem:

1. Existence: suppose $d \in \mathbb{N}$, $d \mid n$. Let $m = \frac{n}{d} \in \mathbb{N}$. Then $\langle x^m \rangle \leq \langle x \rangle$ and
$$\begin{aligned} |\langle x \rangle| &= |x^m| \\ &= \frac{n}{\gcd(m,n)} \\ &= \frac{n}{m} \text{ since } m|n \\ &= d \end{aligned}$$

2. Uniqueness: Let $\langle x^k \rangle, k \in \mathbb{N}$ be a subgroup of G of order d (d is as above). We show $\langle x^k \rangle = \langle x^{\frac{n}{d}} \rangle$. Since $|x^k| = d$,
$$\begin{aligned} d = |x^k| &= \frac{n}{\gcd(n,k)} \\ \Rightarrow \frac{n}{d} &= \gcd(n,k) \\ \Rightarrow \frac{n}{d} &\mid k \\ \Rightarrow k &= \frac{n}{d}\ell, \ell \in \mathbb{N} \\ \Rightarrow \langle x^k \rangle &\subseteq \langle x^{\frac{n}{d}} \rangle \\ \Rightarrow \langle x^k \rangle &= \langle x^{\frac{n}{d}} \rangle \text{ since they are of equal size} \end{aligned}$$

3. Have we found them all? Let $H \leq G$. From above, $H = \langle x^k \rangle, k \in \mathbb{N}$. Then, $|H| = |x^k| = \frac{n}{\gcd(n,k)} \mid n$

□

Example 3.47. Let $G = \mathbb{Z}_{40} = \langle 1 \rangle$.

1. Compute $|12|$. $|12| = |12 \cdot 1| = \frac{40}{\gcd(12,40)} = 10$
2. How many generators does G have? List them. $\varphi(40) = \varphi(8) \times \varphi(5) = 4 \times 4 = 16$. $\{1, 3, 7, 9, ...\}$
3. Draw the subgroup lattice of G.

Order	Generator
1	0
2	20
4	10
8	5
5	8
10	4
20	2
40	1

Omit the lattice graph.

Example 3.48. Let $G = \mathbb{Z}_{18}^{\times}$.

1. Compute $|G|$. $|G| = \varphi(18) = \varphi(2) \times \varphi(9) = 1 \times 6 = 6$.
2. Prove that G is cyclic. Consider $5^0 = 1, 5^1 = 5, 5^2 = 7, 5^3 = 17, 5^4 = 13, 5^5 = 11, 5^6 = 1$, $|G| = 6$, $|5| = 6$, so $G = \langle 5 \rangle$
3. Compute the order of 7. Notice that $7 = 5^2$, so $|7| = \frac{6}{\gcd(6,2)} = 3$
4. List all subgroups of G.

Order	Generator
1	1
2	$\langle 5^3 \rangle = \langle 17 \rangle$
3	$\langle 5^2 \rangle = \langle 7 \rangle$
6	$\langle 5 \rangle$

5. List all generators of G. 5^k, $1 \leq k \leq 6$, $\gcd(k, 6) = 1$. So $5^1, 5^5 = 11$

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 4: September 29

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

4.10 Symmetric Groups

Definition 4.49. Let $n \in \mathbb{N}$,

$$S_n = \{ \text{ bijections on } \{1, 2, ..., n\}\}$$

. The operation is function composition. The elements of S_n are called **permutations**.

Example 4.50. We will use this example to illustrate **disjoint cycle form**. Consider $\sigma \in S_6$ given by $1 \mapsto 6, 2 \mapsto 5, 3 \mapsto 1, 4 \mapsto 4, 5 \mapsto 2, 6 \mapsto 3$. This painful to write. If n gets larger, then it would be infeasible to write all maps down.

For this example, we will write $(163)(25)(4)$. Conventionally, we can omit the self-mapped elements. So $(163)(25)(4) = (163)(25)$

Definition 4.51. An m-cycle in $S_n (m \leq n)$ is a permutation of the form $(a_1 a_2 \cdots a_m) \in S_n$, wherw $a_i \neq a_j$ for $i \neq j$

For example, in S_5, (143) is a 3-cycle.

The disjoint cycle form uses shorter notaiton. More importantly, it works well with composition, order, and inverses.

Example 4.52. $\alpha = (135)(24)$ and $\beta = (15)(34) \in S_5$. Then

$$\begin{aligned} \alpha\beta &= (135)(24)(15)(34) \text{ read from right to left} \\ &= (1)(2453) \\ &= (2453) \end{aligned}$$

Similarly,

$$\begin{aligned}\beta\alpha &= (15)(34)(135)(24) \text{ read from right to left}\\ &= (1423)(5)\\ &= (1423)\end{aligned}$$

For inverses

$$\begin{aligned}\alpha^{-1} &= [(135)(24)]^{-1}\\ &= (24)^{-1}(135)^{-1}\\ &= (24)(531)\\ &= (24)(153)\end{aligned}$$

In general, we have $(a_1a_2\cdots a_m)^{-1} = (a_m a_{m-1}\cdots a_1)$

Definition 4.53. A 2-cycle is called a **transposition**.

Theorem 4.54. Let $n \geq 2$. Every $\sigma \in S_n$ can be written as a product of transpositions.

Proof 4.55. Since σ can be written as a product of disjoint cycles, it is enough to realize that $(a_1a_2\cdots a_m) = (a_1a_m)(a_1a_{m-1})\cdots(a_1a_3)(a_1a_2)$.

For example

$$\begin{aligned}\sigma &= (135)(24)\\ &= (15)(13)(24)\end{aligned}$$

□

This decomposition is NOT unique. For example, $(12) = (34)(12)(34)$.

4.11 Order in S_n

Example 4.56. $\alpha = (145), \beta = (23) \in S_5$. Then

$$\begin{aligned}\beta\alpha &= (23)(145)\\ &= (145)(23)\\ &= \alpha\beta\end{aligned}$$

In general, disjoint cycles commute, since elements don't touch each other. However $(12)(13) = (132)$, but $(13)(12) = (123)$.

Lemma 4.57. If $\delta = (a_1 a_2 \cdots a_m) \in S_n$ is a m-cycle, then $|\sigma| = m$.

Theorem 4.58. Suppose $\sigma \in S_n$ is a product of disjoint cycles

$$\sigma = \alpha_1\alpha_2\cdots\alpha_k$$

Then

$$|\sigma| = \ell cm(|\alpha_1|, |\alpha_2|, ..., |\alpha_k|)$$

Proof 4.59. Let $N = \ell cm(|\alpha_1|, |\alpha_2|, ..., |\alpha_k|)$. Since the d_i's are disjoint,

$$\begin{aligned}\sigma^N &= (\alpha_1\alpha_2\cdots\alpha_k)^N\\ &= \alpha_1^N\alpha_2^N\cdots\alpha_k^N\\ &= e\cdot e\cdots e\\ &= e\end{aligned}$$

Therefore $|\sigma| \mid N$ ($|\sigma| \leq N$). Now,

$$e = \sigma^{|\sigma|} = \alpha_1^{|\sigma|}\alpha_2^{|\sigma|}\cdots\alpha_k^{|\sigma|}$$

Since the α_i;s are disjoint, then $\alpha_i^{|\sigma|} = e$ for each $i = 1, 2, ..., k$. We therefore have that $|\alpha_i| \mid |\sigma|$ for all $i = 1, 2, ..., k$.

So, $|\sigma|$ is a common multiple of the $|\alpha_i|$'s. So $N \leq |\sigma|$. So $N = |\sigma|$.

□

Example 4.60. Let's say we have

$$\begin{aligned}\alpha &= (1425)(36)\\ \beta &= (65)(324)\end{aligned}$$

What is $(\alpha\beta)^{62}[1]$, i.e. what does this map does to 1?

First, compute

$$\begin{aligned}\alpha\beta &= (1425)(36)(65)(324)\\ &= (146)(2)(35)\\ &= (146)(35)\end{aligned}$$

So, $|\alpha\beta| = \ell cm(3,2) = 6$. So $(\alpha\beta)^{62} = (\alpha\beta)^2 = (146)(35)(146)(35) = (164)(2)(3)(5) = (164)$.

So $(\alpha\beta)^{62}[1] = 6$.

4.12 Parity

Fix $n \geq 2$, consider the polynomial

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

In the variables $x_1, x_2, ..., x_n$.

For $\sigma \in S_n$, we define

$$\sigma(\Delta) := \Pi_{i<j}(x_{\sigma(i)} - x_{\sigma(j)})$$

and $\sigma(-\Delta) := -\sigma(\Delta)$. Observe that $\sigma(\Delta) \in \{\Delta, -\Delta\}$

Definition 4.61. Let $\sigma \in S_n$, $n \geq 2$, The **sign** of σ is defined to be

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

Definition 4.62. Let $\sigma \in S_n, n \geq 2$, we say σ is **even** if and only if $sgn(\sigma) = 1$ and **odd** if and only if $sgn(\sigma) = -1$.

Example 4.63. In S_3, $\Delta = (x_1 - x_2)(x_2 - x_3)(x_2 - x_3)$. And let's say we have $\sigma = (12)$. We have $\sigma(\Delta) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta$. So $sgn(\sigma) = -1$ and σ is odd.

However, computing Δ would be too time-consuming for large n. So we will find some efficient way to do so.

Theorem 4.64. Fix $n \geq 2$, for $\sigma, \tau \in S_n$,

$$sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$$

Proof 4.65. Consider

$$\begin{aligned}(\sigma\tau)(\Delta) &= \sigma(\tau(\Delta)) \\ &= \sigma(sgn(\tau)\Delta) \\ &= sgn(\tau)\sigma(\Delta) \\ &= sgn(\tau)sgn(\sigma)(\Delta)\end{aligned}$$

So $sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$ □

Lemma 4.66. Fix $n \geq 2$, a transposition $\sigma = (ab) \in S_n$ is odd.

Proof 4.67. Say $a < b$. σ would swap the sign of

$$\begin{gathered}(x_a - a_{a+1})(x_{a+1} - a_b) \\ (x_a - a_{a+2})(x_{a+2} - a_b) \\ \cdots\cdots \\ (x_a - a_{b-1})(x_{b-1} - a_b) \\ (x_a - x_b)\end{gathered}$$

So there are odd number of signes swapped, so the transposition $\sigma = (ab) \in S_n$ is odd. □

Corollary 4.68. Fix $n \geq 2$, Let $\sigma \in S_n$ be written as a product of transpositions

$$\sigma = \alpha_1\alpha_2 \cdots \alpha_k$$

Then

- σ is odd if and only if k is odd
- σ is even if and only if k is even

Proof 4.69. Let's say $\sigma = \alpha_1\alpha_2\cdots\alpha_k$, then

$$\begin{aligned} sgn(\sigma) &= sgn(\alpha_1)\cdots sgn(\alpha_k) \\ &= (-1)^k \end{aligned}$$

□

Example 4.70. In S_5,

$$\begin{aligned} \sigma &= (153)(24) \\ &= (13)(15)(24) \end{aligned}$$

So σ is odd.

We should see that transpositions are odd. A m-cycle $(a_1a_2\cdots a_m) = (a_1a_m)(a_1a_{m-1})\cdots(a_1a_3)(a_1a_2)$ has $m-1$ transpositions. So $sgn(m\text{-cycle}) = (-1)^{m-1}$. So this m-cycle is odd if and only if m is even, and vice versa.

4.13 Dihedral Groups

Definition 4.71. For $n \geq 3$, we let D_n denote the group of symmetries of the regualar n-gon. We call these grousp **dihedral groups**.

We would try to be able to work with D_n without drawing the n-gons out. We may visualize D_n as a subset of S_n by the following correspondence.

Example 4.72. We have D_4. Mark the four vertices as $\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$.

Then, for $g \in D_4$, and $i \in \{1,2,3,4\}$, we let $\sigma(i)$ denote the vertex number i appears after performing $g\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$

- r "=" (1234) is the 90 degree counter-clockwise rotation
- $r^2 = (13)(24)$.
- $s_1 = (24)$
- $v = (12)(34)$

Example 4.73. For D_5 we have

- $r = (12345)$ is the 72 degree counter-clockwise rotation
- $r^2 = (13524)$
- $r^2 = (14523)$
- s_i is the reflection over the line through the ith vertex which bisects the angle.
- $s_4 = (12)(35)$

Example 4.74. Consider D_4 and let $s = s_1$.

- $rs = (1234)(24) = (12)(34) = V$
- $r^2s = (13)(24)(24) = (13) = s_2$
- $r^3s = (1432)(24) = (14)(23) = H$
- $sr^{-1} = (24)(4321) = (12)(34) = rs$ or $sr = r^{-1}s$

Hence, we can rewrite $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Also note that

$$sr = r^{-1}s$$

$$sr^i = r^{-i}s$$

Example 4.75. Consider D_5 and let $s = s_1$.

- $rs = (12345)(25)(34) = (12)(35) = s_4$
- $r^2s = (12345)(12)(35) = (13)(45) = s_2$
- $r^3s = (12345)(13)(45) = (14)(23) = s_5$
- $r^4s = (12345)(14)(23) = (15)(24) = s_3$
- $sr^{-1} = (25)(34)(54321) = (12)(35) = rs$ or $sr = r^{-1}s$

Hence, we can rewrite $D_5 = \{e, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$. Also note that

$$sr^{-1} = rs$$

$$sr = r^{-1}s$$

$$sr^i = r^{-i}s$$

In general, $D_n = \{e, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., r^{n-1}s\}$ so that $|D_n| = 2n$. Moreover, $rs = sr^{-1}$.

Now we can work with D_n by using r's s's and $rs = sr^{-1}$ to perform group operations.

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 5: October 6

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

5.14 Homomorphism

We want to discuss functions $f : G \to H$ between groups which convet useful group theoretic information between G and H.

Definition 5.76. A function $\varphi : G \to H$ is called a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. Equivalently, this means that homomorphism preserve the group operation.

Example 5.77. Examples of Homomorphisms:

- $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^\times$. In particular, $\varphi(A) = \det A$, $\varphi(AB) = \det(AB) = \det(A)\det(B) = \varphi(A)\varphi(B)$.
- $\varphi : \mathbb{Z} \to \mathbb{Z}_n$. In particular, $\varphi(a) = [a]$, $\varphi(a + b) = [a + b] = [a] + [b] = \varphi(a) + \varphi(b)$.
- $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$. In particular, $\varphi(z) = |z|$, $\varphi(zw) = |zw| = |z| \cdot |w| = \varphi(z)\varphi(w)$.
- $\varphi : \mathbb{C} \to \mathbb{C}$. In particular, $\varphi(z) = \overline{z}$, $\varphi(z + w) = \overline{z + w} = \overline{z} + \overline{w} = \varphi(z) + \varphi(w)$.
- Let $C_2 = \{-1, 1\} \leq \mathbb{C}^\times$. $\varphi S_n \to C_2$. In particular, $\varphi(\sigma) = sgn(\sigma)$, $sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$
- Let $V = \mathbb{R}^n$. $GL(v) = \{T : v \to v \mid T \text{ is invertible and linear}\}$, a group under composition. $\varphi : GL(v) \to GL_n(\mathbb{R})$. In particular, $\varphi(T) = [T]_\beta$, where β is the standard basis of $\mathbb{R}^n$. Then, $[T \circ U]_\beta = [T]_\beta[u]_\beta$. So $\varphi(T \circ U) = \varphi(T) \cdot \varphi(U)$.
- $\varphi : \mathbb{Z}_3 \to \mathbb{Z}_6$, and we define $\varphi(a) = a$. It appears that $\varphi(a + b) = a + b = \varphi(a) + \varphi(b)$. However, $3 = 6$ in $\mathbb{Z}_3$, so $\varphi(3) = 3$, $\varphi(6) = 0$, so φ is not well-defined.

5.15 Properties of Homomorphisms

Theorem 5.78. **Properties of Homomorphisms**: Let G, H be groups. Let $\varphi : G \to H$ be a homomorphism.

1. $\varphi(e_g) = e_H$.
2. for all $g \in G$, $\varphi(g)^{-1} = \varphi(g^{-1})$.

Proof 5.79. Prove each as follows:

1. Observe that $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. So $e_H = \varphi(e_G)$ by multiplying both sides by $\varphi(e_G)^{-1}$.
2. For $g \in G$, $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H$, and similarly $\varphi(g^{-1})\varphi(g) = e_H$. So $\varphi(g)^{-1} = \varphi(g^{-1})$.

□

Theorem 5.80. Let G, H be groups. Let $\varphi : G \to H$ be a homomorphism. Let $A \leq G, B \leq H$. Then:

1. The **image** of A under φ is defined as follows: $\varphi(A) := \{\varphi(a) : a \in A\}$ is a subgroup of H.
2. The **pre-image** of B under φ is defined as follows: $\varphi^{-1}(B) := \{g \in G : \varphi(g) \in B\}$ is a subgroup of G.

Proof 5.81. Prove each as follows:

1. Post on Piazza.
2. Since $e_H \in B$, and $\varphi(e_G) = e_H$, we have $e_G \in \varphi^{-1}(B)$.
   Now, let $g_1, g_2 \in \varphi^{-1}(B)$. Thus, $\varphi(g_1), \varphi(g_2) \in B$ since $B \leq H$, $\varphi(g_2)^{-1} = \varphi(g_2^{-1}) \in B$.
   Thus, $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) \in B$. Hence, $g_1 g_2^{-1} \in \varphi^{-1}(B)$, and so $\varphi^{-1}(B) \leq G$ by the **Subgroup Test**.

□

Theorem 5.82. Let G, H be groups. Let $\varphi : G \to H$ be a homomorphism. The Kernel of φ, which is defined as follows:

$$\ker \varphi := \{g \in G : \varphi(g) = e\}$$

is a subgroup of G.

Proof 5.83. Since $\varphi(e) = e, e \in \ker\varphi$. Note these two es are different, one is in G and one is in H.

Let $a, b \in \ker\varphi$, so that $\varphi(a) = \varphi(b) = e$. Moreover, $\varphi(b^{-1}) = \varphi(b)^{-1} = e^{-1} = e$. Thus, $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = ee = e$. So $ab^{-1} \in \ker\varphi$. By subgroup test, $\ker\varphi$ is a subgroup of G. □

5.16 Isomorphism

Recall several definitions:

Definition 5.84. A function $f : A \to B$ is **injective** (**one-to-one**) if $f(a) = f(b)$ implies $a = b$ for all $a, b \in A$.

Definition 5.85. A function $f : A \to B$ is **surjective** (**onto**) if for all $b \in B$, there exists $a \in A$ such that $f(a) = b$ (i.e. if $f(A) = B$).

Definition 5.86. A function $f : A \to B$ is **bijective** (**invertible**) if it is both injective and surjective

Definition 5.87. Let G, H be groups. Let $\varphi : G \to H$ be a homomorphism.

1. If φ is injective, we call φ an **embedding**.
2. If φ is bijective, we call φ an **isomorphism**.

Definition 5.88. Let G, H be groups. If there exists an isomorphism $\varphi : G \to H$, then we say G and H are isomorphic, and we write $G \cong H$.

Theorem 5.89. Let $\varphi : G \to H$ be a homomorphism. Then φ is an embedding if and only if $\ker\varphi = \{e\}$.

Proof 5.90. $\Rightarrow$: Suppose φ is an embedding, and let $g \in \ker\varphi$. Then $\varphi(g) = e = \varphi(e)$, so $g = e$.

$\Leftarrow$: Suppose $\ker\varphi = \{e\}$, then for $a, b \in G$, if $\varphi(a) = \varphi(b)$, then $\varphi(a)\varphi(b)^{-1} = e$, and then $\varphi(a)\varphi(b^{-1}) = e$, so $\varphi(ab^{-1}) = e$. So, $ab^{-1} \in \ker\varphi = \{e\}$. Hence, $ab^{-1} = e$, and as a result $a = b$. □

Theorem 5.91. Let $\varphi : G \to H$ be a embedding.

1. For all $g \in G$, $|\varphi(g)| = |g|$
2. If $A \subseteq G$ is finite, then $|\varphi(A)| = |A|$.

Proof 5.92. Prove each as follows:

1. Case I: If $|g| = \infty$, then for contradiction, suppose $|\varphi(g)| \neq \infty$, then $|\varphi(g)| = n < \infty$. Then, $\varphi(g)^n = \varphi(g^n) = e$. Since φ is injective, then $g^n = e$, contradiction.

   Case II: Let $|g| = n < \infty$. Then, $\varphi(g)^n = \varphi(g^n) = \varphi(e) = e$, and so $|\varphi(g)| < \infty$.

   Let $|\varphi(g)| = m < \infty$. Since $\varphi(g)^n = e$, we have $m \mid n$. Moreover, we have that $\varphi(g^m) = \varphi(g)^m = e$, and since φ is injective, $g^m = e$. Therefore, we have that $n \mid m$. And so, $m = n$, as required.
2. Post on Piazza.

□

Theorem 5.93. Let $\varphi : G \to H$ be a surjective homomorphism.

1. If G is abelian, then H is abelian.
2. If G is cyclic, then H is cyclic.
3. Every subgroup of H is of the form $\varphi(A)$, where $A \leq G$.

Proof 5.94. Prove each as follows:

1. Suppose G is abelian. Take $h_1, h_2 \in H$. Since φ is surjective, there exists $g_1, g_2 \in G$ such that

$\varphi(g_1) = h_1$, $\varphi(g_2) = h_2$. So,

$$\begin{aligned} h_1h_2 &= \varphi(g_1)\varphi(g_2) \\ &= \varphi(g_1g_2) \\ &= \varphi(g_2g_1) \\ &= \varphi(g_2)\varphi(g_1) \\ &= h_2h_1 \end{aligned}$$

2. Suppose $G = \langle a \rangle$ is cyclic. Thus, $G = \{a^n : n \in \mathbb{Z}\}$. Take $b \in H$. Then, $\varphi(a^n) = b$ for some $n \in \mathbb{Z}$. Hence, $b = \varphi(a)^n \in \langle \varphi(a) \rangle$.

   So, $\langle \varphi(a) \rangle \subseteq H \subseteq \langle \varphi(a) \rangle$. So, $H = \langle \varphi(a) \rangle$

3. Let $B \leq H$. Consider $A = \varphi^{-1}(B)$. We claim that $\varphi(A) = B$. By definition of $\varphi^{-1}(B)$, we have $\varphi(A) \subseteq B$. For $b \in B$, by surjectivity, there exists $g \in G$ such that $\varphi(g) = b \in B$. Thus, $g \in A$, and so $\varphi(A)$, and so $B \subseteq \varphi(A)$. So, $\varphi(A) = B$ as required.

□

Theorem 5.95. Let $\varphi : G \to H$ be an isomorphism. Then $\varphi^{-1} : H \to G$ is an isomorphism.

Proof 5.96. See homework 2. □

The big picture is that

1. If $G \cong H$, then G and H are the same group, up to relabelling.

   For example, $C_2 = \{-1, 1\}$. If we take $\varphi(C_2) \to \mathbb{Z}_2$ such that $-1 \to 1, 1 \to 0$, which is an isomorphism.

2. If $\varphi : G \to H$ is an embedding, then $\varphi : G \to \varphi(G)$ is an isomorphism. Hence

$$G \cong \varphi(G) \leq H$$

5.17 Examples and Practices

Example 5.97. Are the following pairs of groups isomorphic?

- $\mathbb{Z}_8^\times, \mathbb{Z}_{12}^\times$. $\varphi(8) = 2^3 - 2^2 = 4$, and $\varphi(12) = \varphi(4)\varphi(3) = 2 \cdot 2 = 4$. We will draw out the Cayley Tables. For $\mathbb{Z}_8^\times, \mathbb{Z}_{12}^\times$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

So, if we define $\varphi : \mathbb{Z}_8^\times \to \varphi : \mathbb{Z}_{12}^\times$ as

$$1 \to 1$$
$$3 \to 5$$
$$5 \to 7$$
$$7 \to 11$$

Then, φ is an isomorphism. So $\mathbb{Z}_8^\times$ and $\varphi : \mathbb{Z}_{12}^\times$ are isomorphic.

- $\mathbb{Z}_8^\times, \mathbb{Z}_{10}^\times$. We will draw out the Cayley Tables. For $\mathbb{Z}_8^\times, \mathbb{Z}_{10}^\times$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9		
7	7			
9	9			

We can see that for all $a \in \mathbb{Z}_8^\times$, we have $a^2 = 1$, but we have $3^2 \neq 1$ in $\mathbb{Z}_{10}^\times$. If $\varphi : \mathbb{Z}_8^\times \to \mathbb{Z}_{10}^\times$ was an isomorphism, we would have $\varphi(a)^2 = \varphi(a^2) = \varphi(1) = 1$. Therefore, $\mathbb{Z}_8^\times \ncong \mathbb{Z}_{10}^\times$

- S_4, D_{12}. Note that $|S_4| = 4! = 24$, and $|D_{12}| = 2 \cdot 12 = 24$. Take a look at order 2 elements.

  1. S_4
     (a) (ab). $\binom{4}{2} = 6$.
     (b) $(ab)(cd)$, i.e. disjoint cycles. $\frac{\binom{4}{2}}{2} = 3$.
     So, there are 9 elements of order 2 in S_4.
  2. D_{12} has $s, rs, r^2s, r^3s, ..., r^{11}s$ as order 2 elements. This is true because $(r^is)(r^is) = r^ir^{-i}ss = e$

  So, $S_4 \ncong D_{12}$

- $\mathbb{R}^+ = (0, \infty) \leq \mathbb{R}^\times$, $\mathbb{R}$. $\varphi : \mathbb{R} \to \mathbb{R}^+$. Note that we want $\varphi(a + b) = \varphi(a)\varphi(b)$.
  We can actually take $\varphi(x) = 2^x$. Then, $2^{a+b} = 2^a 2^b$. This is an isomorphism. So $\mathbb{R} \cong \mathbb{R}^+$

- $GL_2(\mathbb{R})$, $\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$. $GL_2(\mathbb{R}) \ncong \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$ since $\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$ is abelian, but $GL_2(\mathbb{R})$ is not.
- $M_2(\mathbb{R})$, $\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$. Homework: to verify that $\varphi : \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R} \to M_2(\mathbb{R})$ such that $\varphi(a,b,c,d) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an isomorphism.
- $\mathbb{Z}, \mathbb{Z}\times\mathbb{Z}$. $\mathbb{Z}$ is cyclic, but $\mathbb{Z}\times\mathbb{Z}$ is not cyclic. So, $\mathbb{Z} \ncong \mathbb{Z}\times\mathbb{Z}$
- $\mathbb{Q}^\times, \mathbb{Z}\times\mathbb{Z}$. In $\mathbb{Z}\times\mathbb{Z}$, $n(a,b) = (0,0)$ if and only if $(na,nb) = (0,0)$ if and only if $(a,b) = (0,0)$. However, $(-1)^2 = 1$. And so, $\mathbb{Q}^\times \ncong \mathbb{Z}\times\mathbb{Z}$

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 6: October 20

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

6.18 Motivation

Example 6.98. Consider $G = \mathbb{Z}, H = \langle n \rangle$. To construct $\mathbb{Z}_n$, we consider $a, b \in \mathbb{Z}$ "equal" if and only if $a \equiv b \pmod{n}$ if and only if $n \mid (a - b)$ if and only if $a - b \in \langle n \rangle = H$.

Example 6.99. Consider $G = \mathbb{R}^\times, H = \{1, -1\}$. To construct a group where $a, b \in G$ are considered "equal" if they have the same magnitude (absolute value). We see that $|a| = |b|$ if and only if $|ab^{-1}| = 1$ if and only if $ab^{-1} \in H$

Example 6.100. Consider $G = GL_n(\mathbb{R}), H = SL_n(\mathbb{R})$. To construct a group where $a, b \in G$ are considered "equal" if they have the same determinant. We see that $\det A = \det B$ if and only if $\det(AB^{-1}) = 1$ if and only if $AB^{-1} \in H$.

So the genral idea is that: Let G be a group, and let $H \leq G$. We construct a new group where $a, b \in G$ are identified (glued together) if and only if $ab^{-1} \in H$.

In practice, the subgroup H will contain the "noise" or elements we don't care about. This makes studying G easier because our new group focuses its attention on elements outside of H.

Note that if $a \in H$, then $ae^{-1} = a \in H$. So, the idea is that we will glue elements of H to e.

Definition 6.101. Let G be a group, $H \leq G$, $g \in G$. The **coset** of H in G containing g, is

$$gH := \{gh : h \in H\}$$

Remark: if the operation of G is additionm we write $g + H = \{g + h : h \in H\}$ instead of gH.

Example 6.102. Let $G = \mathbb{Z}$, $H = \langle n \rangle$, $a \in G$. Then

$$\begin{aligned} a + H &= \{a + h : h \in H\} \\ &= \{a + h : h \in \langle n \rangle\} \\ &= \{a + nk : k \in \mathbb{Z}\} \\ &= \{x \in G : a \equiv x \pmod{n}\} \end{aligned}$$

Example 6.103. Let $G = \mathbb{R}^\times, H = \{-1, 1\}, a \in G$. Then

$$\begin{aligned} aH &= \{ah : h \in H\} \\ &= \{a, -a\} \\ &= \{x \in G : |x| = |a|\} \end{aligned}$$

Example 6.104. Let $G = GL_n(\mathbb{R}), H = SL_n(\mathbb{R}), A \in G$. Then

$$\begin{aligned} AH &= \{AB : B \in H\} \\ &= \{AB : \det B = 1\} \\ &= \{C \in G : \det C = \det A\} \end{aligned}$$

To see the last step, we can see that $\{AB : \det B = 1\} \subseteq \{C \in G : \det C = \det A\}$ is obvious. To see $\{C \in G : \det C = \det A\} \subseteq \{AB : \det B = 1\}$, we take $C \in G$ such that $\det C = \det A$. Then, $C = A(A^{-1}C)$. So $\det(A^{-1}C) = 1$.

6.19 Cosets

Theorem 6.105. **Properties of Cosets**: Let $H \leq G$ be a subgroup.

1. For $g \in G$, $g \in gH$
2. For $g \in G$, $gH = H$ if and only if $g \in H$.
3. For $a, b \in G$, $aH = bH$ if and only if $b^{-1}a \in H$
4. The cosets of H in G partition G. That is
   (a) For two cosets aH, bH of H in G, either $aH = bH$ or $(aH) \cap (bH) = \emptyset$.
   (b) Every element of G belongs to a coset of H in G.

Proof 6.106. 1. Since $H \leq G$, $e \in H$, so $g = ge \in gH$.

2. $\Rightarrow$: Suppose $gH = H$. Then $g = ge \in gH = H$ $\Leftarrow$: Suppose $g \in H$. Now $gH = \{gh : h \in H\} \subset H$. Moreover, if $h \in H$, then $h = g\underbrace{g^{-1}h}_{\in H} \in gH$. So $H \subseteq gH$.

3. We see that

$$\begin{aligned} & aH = bH \\ \Leftrightarrow \quad & \{ah : h \in H\} = \{bh : h \in H\} \\ \Leftrightarrow \quad & \{b^{-1}ah : h \in H\} = \{b^{-1}bh : h \in H\} \\ \Leftrightarrow \quad & b^{-1}aH = H \\ \Leftrightarrow \quad & b^{-1}a \in H \text{ by property 2} \end{aligned}$$

4. (a) Take $a, b \in G$ and consider aH, bH. If $(aH) \cap (bH) = \emptyset$, then we are done. So, suppose $x \in (aH) \cap (bH) \neq \emptyset$. Then, $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Therefore, $b^{-1}a = h_2h_1^{-1} \in H$, and so $aH = bH$.

   (b) For $g \in G$, $g \in gH$

□

Definition 6.107. We define the **index** of H in G, $[G : H]$ to be the number of distinct cosets of H in G.

We denote the set of cosets of H in G by G/H, read as "G mod(ulo) H".

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

Example 6.108. For each of the following, compute G/H and $|G/H|$

- Let $G = S_n$, $H = A_n$. For $\sigma, \tau \in G$, $\sigma H = \tau H$ if and only if $\tau^{-1}\sigma \in A_n$, if and only if $sgn(\tau^{-1}\sigma) = sgn(\tau^{-1})sgn(\sigma) = 1$, if and only if $sgn(\tau)sgn(\sigma) = 1$, if and only if $sgn(\tau) = sgn(\sigma)$.

  So $G/H = \{eH, (12)H\}$. So $[G : H] = |G/H| = 2$

- $G = \mathbb{C}^\times, H = \{z \in \mathbb{C}^\times : |z| = 1\}$. For $a, b \in G$, $aH = bH$ if and only if $b^{-1}a \in H$, if and only if $|b^{-1}a| = 1$, if and only if $|a| = |b|$.

  So $G/H = \{aH : a \in [0, \infty)\}$, so $[G : H] = |G/H| = \infty$

- $G = \mathbb{Z}, H = \langle n \rangle$. For $a, b \in \mathbb{Z}$, $a + H = b + H$ if and only if $-b + a \in H$, if and only if $a - b \in H$, if and only if $n \mid (a - b)$, if and only if $a \equiv b \pmod{n}$.

  So $G/H = \{0 + H, 1 + H, ..., (n-1) + H\}$, so $[G : H] = |G/H| = n$

- $G = D_4$, $H = \langle s \rangle = \{e, s\}$. For $a, b \in D_4$, $aH = bH$ if and only if $b^{-1}a \in H$, if and only if $b^{-1}a = e$ or $b^{-1}a = s$, if and only if $a = b$ or $a = bs$.

So, $G/H = \{\underbrace{eH}_{H}, rH, r^2H, r^3H\}$. $[G:H] = |G/H| = 4$

Note that $r^i sH = r^i H$ since $a = r^i s$, and $b = r^i$.

Also, for $i \neq j \in \{0,1,2,3\}$, $r^i r^{-j} \notin \langle s \rangle$.

6.20 Lagrange's Theorem

Recall that $H \leq G$, say $G/H = \{\underbrace{a_1H, a_2H, ..., a_nH}_{\text{no repetition}}\}$, so $[G:H] = n$. Moreover G is the disjoint union of these cosets

$$G = \cup_{i=1}^{n} a_i H$$

Lemma 6.109. Let $H \leq G$, G is finite. For every $g \in G$, $|gH| = |H|$

Proof 6.110. Consider $f : H \to gH$, then $f(h) = gh$.

$gh_1 = gh_2$ implies $h_1 = h_2$. So f is injective.

For all $g \underbrace{h}_{\in H} \in gH$, $f(h) = gh$, so f is surjective.

Note that $H = eH$ □

Theorem 6.111. Let $H \leq G$, G be finite. $[G:H] = \frac{|G|}{|H|}$.

Proof 6.112. Let $a_1H, ..., a_nH$ be the list of distinct cosets of H in G. Since $G = \cup_{i=1}^{n} a_i H$, $|G| = \sum_{i=1}^{n} |a_i H| = \sum_{i=1}^{n} |H| = n|H|$. So $[G:H] = n = \frac{|G|}{|H|}$. □

Theorem 6.113. **Lagrange Theorem**: Let $H \leq G$, G be a finite group. Then, $|H|$ divides $|G|$

Proof 6.114. This is because $\frac{|G|}{|H|} = [G:H] \in \mathbb{N}$ □

Corollary 6.115. Let G be a finite group,

1. If $g \in G$, then $|g| \mid |G|$
2. Every group of prime order is cyclic

Proof 6.116. 1. Let $g \in G$. Consider $\langle g \rangle$. Then $|g| = |\langle g \rangle| \mid |G|$

2. Suppose G is a group of prime order p. Take any $e \neq g \in G$, then $|g| \mid p$, so $|g| = 1$ or p. However, since $g \neq e$, we have $|g| > 1$. Thus, $|g| = p = |G|$. So $\langle g \rangle = G$.

□

6.21 Quotient Groups

We hope to make G/H into a group via the operation $(aH)(bH) = abH$.

Remark: It appears that

1. $(eH)(aH) = eaH = aH$, $(aH)(eH) = aeH = aH$. Note that $eH = H$.
2. $(aH)(a^{-1}H) = aa^{-1}H = eH = H$, $(a^{-1}H)(aH) = a^{-1}aH = eH = H$
3. $(aH)[(bH)(cH)] = (aH)(bcH) = abcH = (abH)(cH) = [(aH)(bH)](cH)$.

However, we must check that this operation is well-defined.

Example 6.117. Let $G = S_3$, $H = \langle (12) \rangle = \{e, (12)\}$.

So, $(13)(12) = (123)$, $(13)^{-1}(123) = (12) \in H$. So, $(123)H = (13)H$.

However, if we consider $[(123)H] \cdot [(13)H] = [(13)H] \cdot [(13)H]$. By the operation above, $LHS = (23)H$, $RHS = eH = H$. $LHS \neq RHS$. This is because $(23) \notin H$.

Hence, this operation is not necessarily well-defined.

Motivation (for the fix): Let $H \leq G$, $g \in G, h \in H$. We would want to make sure that $gH = (eH)(gH) = (hH)(gH)$. This happens if and only if $gh = hgH$, if and only if $g^{-1}hg \in H$.

Definition 6.118. Let $H \leq G$. We say H is a **normal** subgroup of G if $gHg^{-1} := \{ghg^{-1} : h \in H\} = H$ for all $g \in G$.

If H is normal, we write $H \trianglelefteq G$.

Note that if $H \trianglelefteq G$, $g \in G$, $g^{-1}Hg = H$.

Example 6.119. Let $G = S_3$, $H = \langle (12) \rangle$.

We have $(12) \in H$, and we compute $(13)(12)(13)^{-1} = (13)(12)(13) = (23) \notin H$

So H is not a normal subgroup of G.

Example 6.120. Let $G = GL_n(\mathbb{R}), H = SL_n(\mathbb{R})$. For $A \in G$, and $B \in H$, $\det(ABA^{-1}) = \det B = 1$. So $ABA^{-1} \in H$, so $AHA^{-1} \subseteq H$.

Let $B \in H$, and consider $A^{-1}BA$. As above, $A^{-1}BA \in H$. So $B = A\underbrace{(A^{-1}BA)}_{\in H}A^{-1} \in AHA^{-1}$

So $AHA^{-1} = H$. So $H \trianglelefteq G$.

Exercise: Prove that $H \trianglelefteq G$ if and only if for all $g \in G$, $gHg^{-1} \subseteq H$.

Remark:

1. When we say $gHg^{-1} = H$, this doesn't mean $ghg^{-1} = h$ for all $h \in H$. It means that for all $g \in G, h \in H$, $ghg^{-1} = h'$ for some $h' \in H$.
2. If G is abelian, then $H \leq G$ implies that $H \trianglelefteq G$. To see why, for $g \in G$, $h \in H$, $ghg^{-1} = h \in H$. So, every subgroup of an abelian group is normal.
3. Let G be a group. $Z(G) \trianglelefteq G$.

Theorem 6.121. Let $H \trianglelefteq G$ be a normal subgroup of G. The operation $(aH)(bH) = abH$ is well defined. Hence, G/H is a group via this operation.

Note that the groups of the form G/H are called **quotient groups**.

Proof 6.122. Suppose $H \trianglelefteq G$, and $a, a', b, b' \in G$ such that $aH = a'H$ and $bH = b'H$. We show: $\underbrace{abH}_{(aH)(bH)} = \underbrace{a'b'H}_{(a'H)(b'H)}$.

Now, $a^{-1}a', b^{-1}b' \in H$. Moreover,

$$\begin{aligned}(ab)^{-1}(a'b') &= b^{-1}\underbrace{a^{-1}a'}_{\in H}b' \\ &= \underbrace{b^{-1}a^{-1}a'b}_{\in H}\underbrace{b^{-1}b'}_{\in H} \\ &\in H\end{aligned}$$

So $abH = a'b'H$. □

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 7: October 27

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

7.22 Quotient Groups

Piazza Discussion: Let $H \leq G$. Prove that if the operation $(aH)(bH) = abH$ is well-defined, then $H \trianglelefteq G$.

Theorem 7.123. Let $H \leq G$. Then $H \trianglelefteq G$ if and only if $H = \ker \varphi$ for some homomorphism $\varphi : G \to G'$

Proof 7.124. $\Rightarrow$: Suppose $H \trianglelefteq G$. Thus G/H is a group. Moreover, $\varphi : G \to G/H$ in which $\varphi(g) = gH$ is a homomorphism. To see this, note that $\varphi(ab) = abH = (aH)(bH) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

Also, note that $g \in \ker \varphi$ if and only if $\varphi(g) = H$, if and only if $gH = H$, if and only if $g \in H$. And so $\ker \varphi = H$.

$\Leftarrow$: Suppose $H = \ker \varphi$, and $\varphi : G \to G'$ is a homomorphism. Let $g \in G$ and $h \in H$. Then, $\varphi(h) = e$, and so $\varphi(ghg^{-1}) = \varphi(g) \cdot \underbrace{\varphi(h)}_{e} \varphi(g)^{-1} = e$. Hence $ghg^{-1} \in H$, and so $gHg^{-1} \subseteq H$.

Hence, $H \trianglelefteq G$. □

Theorem 7.125. Let $H, K \trianglelefteq G$, $H \cap K = \{e\}$. Then G is isomorphic to a subgroup of $G/H \times G/K$.

Proof 7.126. Let $\varphi : G \to G/H \times G/K$. If we can prove φ is injective, then we are done.

Let $\varphi(g) = (gH, gK)$. Showing φ is a homomorphism is left as an exercise.

Now, we just need to show that $\ker \varphi = \{e\}$. Note that $g \in \ker \varphi$ if and only if $\varphi(g) = (gH, gK) = (H, K)$, if and only if $gH = H$ and $gK = K$, if and only if $g \in H$ and $g \in K$. Hence, $g \in H \cap K = \{e\}$. So, $\ker \varphi = \{e\}$, and so φ is an embedding. □

Theorem 7.127. Let $H \leq G$. If $[G : H] = 2$, then $H \trianglelefteq G$.

Proof 7.128. Let $H \leq G$ such that $[G : H] = 2$. Let $g \in G$.

- If $g \in H$, then $gHg^{-1} \subseteq H$
- Suppose $g \notin H$. Therefore we have $gH \neq H$. Hence, $G/H = \{H, gH\}$. Suppose for contradiction, $gHg^{-1} \not\subseteq H$, so that there exists $h \in H$ such that $ghg^{-1} \notin H$. So, $ghg^{-1}H = gH$. So $hg^{-1}H = H$, and hence $g^{-1}H = h^{-1}H = H$. So $g^{-1} \in H$ which implies $g \in H$. Contradiction.

  Hence, $gHg^{-1} \subseteq H$.

Hence, we have $H \trianglelefteq G$. □

7.23 First Isomorphism Theorem

Theorem 7.129. **First Isomorphism Theorem**: Let $\varphi : G \to H$ be a homomorphism. Then, $G/\ker\varphi \cong \varphi(G)$.

Proof 7.130. Let $K = \ker\varphi$. Consider $\psi : G/K \to \varphi(G)$, $\psi(gK) = \varphi(g)$. We need to prove that it is well-defined.

Suppose $aK = bK$ in G/K, then $a^{-1}b \in K$, and $\varphi(a^{-1}b) = e$. So $\varphi(a)^{-1}\varphi(b) = e$. So, we would have $\varphi(a) = \varphi(b)$, so $\psi(aK) = \psi(bK)$.

We also need to prove that ψ is a homomorphism. For $aK, bK \in G/K$, we have $\psi(aK \cdot bK) = \psi(abK) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aK)\psi(bK)$.

We need to prove that ψ is injective and surjective.

Suppose $aK, bK \in G/K$ such that $\psi(aK) = \psi(bK)$. So $\varphi(a) = \varphi(b)$. So $\varphi(a^{-1}b) = e$, so $a^{-1}b \in K$. By theorem, $aK = bK$. So ψ is injective.

Let $y \in \psi(G)$. Then, there exists $g \in G$ such that $y = \varphi(g)$. Then, $\psi(gK) = \varphi(g) = y$, and so ψ is surjective.

Hence, ψ is an isomorphism.

□

7.24 Practice

Example 7.131. Let's find some examples of isomorphism from quotient groups to non-quotient groups

- Consider $GL_n(\mathbb{R})/SL_n(\mathbb{R})$. What is this group isomorphic to? Let $H = SL_n(\mathbb{R})$. Consider $AH = BH$, this happens if and only if $B^{-1}A \in H$, if and only if $\det(B^{-1}A) = 1$, if and only if $\det A = \det B$.

  So, we claim that $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$. Let $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ be given by $\varphi(A) = \det A$. We already know that φ is a homomorphism. Moreover, we need information about kernel about this map. $A \in \ker\varphi$ if and only if $\det A = 1$, if and only if $A \in SL_n(\mathbb{R})$.

  By the First Isomorphism Theorem, $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \underbrace{\varphi(GL_n(\mathbb{R}))}_{\subseteq \mathbb{R}^\times}$

  Moreover, for $\alpha \in \mathbb{R}^\times$,

  $$\begin{bmatrix} \alpha & \cdots & 0 \\ \vdots & 1 & \vdots \\ 0 & \cdots & 1 \end{bmatrix} \to \alpha \text{ under } \varphi$$

  So φ is surjective. So, $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$

- Consider S_n/A_n. A_n has index 2, so S_n/A_n is indeed group. What is this group isomorphic to? Consider $\sigma A_n = \tau A_n$, this happens if and only if $\sigma^{-1}\tau \in A_n$, if and only if $sgn(\sigma^{-1}\tau) = 1$, if and only if $sgn(\sigma)sgn(\tau) = 1$, if and only if $sgn(\sigma) = sgn(\tau)$.

  So, we claim that $S_n/A_n \cong \{1, -1\} = C_2$. $\varphi : S_n \to C_2$, $\varphi(\sigma) = sgn(\sigma)$.

- Consider $\mathbb{R}/\mathbb{Z}$. Consider $2.713 + \mathbb{Z} = 0.713 + \mathbb{Z}$ because $2.713 - 0.713 = 2 \in \mathbb{Z}$. So, we can just consider $[0, 1)$. But this is not a group. We can consider it as a circle, where the start point is 0.

  So we claim that $\mathbb{R}/\mathbb{Z} \cong \{z \in \mathbb{C}^\times : |z| = 1\}$. Consider $\varphi : \mathbb{R} \to S^1$ given by $\psi(x) = e^{ix2\pi} = e^{2\pi ix}$.

  This is a homomorphism. For $x, y \in \mathbb{R}$, $\varphi(x + y) = e^{2\pi i(x+y)} = e^{2\pi ix}e^{2\pi iy} = \varphi(x)\varphi(y)$. So φ is a homomorphism.

  Let $z \in S^1$. Then $z = \cos\theta + i\sin\theta = e^{i\theta}$ for some $\theta \in \mathbb{R}$. So, $\varphi(\frac{\theta}{2\pi}) = e^{i\theta} = z$, so φ is surjective.

  Now, $x \in \ker\varphi \Leftrightarrow e^{2\pi ix} = 1$, if and only if $\cos(2\pi x) + i\sin(2\pi x) = 1$, if and only if $\cos(2\pi x) = 1$ and $\sin(2\pi x) = 0$, if and only if $x \in \mathbb{Z}$.

  By the First Isomorphism Theorem, $\mathbb{R}/\mathbb{Z} \cong \varphi(\mathbb{R}) = S^1$

7.25 Automorphisms

Definition 7.132. An isomorphism $\varphi : G \to G$ is called an **automorphism**. We denote the set of automorphisms of G by $Aut(G)$.

Remark: $Aut(G)$ is a group under composition.

Theorem 7.133. Let G be a group, $g \in G$. The map $\varphi_g(x) = gxg^{-1}$ is an automorphism of G.

Definition 7.134. Automorphisms of G of the form φ_g are called **inner automorphisms**. The set of inner automorphisms of G is denoted by $Inn(G)$.

Theorem 7.135. Let G be a group. $Inn(G) \trianglelefteq Aut(G)$

Proof 7.136. We see that $e = \varphi_e \in Inn(G)$. Let $\varphi_a, \varphi_b \in Inn(G)$.

- For $x \in G$, $\varphi_a \circ \varphi_b(x) = \varphi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x)$. So, $\varphi_a \circ \varphi_b = \varphi_{ab} \in Inn(G)$.
- For $x \in G$, $\varphi_a \circ \varphi_{a^{-1}}(x) = \varphi_a(a^{-1}xa) = aa^{-1}xaa^{-1} = x$, So $\varphi_a \circ \varphi_{a^{-1}} = e$.
  Similarly, $\varphi_{a^{-1}} \circ \varphi_a = e$.
  So, $\varphi_a^{-1} = \varphi_{a^{-1}} \in Inn(G)$.
  Thus, $Inn(G) \leq Aut(G)$.
- Let $\psi \in Aut(G)$ and $\varphi_g \in Inn(G)$. For $x \in G$, $(\psi \circ \varphi_g \circ \psi^{-1})(x) = \psi(g\psi^{-1}(x)g^{-1}) = \psi(g)x\psi(g)^{-1}$. So, $\psi \circ \varphi_g \circ \psi^{-1} = \varphi_{\psi(g)} \in Inn(G)$.
  SO, $\psi Inn(G)\psi^{-1} \subseteq Inn(G)$, which implies that $Inn(G) \trianglelefteq Aut(G)$.

□

Theorem 7.137. $G/Z(G) \cong Inn(G)$.

Proof 7.138. Define $\psi : G \to Inn(G)$ by $\psi(g) = \varphi_g$.

For $a, b \in G$, we have $\psi(ab) = \varphi_{ab} = \varphi_a \circ \varphi_b = \psi(a)\psi(b)$. So ψ is a homomorphism.

Since every element of $Inn(G)$ is of the form φ_g, $g \in G$, ψ is surjective.

Next, observe that $a \in \ker \psi$ if and only if $\psi_a = e \in Inn(G)$, if and only if $\psi_a(x) = x$ for all $x \in G$, if and only if $axa^{-1} = x$ for all $x \in G$, if and only if $ax = xa$ for all $x \in G$, if and only if $a \in Z(G)$.

By the First Isomorphism Theorem, $G/Z(G) \cong Inn(G)$. □

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 8: November 3

Lecturer: Blake Madill *Noted By: Haochen Wu*

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this course only with the permission of the instructors.*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

8.26 Group Actions

Definition 8.139. Let G be a group, X be a non-empty set. A **group action** of G on X is a map

$$\cdot : G \times X \to X$$

such that

1. For all $x \in X$, $e \cdot x = x$
2. For all $a, b \in G$, for all $x \in X$, $(ab) \cdot x = a \cdot (b \cdot x)$

Definition 8.140. Suppose G acts on X

1. For $x \in X$
$$stab(x) = \{g \in G : gx = x\}$$
is called the **stabilizer** of x.
2. For $x \in X$,
$$\mathcal{O}_x = \{gx : g \in G\} \subseteq X$$
is called the **orbit** of x.

For piazza exercises, prove that $stab(x) \leq G$.

Example 8.141. Let's see some examples of group actions:

- Let $G = S_n$, $X = \{1, 2, ..., n\}$. $\sigma \cdot i = \sigma(i)$.
- Let $G = D_4$. $X = \{\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix} ...\}$. There are eight of them.

- Let $G = S_n$, $X = \{\Delta, -\Delta\}$. $stab(\Delta) = \{\sigma \in S_n : \sigma(\Delta) = \Delta\} = A_n$
- Let $G = GL_n(\mathbb{R})$, $X = \mathbb{R}^n$. $A \underbrace{\cdot}_{\text{group action}} v = A \underbrace{\quad}_{\text{matrix multiplication}} v$
- Let H be a group. Let $G = Aut(H)$, $X = H$. Then $\varphi \cdot h = \varphi(h)$.

There are four very important group actions:

1. Left Multiplication I: Take G be any group, $X = G$. We define $g \cdot x = gx$. The action is the group operation.

   Take $x \in X$: $stab(x) = \{g \in G : gx = x\} = \{e\}$. $\mathcal{O}_x = \{gx : g \in G\} = G = X$.
2. Left Multiplication II: Take G be any group. Let $H \leq G$. Let $X = G/H$. We define $g \cdot aH = (ga)H$.
3. Conjugation I: Take G be any group, $X = G$. We define $g \cdot x = gxg^{-1}$.

   Take $x \in X$: $stab(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} =: C(x)$. We called it the **centralizer** of $x \in G$.
4. Conjugation II: Take G be any group, $X = \{H : H \leq G\}$. We define $g \cdot H = gHg^{-1} \leq G$.

   Take $H \leq G$ ($H \in X$), $stab(H) = \{g \in G : gHg^{-1} = H\} =: N_G(H)$. We called it the **normalizer** of H in G.

Remark:

1. $N_G(H) \leq G$
2. $H \trianglelefteq N_G(H)$
3. $N_G(H) = G$ if and only if $H \trianglelefteq G$.

8.27 Orbit-Stabilizer

Theorem 8.142. **Orbit-Stabilizer Theorem**: Let G be a finite group acting on a set X. For all $x \in X$,

$$|G| = |stab(x)| \cdot |\mathcal{O}_x|$$

Proof 8.143. The idea is to show that $|G/stab(x)| = |\mathcal{O}_x|$. We want to construct a bijection between them.

Define $\varphi : G/stab(x) \to \mathcal{O}_x$ by $\varphi(g \cdot stab(x)) = gx$. We claim that this is a bijection.

1. It is well-defined. Suppose $g \cdot stab(x) = h \cdot stab(x)$ for some $g, h \in G$. Then, $g^{-1}h \in stab(x)$. So, $g^{-1}hx = x$, so $hx = gx$, and so $\varphi(h \cdot stab(x)) = \varphi(g \cdot stab(x))$

2. It's injective. Suppose $\varphi(g \cdot stab(x)) = \varphi(h \cdot stab(x))$, this means that $gx = hx$, and so $g^{-1}hx = x$. So, $g^{-1}h \in stab(x)$. So, $g \cdot stab(x) = h \cdot stab(x)$ as required.
3. It's surjective. For $y \in \mathcal{O}_x$, there exists $g \in G$ such that $y = gx$. Then, $\varphi(g \cdot stab(x)) = gx = y$.

So, φ is a bijection, so, $|G/stab(x)| = |\mathcal{O}_x|$. □

Notation: For orbits of x, we may have

$$Orb(x) = \mathcal{O}_x$$

Example 8.144. Let G be the group of symmetries of the cube. What's $|G|$?

$X = \{$ faces of the cube $\}$

$$\begin{aligned} |G| &= |stab(f_1)| \cdot |\mathcal{O}_{f_1}| \\ &= 4 \times 6 \\ &= 24 \end{aligned}$$

8.28 Class Equation

Remark: Let G be a group and consider G acting on $X = G$ by conjugation, i.e. $g \cdot x = gxg^{-1}$.

From last section, $stab(x) = C(x)$, the centralizer of x. Further, we call $\mathcal{O}_x = \{gxg^{-1} : g \in G\}$ the **conjugacy** class of x in G

Lemma 8.145. Let G be a group acting on a set X. For $x, y \in X$, either

- $\mathcal{O}_x = \mathcal{O}_y$ or
- $\mathcal{O}_x \cap \mathcal{O}_y = \emptyset$

Proof 8.146. Suppose $\mathcal{O}_x \cap \mathcal{O}_y \neq \emptyset$, and let $z \in \mathcal{O}_x \cap \mathcal{O}_y$.

Thus, there exists $a, b \in G$ such that $ax = z = by$. This means $x = a^{-1}by.y = b^{-1}ax$. $\mathcal{O}_x \subseteq \mathcal{O}_y$, and also $\mathcal{O}_y \subseteq \mathcal{O}_x$. Hence, $\mathcal{O}_x = \mathcal{O}_y$ as desired. □

Remark: Let G acts on finite X:

1. for all $x \in X$, $ex = x$ and so $x \in \mathcal{O}_x$

2. If $\mathcal{O}_{x_1}, \mathcal{O}_{x_2}, ..., \mathcal{O}_{x_n}$ are distinct orbits of the action,

$$X = \bigcup_{i=1}^{n} \mathcal{O}_{x_i} \text{ i.e. the disjoint union}$$

   We call $x_1, ..., x_n \in X$ the orbit **representatives**.

3. $$|X| = \sum_{i=1}^{n} |\mathcal{O}_{x_i}|$$

Remark: Let G be a finite group acting on $X = G$ by conjugation. Let $g_1, ..., g_n \in G$ be a complete list of conjugacy class (orbit) representatives. Then:

$$\begin{aligned} |G| &= \sum_{i=1}^{n} |\mathcal{O}_{g_i}| \\ &= \sum_{i=1}^{n} \frac{|G|}{|stab(g_i)|} \\ &= \sum_{i=1}^{n} \frac{|G|}{|C(g_i)|} \\ &= \sum_{i=1}^{n} [G : C(g_i)] \end{aligned}$$

Note that $g \in Z(G)$ if and only if $\mathcal{O}_g = \{hgh^{-1} : h \in G\} = \{g\}$. Hence, $|G| = |Z(G)| + \sum_{i=1}^{m} [G : C(a_i)]$ where a_i's are a complete list of **non-central** conjugacy class representatitives.

We call

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C(a_i)]$$

as the **class equation**.

Corollary 8.147. Let p be a prime. If G is a group of order $|G| = p^n$, $n \in \mathbb{N}$, then $Z(G) \neq \{e\}$

Proof 8.148. $p^n = |G| = |Z(G)| + \sum_{i=1}^{m} [G : C(a_i)]$. Note that $C(a_i) \neq G$, so $[G : C(a_i)] > 1$. Also, $[G : C(a_i)] = \frac{|G|}{|C(a_i)|} \mid |G| = p^n$.

$$\begin{aligned} \underbrace{p^n}_{\equiv 0 \pmod p} = |G| = |Z(G)| + \sum_{i=1}^{m} \underbrace{[G : C(a_i)]}_{\equiv 0 \pmod p} \\ \Rightarrow |Z(G)| \equiv 0 \pmod p \\ \Rightarrow |Z(G)| \neq 1 \end{aligned}$$

□

Corollary 8.149. Let p be a prime. Every group of order p^2 is abelian.

Proof 8.150. From assignment, we know that $Z(G) = \{e\}$ or $\underbrace{Z(G) = G}_{G \text{ is abelian}}$.

From the last result, $Z(G) \neq \{e\}$. □

8.29 Cauchy's Theorem

Example 8.151. Let $G = S_4$, $|G| = 24$. $6 \mid 24$ but there does not exist $g \in S_4$ with $|g| = 6$.

Thinking from the disjoint cycle form. We can't have a 2-cycle and 3-cycle as disjoint cycles.

Lemma 8.152. If G is a finite cyclic group of order n and $d \in \mathbb{N}$ such that $d \mid n$, then there exists $g \in G$ with $|g| = d$

Proof 8.153. Suppose $d \mid n$. Then, there exists a subgroup $H \leq G$ of order d. Moreover, $H = \langle g \rangle$ for some $g \in H$. Therefore, $|g| = |H| = d$. □

Lemma 8.154. Let G be a finite **abelian** group. If p is a prime such that $p \mid |G|$, then there exists $g \in G$ with $|g| = p$.

Proof 8.155. We use induction on $n = |G|$.

Base Case: if $n = p$, then G is cyclic. We are done by the previous lemma.

Inductive Hypothesis: Assume the result for all abelian groups $|G'|$ such that $p \mid |G'|$ and $|G'| < n$ holds true.

Inductive Conclusion: Let G be an abelian group of order n with $p \mid n$.

Take $e \neq a \in G$, then $H = \langle a \rangle \trianglelefteq G$

1. If $p \mid |H|$, then there exists $g \in H$ such that $|g| = p$ because H is a cyclic group.
2. If $p \nmid |H|$. Since $|G/H| = \frac{|G|}{|H|} < |G|$, we have $p \mid |G/H|$. By inductive hypothesis, there exists gH such that $|gH| = p$.

   Note that $(gH)^{|g|} = g^{|g|}H = eH = H$. So, $p = |gH|$ divides $|g|$. Hence, $p \mid |\langle g \rangle|$, so $\langle g \rangle$ has an element of order p.

□

Theorem 8.156. **Cauchy's Theorem**: Let G be a finite group. If p is a prime such that $p \mid |G|$, then there exists $g \in G$ with $|g| = p$.

Proof 8.157. By the class equation, $|G| = |Z(G)| + \sum_{i=1}^{m} [G : C(a_i)]$.

1. If $p \mid |Z(G)|$, then we are done by the previous lemma
2. Suppose $p \nmid |Z(G)|$, then there exists a_i such that $p \nmid [G : C(a_i)]$.

   This means that $p \nmid \frac{|G|}{|C(a_i)|}$, which means that $p \mid |C(a_i)|$. Note that $|C(a_i)| < |G|$, and we may apply induction here.

   The result follows by induction.

□

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 9: November 10

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

9.30 Burnside's Lemma

Definition 9.158. Let G be a finite group acting on a finite set X:

- For $g \in G$, we define
$$Fix(g) = \{x \in X : gx = x\}$$
- We let $X \setminus G$ denote the set of distinct orbits of X under this action.

We can see that

$$\begin{aligned}
\sum_{g\in G} |Fix(g)| &= |\{(g,x) \in G \times X : gx = x\}| \\
&= \sum_{x\in X} |stab(x)| \\
&= \sum_{x\in X} \frac{|G|}{|\mathcal{O}_x|} \text{ by Orbit Stablizer Theorem} \\
&= |G| \sum_{x\in X} \frac{1}{|\mathcal{O}_x|} \\
&= |G| \sum_{A\in X\setminus G} \sum_{x\in A} \frac{1}{|\mathcal{O}_x|} \\
&= |G| \sum_{A\in X\setminus G} \sum_{x\in A} \frac{1}{|A|} \\
&= |G| \sum_{A\in X\setminus G} |A| \frac{1}{|A|} \\
&= |G| \sum_{A\in X\setminus G} 1 \\
&= |G| \cdot |X \setminus G|
\end{aligned}$$

Lemma 9.159. Burnside's Lemma: $|X \setminus G| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$

9.31 Example

Example 9.160. How many necklaces can be made using 4 spherical beads, where n colours of beads are available?

Let X be the set of all "configurations" of all such necklaces.

Let $G = D_4$. Consider the natrual action of G on X.

Remark: Take $x, y \in X$. Then $\mathcal{O}_x = \mathcal{O}_y$ if and only if there exists $g \in D_4$ such that $gx = y$. This means that x and y are the same necklace.

The number of such necklaces is $|X \setminus G|$, which gives that

$$\begin{aligned} |X \setminus G| &= \frac{1}{|G|} \sum_{g \in G} |Fix(g)| \\ &= \frac{1}{8} \sum_{g \in G} |Fix(g)| \\ &= \frac{1}{8}(n^4 + 2n^3 + 3n^2 + 2n) \end{aligned}$$

Since

$g \in D_4$	$\lvert Fix(g)\rvert$
e	n^4
r	n
r^2	n^2
r^3	n
s	n^3
sr	n^2
sr^2	n^3
sr^3	n^2

Example 9.161. How many ways can the points be coloured using n colors? There are 8 points on the crown.

Let X be the configurations of all such colourings.

Let $G = \{e, r, r^2, ..., r^7\} \leq D_8$.

Hence, the number of such crowns is equal to $|X \setminus G|$ which gives that

$$\begin{aligned} |X \setminus G| &= \frac{1}{|G|} \sum_{g \in G} |Fix(g)| \\ &= \frac{1}{8} \sum_{g \in G} |Fix(g)| \\ &= \frac{1}{8}(n^8 + n^4 + 2n^2 + 4n) \end{aligned}$$

Since

$g \in G$	$\lvert Fix(g)\rvert$
e	n^8
r	n
r^2	n^2
r^3	n
r^4	n^4
r^5	n
r^6	n^2
r^7	n

Example 9.162. How many ways we can colour the edges of a square if

- 5 colors are available
- no one colour can be used on more than two edges
- at least one colour is used more than once

Let X be the configurations of all such colourings.

Let $G = D_4$. Consider the natrual action of G on X.

The number of such necklaces is $|X \setminus G|$, which gives that

$$\begin{aligned} |X \setminus G| &= \frac{1}{|G|} \sum_{g \in G} |Fix(g)| \\ &= \frac{1}{8} \sum_{g \in G} |Fix(g)| \\ &= \frac{1}{8}(420 + 20 + 20 + 80 + 20 + 80) \\ &= 80 \end{aligned}$$

Since

$g \in D_4$	$\lvert Fix(g)\rvert$
e	$5^4 - 5 \cdot 4 \cdot 3 \cdot 2 - \binom{4}{3} 5 \cdot 4 - 5 = 420$
r	0
r^2	$5 \cdot 4 = 20$
r^3	0
s	$5 \cdot 4 = 20$
sr	$5 \cdot 4 \cdot 4 = 80$
sr^2	$5 \cdot 4 = 20$
sr^3	$5 \cdot 4 \cdot 4 = 80$

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 10: November 17

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

10.32 Finite Abelian Groups

Theorem 10.163. Let $H, K \trianglelefteq G$, consider $HK \leq G$ (from assignment 1), then $HK \trianglelefteq G$

Proof 10.164. Let $h \in H, k \in K$, so that $hk \in HK$. For $g \in G$,

$$ghkg^{-1} = \underbrace{(ghg^{-1})}_{\in H}\underbrace{(gkg^{-1})}_{\in K} \in HK$$

Hence, $HK \trianglelefteq G$ □

Theorem 10.165. Let $H, K \trianglelefteq G$, and $H \cap K = \{e\}$. If $h \in H$ and $k \in K$, then $hk = kh$

Proof 10.166. Take $h \in H$ and $k \in K$. Then,

$$\underbrace{hkh^{-1}}_{\in K}k^{-1} \in K, h\underbrace{kh^{-1}k^{-1}}_{\in H} \in H$$

Hence, $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, and $hkh^{-1}k^{-1} = e$. □

Theorem 10.167. Let $H, K \trianglelefteq G$, and $H \cap K = \{e\}$. $HK \cong H \times K$

Proof 10.168. Consider $\varphi : H \times K \to HK$ given by $\varphi(h,k) = hk$.

1. It is a homomorphism:
$$\begin{aligned}\varphi((h_1,k_1)(h_2,k_2)) &= \varphi(h_1h_2, k_1k_2)\\ &= h_1h_2k_1k_2\\ &= h_1k_1h_2k_2\\ &= \varphi(h_1,k_1)\varphi(h_2,k_2)\end{aligned}$$
2. It is injective: Take $(h,k) \in \ker\varphi$, so that $hk = e$, then, $h = k^{-1} \in H \cap K = \{e\}$. Hence, $h = k = e$. So, $(h,k) = (e,e)$. So, $\ker\varphi = \{(e,e)\}$, so φ is injective.
3. It is surjective: For $hk \in HK$, $\varphi(h,k) = hk$.

□

Theorem 10.169. Let $H_1, H_2, ..., H_n \trianglelefteq G$, $H_i \cap H_1H_2\cdots H_{i-1}H_{i+1}\cdots H_n = \{e\}$, then

1. If $a \in H_i$ and $b \in H_i \cap H_1H_2\cdots H_{i-1}H_{i+1}\cdots H_n$, then $ab = ba$
2. $H_1H_2\cdots H_n \cong H_1 \times H_2 \cdots \times H_n$

We may use notation to simplify the work we have

$$\hat{H_i} := H_1H_2\cdots H_{i-1}H_{i+1}\cdots H_n$$

Motivation:

1. If $|G| = p$ is a prime, then G is cyclic, and $G \cong \mathbb{Z}_p$.
2. If $|G| = p^2$, then G is abelian, and
   (a) There exists $a \in G$, $|a| = p^2$, and we have $G = \langle a\rangle \cong \mathbb{Z}_{p^2}$
   (b) There does not exist $a \in G$ such that $|a| = p^2$. By Lagrange's Theorem, if $e \neq a \in G$, then $|a| = p$.
   Take $a \in G$ with $|a| = p$. If $H := \langle a\rangle$, then $|H| = p$. Take $e \neq b \in G$, $b \notin H$. If $K := \langle b\rangle$ then $|K| = p$.
   Note that $H \cap K \leq K$, $H \cap K \neq K$ since $b \notin H \cap K$.
   Hence, $|H \cap K| \mid p$, and $|H \cap K| \neq p$. Hence, $H \cap K = \{e\}$.
   Since $HK \cong H \times K$, $|HK| = |H|\cdots|K| = p^2$. Hence, $G = HK \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$.
3. If p, q are distinct primes and G is abelian with $|G| = pq$, then By Cauchy's Theorem, there exists $a, b \in G$ with $|a| = p$ and $|b| = q$.

Let $H := \langle a \rangle$ and $K := \langle b \rangle$. We have $|H| = p, |K| = q$.
Then, $|H \cap K| \mid |H|$, and $|H \cap K| \mid |K|$. Hence, $H \cap K = \{e\}$.
Hence, we know, $HK \cong H \times K$, and $G = HK \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ by Assignment 2.

Definition 10.170. Let p be a prime and let G be a group of order $p^n m$ where $p \nmid m$. Any subgroup of G order p^n is called a **Sylow p-subgroup** of G

Example 10.171. Consider $G = A_4$. We have $|G| = 12 = 2^2 \times 3$.

Let $H_1 = \{e, (12)(34), (13)(24), (14)(23)\}$. This is a Sylow 2-subgroup.

Let $H_2 = \langle (123) \rangle$. This is a Sylow 3-subgroup.

Let $H_3 = \langle (124) \rangle$. This is a Sylow 3-subgroup.

Theorem 10.172. Let G be a finite abelian group of order

$$|G| = p^n m, p \nmid m$$

Then G contains a Sylow p-subgroup.

Proof 10.173. We proceed by induction on n.

Base Case: If $n = 1$, then $|G| = pm, p \nmid m$. By Cauchy's Theorem, there exists $g \in G$ such that $|g| = p$. Thus, $\langle g \rangle$ is a Sylow p-subgroup.

Inducitve Hypothesis: Assume the result holds for $n - 1$

Inductive Conclusion: Let $|G| = p^n m, p \nmid m$. Using Cauchy, choose $g \in G$ such that $|g| = p$. Then, $\langle g \rangle \trianglelefteq G$ since G is abelian. Then, $|G/\langle g \rangle| = p^{n-1} m$.

By inductive hypothesis, $G/\langle g \rangle$ has a subgroup $\bar{H}$ of order p^{n-1}. By Assignment, we know that $\bar{H} = H/\langle g \rangle$ for some $\langle g \rangle \leq H \leq G$.

Note that $p^{n-1} = |\bar{H}| = \frac{|H|}{|\langle g \rangle|} = \frac{|H|}{p}$. Hence, $|H| = p^n$. □

Remark: let G be abelian, and $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where p_i's are distinct primes. For each p_i, let H_i be a Sylow p_i-subgroup.

1. $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k = \{e\}$. This is because

$$\gcd(\underbrace{|H_i|}_{p_i^{n_i}}, \underbrace{|H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k|}_{p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}}) = 1$$

This intersection is in both H_i and $H_1H_2\cdots H_{i-1}H_{i+1}\cdots H_k$. By Lagrange's Theorem, the order has to divide both subgroup. Since the order of these two subgroups are coprime, the intersection has to be trivial.

2. $H_1, H_2, ..., H_k \trianglelefteq G$ since G is abelian.
3. $H_1H_2\cdots H_k \cong H_1 \times H_2 \times \cdots \times H_k$. In particular, $H_1H_2\cdots H_k = G$. So, $G \cong H_1 \times H_2 \times \cdots \times H_k$

Theorem 10.174. Every group of order p^n, where p is a prime, is isomorphic to a direct product cyclic groups.

Theorem 10.175. Fundamental Theorem of Finite Abelian Group: Every finite abelian group is isomorphic to a direct product of cyclic groups.

Recall that

1. $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ if and only if $\gcd(m, n) = 1$
2. If $A_i \cong B_i$ where $(1 \leq i \leq n)$, then $A_1 \times \cdots \times A_n \cong B_1 \times \cdots \times B_n$.

Lemma 10.176. Let G, H be finite groups. If $\gcd(|G|, |H|) = 1$, and $d \in \mathbb{N}$ divides $|G|$, then $(g, h) \in G \times H$ has order d if and only if $h = e$ and $|g| = d$

Corollary 10.177. Let G, H be finite groups. If $\gcd(|G|, |H|) = 1$, and $d \in \mathbb{N}$ divides $|G|$, then

$$|\{(g, h) \in G \times H : |(g, h)| = d\}| = |\{g \in G : |g| = d\}|$$

Example 10.178. Write down an irredundant and complete list of abelian groups of order $36 = 2^2 \times 3^2$ up to isomorphism.

	$\lvert g\rvert = 2$	$\lvert g\rvert = 3$
$\mathbb{Z}_{36} \cong \mathbb{Z}_4 \times \mathbb{Z}_9$	1	2
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$	3	2
$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	1	8
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	3	8

By the **Fundamental Theorem of Abelian Groups**, we know this list is complete.

By the order computations, the list is irredundant.

PMATH336: Introduction to Group Theory **Fall 2020**

Lecture 11: November 24

Lecturer: Blake Madill *Noted By: Haochen Wu*

This lecture's notes tend to be supplementary (add-on notes) of the course notes provided.

11.33 Sylow Theorem

Definition 11.179. Let p be a prime. A group of order $p^n, n \in \mathbb{Z}$ is called a p**-group**.

Definition 11.180. If $H \leq G$ and H is a p**-group**, we call H a p**-subgroup** of G.

Definition 11.181. Let p be a prime, and let G be a group of order $|G| = p^n m$, where $n, m \in \mathbb{N}$ with $p \nmid m$. Any subgroup of G of order p^n is called a Sylow p**-subgroup** of G.

The general idea is that, we want to study Sylow p-subgroups. It is a powerful tool that will allow us to prove results about finite groups, when **given only the order of the group**.

Theorem 11.182. Sylow's First Theorem: Let G be a finite group. If p is a prime such that $p \mid |G|$. Then G contains a Sylow p-subgroup.

Proof 11.183. We proceed by induction on $|G|$.

If $|G| = 2$ then G is a Sylow 2-subgroup of itself.

Assume the result for all groups of order less than k. Let G be a group of order k.

Suppose p is a prime with $p \mid |G|$. Say $|G| = p^n m, p \nmid m$

1. When $p \mid |Z(G)|$. Say $|Z(G)| = p^\ell t$, $p \nmid t$.
   Since $Z(G)$ is abelian, there exists $H \leq Z(G)$ such that $|H| = p^\ell$. Since $H \subseteq Z(G)$, $H \trianglelefteq G$.

Consider G/H. By Inductive Hypothesis, there exists $\bar{K} \leq G/H$ such that $|\bar{K}| = p^{n-\ell}$.

From previous practices, we know that there exists $K \leq G$ such that $\bar{K} = K/H$. This tells us that $p^{n-\ell} = \frac{|K|}{p^\ell}$. And hence, $|K| = p^n$.

2. When $p \nmid |Z(G)|$. By the class equation, there exists $a \notin Z(G)$ such that $p \nmid \underbrace{[G : C(a)]}_{>1}$. So, $p^n \mid |C(a)|$.

   By Inductive Hypothesis, since $|C(a)| < |G|$, there exists $H \leq C(a)$ such that $|H| = p^n$.

□

Remark: Sylow's First Theorem provides a partial converse of Lagrange's Theorem.

Example 11.184. Let $G = A_4$. $|G| = 2^2 \cdot 3$.

- There does not exist $H \leq G$ such that $|H| = 6$.
- There exists $H \leq G$ such that $|H| = 4$.
- There exists $H \leq G$ such that $|H| = 3$.

Example 11.185. Consider $G = S_3$, $|G| = 2 \cdot 3$. Let $P = \langle (12) \rangle, Q = \langle (13) \rangle$ be Sylow 2-subgroups of G.

Note that $(23)(12)(23)^{-1} = (13)$. In particular

$$(23)P(23)^{-1} = Q$$

Remark: Let G be a finite group. If $H \leq G$, then for all $g \in G$, $gHg^{-1} \leq G$, and $|gHg^{-1}| = |H|$. This is because $h \to ghg^{-1}$ is a bijection.

In particular, if H is a Sylow p-subgroup of G, then so is gHg^{-1} for all $g \in G$.

Theorem 11.186. If $|G| = p^n m, p \nmid m$. If P, Q are Sulow p-subgroups of G, then there exists $g \in G$ such that $gPg^{-1} = Q$.

i.e. This means that Sylow p-subgroups are conjugate one another.

Remark: If $|G| = p^n m, p \nmid m$, then we say $Syl_p(G) := \{H \leq G : H \text{ is a Sylow } p\text{-subgroup}\}$

1. Then G acts on $Syl_p(G)$ by conjugation, i.e. $g \cdot H = gHg^{-1}$
2. If $H \in Syl_p(G)$, then $stab(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$.

3. $[G : N_G(H)] = \frac{|G|}{|N_G(H)|} = \frac{|G|}{|stab(H)|} = |\mathcal{O}_H|$ By Orbit Stablizer Theorem.

Lemma 11.187. If $|G| = p^n m, p \nmid m$, $P \in Syl_p(G)$, let $Q \leq G$, $|Q| = p^k, k \leq n$, then $Q \cap N_G(P) = Q \cap P$.

Proof 11.188. We know that $P \subseteq N_G(P)$. So, $Q \cap P \subseteq Q \cap N_G(P)$.

Let $N := N_G(P)$, $H := Q \cap N$. Then, we want to show that $H \subseteq Q \cap P$.

Note $H \leq N$, $P \trianglelefteq N$. Hence, $HP \leq N$ (By assignment 1).

Then, $|HP| = \frac{|H| \cdot |P|}{|H \cap P|} = p^\ell, \ell \leq n$.

On the otherhand, we know $P \leq HP$, so $p^n = |P| \leq |HP| = p^\ell$. So, $n \leq \ell$.

Hence, $n = \ell$. As a result, $P = HP$.

So, $H \subseteq HP = P$. $H \subseteq Q \cap P$ as desired. □

Lemma 11.189. Let $|G| = p^n m, p \nmid m$, $P \in Syl_p(G)$, let $Q \leq G$, $|Q| = p^k, k \leq n$. Let $X = \{gPg^{-1} : g \in G\}$. Then, Q acts on X by conjugation. Say the orbit representatives are $P = P_1, P_2, ..., P_\ell$.

Then,

$$|X| = \sum_{i=1}^{\ell} [Q : Q \cap P_i]$$

Proof 11.190.

$$\begin{aligned} |X| &= \sum_{i=1}^{\ell} |\mathcal{O}_{P_i}| \\ &= \sum_{i=1}^{\ell} \frac{|Q|}{|stab(P_i)|} \text{ by Orbit Stablizer Theorem} \\ &= \sum_{i=1}^{\ell} \frac{|Q|}{|Q \cap P_i|} \\ &= \sum_{i=1}^{\ell} [Q : Q \cap P_i] \end{aligned}$$

Note that

$$\begin{aligned} stab(P_i) &= \{g \in Q : gP_ig^{-1} = P_i\} \\ &= N_G(P_i) \\ &= P_i \cap Q \text{ by the previous lemma} \end{aligned}$$

□

Here is the proof of **Sylow's Second Theorem**

Proof 11.191. Let $P, Q \in Syl_p(G)$. We want to show that there exists $g \in G$ such that $gPg^{-1} = Q$. Let $X = \{gPg^{-1} : g \in G\}$.

Say P acts on X by conjugation with orbit representatives $P = P_1, P_2, ..., P_\ell$.

So,

$$\begin{aligned} |X| &= \sum_{i=1}^{\ell} [P : P \cap P_i] \text{ by the previous lemma} \\ &= 1 + \sum_{i=2}^{\ell} \underbrace{[P : P \cap P_i]}_{>1, \text{ divides } |P|=p^n} \end{aligned}$$

So $|X| \equiv 1 \pmod{p}$.

Then, consider Q acting on X by conjugation with orbit representatives $P = Q_1, Q_2, ..., Q_k$. Suppose, for contradiction, $Q \neq Q_i$ for all $1 \leq i \leq k$.

Then,

$$\begin{aligned} |X| &= \sum_{i=1}^{k} [Q : Q \cap Q_i] \text{ by the previous lemma} \\ &= \sum_{i=1}^{k} \underbrace{[Q : Q \cap Q_i]}_{>1 \text{ divide } |Q|=p^n} \text{ since } Q \neq Q_i \\ &\equiv 0 \pmod{p} \end{aligned}$$

So, we reach a contradiction. So, there exists i such that $Q = Q_i$, where Q_i is a conjugate of P, i.e. $gPg^{-1} = Q_i$ for some $g \in G$. □

Recall $|G| = p^n m, p \nmid m$, $P \in Syl_p(G)$. we have

$$X = \{gPg^{-1} : g \in G\} = Syl_p(G)$$

by Sylow's Second Theorem.

We introduce the notation that $n_p = |Syl_p(G)|$. We prove that $n_p = |X| \equiv 1 \pmod{p}$.

Also, $n_p = |\mathcal{O}_P| = [G : N_G(P)]$ By Orbit Stablizer Theorem.

Theorem 11.192. Let $|G| = p^n m, p \nmid m$. Then, if $n_p = |Syl_p(G)|$

1. $n_p \equiv 1 \pmod{p}$
2. $n_p \mid m$

Proof 11.193. 1. Already proved above

2. We have $n_p = [G : N_G(P)], P \in Syl_p(G)$. So, $n_p \mid |G| = p^n m$.
   Then, we know that $\gcd(n_p, p^n) = 1$ since $n_p \equiv 1 \pmod{p}$. So, $n_p \mid m$

□

Remark: Let $|G| = p^n m, p \nmid m$, we have

1. $n_p = [G : N_G(P)]$ where $P \in Syl_p(G)$. Then, $n_p = 1$ if and only if $G = N_G(P)$, this happens if and only if $P \trianglelefteq G$.
2. Let $p \neq q$ be distinct primes. Let $p, q \mid |G|$. Let $P \in Syl_p(G), Q \in Syl_q(G)$. By Lagrange's Theorem, $P \cap Q = \{e\}$. In particular, $P \trianglelefteq G$, i.e. $n_p = 1$, and $Q \trianglelefteq G$, i.e. $n_q = 1$, then we have $PQ \trianglelefteq G$. Moreover, for $a \in P$ and $b \in Q$, we have $ab = ba$.
3. When $|G| = pm, p \neq m$. Let $P_1, P_2 \in Syl_p(G)$. If $P_1 \neq P_2$, then $P_1 \cap P_2 = \{e\}$.

In general, we can have $P_1, P_2 \in Syl_p(G)$ with $P_1 \cap P_2 \neq \{e\}$.

Example 11.194. Consider $p < q$ be primes such that $p \nmid q - 1$. Every group of order pq is cyclic.

The proof is as below: Let G be a group with $|G| = pq$. Then,

1. $n_p \equiv 1 \pmod{p}$, and $n_p \mid q$. This tells us $n_p \in \{1, q\}$. But $n_p \neq q$ since $q \not\equiv 1 \pmod{p}$.
2. $n_q \equiv 1 \pmod{q}$, and $n_q \mid p$. This tells us $n_q \in \{1, p\}$. But $n_p \neq q$ since $p \not\equiv 1 \pmod{q}$ as we have $p < q$.

Combining them together, we have $n_p = 1$ and $n_q = 1$.

Let $P \in Syl_p(G), Q \in Syl_q(G)$. Then, $P \trianglelefteq G$, and $Q \trianglelefteq G$.

Hence, $PQ \trianglelefteq G$, $|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = |P| \cdot |Q| = pq = |G|$.

So, $G = PQ \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ since $\gcd(p, q) = 1$.

Definition 11.195. We say G is **simple** if G has no proper non-trivial **normal** subgroups.

Example 11.196. We can prove that no group of order 56 is simple.

First, note that $56 = 2^3 \cdot 7$. By Sylow's Theorem, $n_7 \equiv 1 \pmod 7$, and we have $n_7 \mid 8$. This means $n_7 \in \{1, 8\}$.

1. If $n_7 = 1$, then G has a normal Sylow 7-subgroup.
2. Suppose $n_7 = 8$. If $P \neq Q \in Syl_7(G)$, then $P \cap Q = \{e\}$ since $7^2 \nmid 56$.

   This accounts for $8(7-1) = 48$ non-identity elements of G. This leaves $56-48 = 8$ elements unaccounted for. So, $n_2 = 1$, and so G has a normal Sylow 2-subgroup.