Group Theory

Langston Barrett

Spring 2017

Contents

- Instructor: Mckenzie West
- Textbook:
  - Title: Abstract Algebra, 3rd Edition
  - Author: David S. Dummit & Richard M. Foote
  - ISBN: 0471452343, 9780471452348

Definition 0.1. A diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[d, "g"] \\ C \arrow[r, "i"] & D \end{tikzcd}$$

is said to be commutative if $g \circ f = h \circ i$

1 Introduction to Groups

1.1 Basic Axioms and Examples

[Here, I skip some notions from Analysis, such as binary operations, associativity, commutativty, etc.]

Definition 1.1. A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying

1. Associativity: $\forall a, b, c \in G, (a \star b) \star c = a \star (b \star c)$
2. Identity: $\exists e \in G, \forall a \in G, e \star a = a \star e = a$
3. Inverse: $\forall a \in G, \exists a^{-1} \in G, a \star a^{-1} = a^{-1} \star a = e$

A group is commutative (abelian) if $\forall a, b \in G, a \star b = b \star a$.

Example 1.2.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a$
2. $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ are groups under $\cdot$ with $e = 1$ and $a^{-1} = 1/a$
3. Roots of unity$\cong$cyclic group of order $n$$\cong$the integers mod n. The roots of unity are $C_n \coloneqq \{x \in \mathbb{C} : x^n = 1\}$ and the operation is multiplication.

Definition 1.3. If $(A, \star), (B, \diamond)$ are groups, their direct product is

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

with the pointwise group operation

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$

and pointwise inversion:

$$(a_1, b_1)^{-1} = (a_1^{-1}, b_1^{-1})$$

Theorem 1.4 (Four Basic Group Properties)**.** Let $(G, \star)$ be a group. Then

1. The identity of G is unique.
2. Inverses are unique: $\forall a \in G, \exists! a^{-1}$
3. Inversion is involutive: $\forall a \in G, (a^{-1})^{-1} = a$
4. $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$

Proof.

1. Assume that $e_1, e_2 \in G$ are identities. Then

$$e_1 e_2 = e_1 \qquad\qquad e_1 e_2 = e_2$$

By the transitivity of $=$, $e_1 = e_2$.

2.

3.

$$
\begin{aligned}
(a \star b) \star (-b \star -a) &= a \star (b \star -b) \star -a && \text{Generalized associativity} \\
&= a \star e \star -a && \text{Definition of inverses} \\
&= a \star -a && \text{Left identity} \\
&= e && \text{Definition of inverses}
\end{aligned}
$$

So $-(a \star b) = (-b \star -a)$.

4.

$\square$

Theorem 1.5 (Left and Right Cancellation in Groups)**.** If $(G, \star)$ is a group, $\forall a, u, v \in G$,

$$au = av \implies u = v \qquad\qquad ua = va \implies u = v$$

Definition 1.6. The order of a group is its cardinality $|G|$. A group is finite if $|G| < \infty$.

The order of an element $x \in G$ is the smallest positive integer n such that $x^n = 1$. Equivalently, the order of $x \in G$ is the order of the (cyclic) subgroup of G generated by x, $|x| = |\langle x \rangle|$.

1.2 Dihedral Groups

Definition 1.7. Let $n \geq 3$. The dihedral group D_{2n} is the group of symmetries of a regular n-gon. It is of order $|D_{2n}| = 2n$.

If we let r be rotation by $2\pi/n$ radians and s be a flip across the vertical axis, these suffice in building D_{2n}.

Example 1.8. The symmetry group for the equalateral triangle is D_6.

Remark 1.9.

- $1, r, r^2, \ldots, r^{n-1}$ are all distinct, $|r| = n$.
- $1, s$ are distinct and $s^2 = 1$, so $|s| = 2$.
- $\forall 0 < i, j < n - 1, r^i \neq s^j$
- $rs = sr^{-1}$
- $D_{2n} = \left\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\right\}$

Definition 1.10. A subset $S \subseteq G$ is a set of generators of G if every element of G can be written as a product of elements of S and their inverses. We write this $G = \langle S \rangle$.

Example 1.11.

1. For D_{2n}, $S = \{r, s\}$ is a set of generators.
2. For $(\mathbb{Z}, +)$, $S = \{1\}$ is a set of generators.
3. For $(\mathbb{Q} \setminus \{0\}, \cdot)$, $S = \mathbb{Z} \setminus \{0\}$ generates $\mathbb{Q}$ multiplicatively.

Definition 1.12. Any equality satisfied by generators of a group (and the identity) is called a relation.

Example 1.13. In D_{2n}, $S = \{r, s\}$.

$$rs = sr^{-1} \qquad\qquad r^n = 1 = s^2$$

Any other relation on D_{2n} can be derived from these.

Definition 1.14. If S generates $(G, \star)$ and $R_1, R_2, \ldots, R_m$ are relations satisfied by the elements of S and the identity, such that all other relations satisfied by elements of S can be constructed (combined using the group operation, equalities, etc.) using these, then a presentation of G is

$$G = \langle S | R_1, R_2, \ldots, R_m \rangle$$

Note that this set $R_1, R_2, \ldots, R_m$ might not be minimal.

Example 1.15.

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

2. $$\mathbb{Z} = \langle 1 \rangle$$

3. A finite group of order 4:

$$G = \langle x, y | x^2 = y^2 = (xy)^2 = 1 \rangle$$

4. An infinite group:

$$H = \langle x, y | x^3 = y^3 = (xy)^3 = 1 \rangle$$

1.3 Symmetric Groups

Definition 1.16. If Ω is a non-empty set, the symmetric group S_Ω is the group of bijections $\varphi : \Omega \to \Omega$ where the operation is composition $\circ$.

If $\Omega = \{1, \ldots, n\}$ we write S_n for S_Ω. This is called the symmetric group of degree n.

An element $\varphi \in S_\Omega$ is called a permutation.

Note. What is the order of $|S_n|$?
Well if we fix the image of the first element, the next one has $n-1$ choices. Then the next one has $n-2$. So we get

$$|S_n| = n!$$

Remark 1.17. How can we write the symmetric group concisely? If we have

$$\begin{aligned} 1 &\to 4 \\ 2 &\to 3 \\ 3 &\to 2 \\ 4 &\to 1 \end{aligned}$$

We write

$$(1423)$$

But this doesn't work if we have

$$\begin{aligned} 1 &\to 2 \\ 2 &\to 1 \\ 3 &\to 4 \\ 4 &\to 3 \end{aligned}$$

for which we write

$$(12)(34)$$

Our algorithm is as follows:

1. Pick the smallest integer not in a cycle and call it a, our new cycle is now $(a$

2. Let $b = \varphi(a)$.

   (a) If $b = a$ then close the cycle as (a), return to (1)

   (b) Otherwise, write b next to a in the cycle as $(ab$

3. Let $c = \varphi(b)$

   (a) If $c = a$, close the cycle

   (b) Otherwise, write $(abc$ and repeat from step 3 with $b = c$.

4. Remove anything of the form (a), called 1-cycles.

Two cycles are disjoint if they have no integers in common.

Note. While S_n is in general non-abelian, disjoint cycles _.
Commute.

Note. The order of a cycle in S_n is also the _.
Least common multiple of the lengths of the cycles in its cycle decomposition.

1.4 Matrix Groups

Definition 1.18. A field is a set F together with binary operations $+$ and $\cdot$ such that $(F, +)$ is a commutative group with identity 0 and $(F \setminus \{0\}, \cdot)$ is also a commutative group with the the left distributive law between them:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

For any field F, $F^\times = F \setminus \{0\}$.

Example 1.19. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. So is $\mathbb{Z}/p\mathbb{Z}$ where p is prime:

- $\overline{0}$ is the additive identity
- $\overline{1}$ is the multiplicative identity
- $(\mathbb{Z}/p\mathbb{Z})^\times = \left\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\right\} = \mathbb{Z}/p\mathbb{Z} \setminus \left\{\overline{0}\right\}$

We notate this $\mathbb{F}_p$.

Definition 1.20. For each an arbitrary field F and $n \in \mathbb{N}$, let the general linear group of degree n (denoted $\mathrm{GL}_n(F)$) be the set of $n \times n$ matrices whose entries come from F and whose determinant is nonzero.

1.5 The Quaternion Group

Definition 1.21. The quaternion group Q_8 is defined to be

$$Q_8 \coloneqq \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows (for all $a \in Q_8$):

$$\begin{aligned}
1 \cdot a = a \cdot 1 &= a \\
-1 \cdot -1 &= 1 \\
-1 \cdot a = a \cdot -1 &= -a \\
i \cdot i = j \cdot j = k \cdot k &= -1
\end{aligned}$$

$$\begin{aligned}
i \cdot j &= k & j \cdot i &= -k \\
j \cdot k &= -i & k \cdot j &= -i \\
k \cdot i &= j & i \cdot k &= -j
\end{aligned}$$

Note. What are the generators for the Quaternion Group Q_8?
$\{i, j\}$ generates Q_8:

$$\begin{aligned}
i \cdot j &= k \\
j \cdot i &= k \\
i \cdot i &= j \cdot j = 1
\end{aligned}$$

1.6 Homomorphisms and Isomorphisms

Definition 1.22. Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $f : G \to H$ is a homomorphism if for all $x, y \in G$,

$$f(x \star y) = f(x) \diamond f(y)$$

Definition 1.23. Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $f : G \to H$ is an isomorphism if

1. f is a homomorphism
2. f is a bijection

In this case, G and H are isomorphic, and we write $G \cong H$

Example 1.24.
1. For any group G, $G \cong G$ with the identity map (and possibly others)

2. The exponential function $\exp : \mathbb{R} \to \mathbb{R}^+$ is an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$. It is a bijection because it has an inverse, and preserves the group operations: $e^{x+y} = e^x e^y$.
3. All symmetric groups of the same cardinality are isomorphic, and the converse holds as well.
4. Isomorphism is an equivalence relation (with transitivity being provided by composition and symmetry by inverses).

Note. What conditions need to hold for it to be *possible* that two groups are isomorphic?
For two groups $(G, \star)$ and $(H, \diamond)$, we need to have

1. $|G| = |H|$
2. G is commutative if and only if H is commutative
3. The order of elements is preserved under the isomorphism

Theorem 1.25 (Homomorphisms and Presentations)**.** If

a. $(G, \star)$ is a finite group or order n with presentation,

b. $S = \{s_1, \ldots, s_m\}$ is its set of generators,

c. H is another group with $r_1, \ldots, r_m \in H$,

d. every relation satisfied in G by s_i is satisfied in H by r_i,

then there is a unique homomorphism $f : G \to H$ which maps s_i to r_i. If H is generated by $\{r_1, \ldots, r_m\}$ and is also of order n, then $G \cong H$.

1.7 Group Actions

Definition 1.26. If $(G, \star)$ is a group and A is a set, then a group action by G on A is a map $(\cdot) : G \times A \to A$ denoted by $(g \cdot a)$ such that

1. For all $g_1, g_2 \in G, a \in A$,
$$g_1 \cdot (g_2 \cdot a) = (g_1 \star g_2) \cdot A$$
2. For all $a \in A$,
$$1 \cdot a = a$$

If G acts on A, we call A a G-set.

Example 1.27. 1. Scalar mutliplication: the map from $\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ given by

$$c \cdot \vec{v} = c\vec{v}$$

2. $(D_{2n}, \circ)$ and $A = \{1, \ldots, n\}$: Fix a labeling of the vertices of the n-gon, then for $\alpha \in D_{2n}$, we define $\sigma_\alpha : D_{2n} \times A \to A$ to be the permutation of these vertices that's induced by α.

3. $\mathrm{GL}_n(F)$ acts on F^n via applying the (invertible) linear transformation that corresponds to the matrix via the standard basis. In this way, $\mathrm{GL}_n(F) \hookleftarrow \mathrm{Aut}(F^n)$.

4. A group G acts on itself via left multiplication:

$$G \times G \longrightarrow G \qquad\qquad (g, x) \longmapsto gx$$

This gives the associated map

$$G \hookrightarrow \mathrm{Aut}(G)$$

which means that any finite group is isomorphic to a subgroup of $S_{|G|}$.

Note. What is the trivial group action of a group G on a set A?
For all $g \in G, a \in A$, define $g \cdot a = a$.

Theorem 1.28 (Group Actions as Permutations)**.** If

a. $(G, \cdot)$ is a group

b. A is a set

c. G acts on A

then $\sigma_g : A \to A, \sigma_g(a) = g \cdot a$ is a permutation (bijection) of A for all $g \in G$.

Proof.

$$\sigma_g \circ \sigma_{g^{-1}}(a) = \sigma_g(g^{-1} \cdot a) = g \cdot (g^{-1} \cdot a) = (gg^{-1}) \cdot a = 1 \cdot a = a$$

Since we chose g arbitrarily, we can swap g, g^{-1} to show that it is a double-sided inverse. Thus, σ_g has an inverse, and as so, is bijective. $\square$

Theorem 1.29. If

a. $(G, \cdot)$ is a group,

b. A is a set,

c. G acts on A, and

d. for each $g \in G$ we define the permutation

$$\sigma_g : A \longrightarrow A \qquad \text{by} \qquad \sigma(a) \coloneqq g \cdot a$$

then there is a group homomorphism

$$\varphi : G \longrightarrow S_A \qquad \text{defined by} \qquad \varphi(g) \coloneqq \sigma_g$$

Proof. Let $g_1, g_2 \in G, a \in A$. We want to show that

$$\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$$

We need:

$$\varphi(g_1 g_2)(a) = (\varphi(g_1) \circ \varphi(g_2))(a)$$

We have

$$\begin{aligned} \varphi(g_1 g_2) &= \sigma_{g_1 g_2}(a) \\ &= (g_1 g_2) \cdot a \\ &= g_1 \cdot (g_2 \cdot a) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) \\ &= (\varphi(g_1) \circ \varphi(g_2))(a) \end{aligned}$$

□

Remark 1.30. We have a correspondence from actions by G on A to homomorphisms from G to S_A. Can we invert this correspondence? Let $\varphi : G \to S_A$ be a homomorphism. Define a map

$$G \times A \longrightarrow A \qquad \text{by} \qquad (g, a) \longmapsto g \cdot a = \varphi(g)(a)$$

Claim: This is an action.

Proof.

$$\begin{aligned} 1_G \cdot a &= \varphi(1)(a) \\ &= \mathrm{id}_A(a) \qquad \text{(Homomorphisms preserve identities)} \\ &= a \end{aligned}$$

and

$$\begin{aligned}(g_1g_2)\cdot a &= \varphi(g_1g_2)(a)\\ &= (\varphi(g_1)\circ\varphi(g_2))(a) \quad \varphi \text{ is a homomorphism}\\ &= \varphi(g_1)(\sigma_{g_2}(a))\\ &= \sigma_{g_1}(\sigma_{g_2}(a))\end{aligned}$$

$\square$

Thus, we have a bijection between group actions by G on A and homomorphisms from $G \to S_A$.

Note. There is a bijection between group actions by a group G on a set A and __.
There is a bijection between group actions by a group G on a set A and homomorphisms from G into S_A, the symmetric group on A.

Definition 1.31. A group action of G on A is faithful if every $g \in G$ induces a unique permutation on A. Equivalently,

$$\varphi : G \longrightarrow S_A = \mathrm{Aut}(A) \qquad\qquad g \longmapsto (x \mapsto g\cdot x)$$

is injective. Equivalently, the kernel of the action is the identity.

Definition 1.32. For any group $(G,\cdot)$, we can define an action of G on G:

$$G\times G \longrightarrow G \qquad\qquad (g,a)\longmapsto gag^{-1}$$

This is called conjugation by G.

2 Subgroups

2.1 Definition and Examples

Definition 2.1. If $(G,\star)$ is a group, we say $H \subseteq G$ is a subgroup of G if $(H,\star|_H)$ is a group. We denote this $H \leqslant G$. If $H \neq G$, then H is a proper subgroup of G.

Lemma 2.2 (Necessary and Sufficient Conditions for Subgroups)**.** If $(G,\star)$ is a group, then $(H,\star|_H)$ is a group if and only if

1. $1_G \in H$

2. $h_1, h_2 \in H \implies h_1 \star h_2 \in H$

3. $h \in H \implies h^{-1} \in H$

Example 2.3. 1. If $G = (\mathbb{Z}, +)$, $n \in \mathbb{Z}$, then $n\mathbb{Z} = \{nm | m \in Z\}$ is a subgroup of G.

2. If $G = (D_8, \circ)$, then $\left\{1, r, r^2, r^3\right\} \leqslant G$. You can see the relationships between more subgroups in Figure **??**.

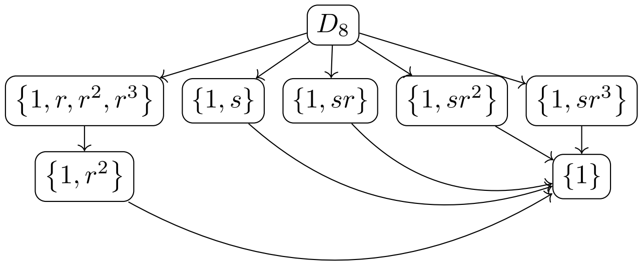

Figure 1: Some subgroups of D_8

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Definition 2.4. If $(G, \cdot)$ is a group and $a \in G$, then the centralizer of a is

$$C_G(a) \coloneqq \left\{g \in G | gag^{-1} = a\right\}$$

If $A \subseteq G$,

$$C_G(A) \coloneqq \left\{g \in G | gag^{-1} = h \;\forall a \in A\right\}$$

Note. What is the meaning of the centralizer of $A \subseteq G$?
It is the set of elements that commute with g.

$$xgx^{-1} = g \iff xg = gx$$

Theorem 2.5 (Centralizers and Subgroups)**.** If $H \subseteq G$ then $C_G(H)$ is a subgroup of G.

Proof. 1. Identity: $1a1^{-1} = a$ for all $a \in H$, so $1 \in C_G(H)$

2. Closure: Let $x, y \in C_G(H)$. Then for $z \in H$, we have

$$(xy)z(xy)^{-1} = xyzy^{-1}x^{-1} = xzx^{-1} = z$$

$\square$

Definition 2.6. If $(G, \cdot)$ is a group, then

$$Z(G) = \{g \in G | gx = xg \; \forall x \in G\} = C_G(G)$$

is the **center** (Zentrum) of G, the set of elements that commute with everything.

Definition 2.7. If $A \subseteq G$, we define

$$gAg^{-1} = \left\{gag^{-1} | a \in A\right\}$$

for any $g \in G$. The normalizer of A in G is

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

Lemma 2.8 (Relationship Between the Normalizer and Centralizer)**.** If $x \in C_G(A)$, then $xAx^{-1} = \left\{gag^{-1} | a \in A\right\} = A$, and so $C_G(A) \subseteq N_G(A)$.

Example 2.9.

$$C_{D_8}(r^2) = \left\{1, r, r^2, r^3, s, \ldots\right\} = D_8$$

since $sr^2 = r^{-2}s = r^2 s$.

$$C_{D_8}(\left\{sr, sr^3\right\}) = \left\{1, r^2, sr, sr^3\right\}$$

Definition 2.10. The kernel of an action of $(G, \cdot)$ on A is

$$\{g \in G | g \cdot a = a, \forall a \in A\}$$

Definition 2.11. If $(G, \cdot)$ acts on A and $a \in A$, then the stabilizer of a in G is

$$G_s := \{g \in G | ga = a\}$$

This is a subgroup of G.

2.3 Cyclic Groups and Cyclic Subgroups

Definition 2.12. A group G is cyclic if it is generated by one element, i.e. there is some $x \in G$ such that

$$G = \{x^n (= nx) : n \in Z\}$$

We write

$$G = \langle x \rangle$$

Lemma 2.13. Cyclic groups are commutative.

Example 2.14.

$$\mathbb{Z} = \langle 1 \rangle \qquad \mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle \qquad \langle r \rangle \leqslant D_{2n}$$

Lemma 2.15 (The Order of Cyclic Subgroups)**.** If

a. G is a group

b. $(H, \cdot)$ is a subgroup of G

c. H is cyclic

then

- $|H| = \infty$ if and only if $x^a \neq x^b$ for all $a, b \in \mathbb{Z}$ with $a \neq b$
- $|H| = n$ for $n \in \mathbb{N}_{>0}$ if and only if $H = \left\{1, x, \ldots, x^{n-1}\right\}$ and $|x| = n$.

Lemma 2.16. If $(G, \cdot, 1)$ is a group, then

1. If $x^n = 1$, $x^m = 1$, then $x^{\gcd(m,n)} = 1$
2. If $x^n = 1$, then $|x|\big|n$
3. If $|x| = \infty$, then $|x^a| = \infty$
4. If $|x| = n < \infty 0$, then $|x^a| = \frac{n}{\gcd(n,a)}$
5. If $|x| = \infty$, then $H = \langle x^a \rangle \iff a = \pm 1$
6. If $|x| = n < \infty$, then $H = \langle x^a \rangle \iff \gcd(n, a) = 1$

Theorem 2.17 (Classification of Cyclic Groups)**.** Any two cyclic groups of the same order are isomorphic.

1. If $\langle x \rangle$ and $\langle y \rangle$ are finite grouups of order n, then

$$\varphi : \langle x \rangle \longrightarrow \langle y \rangle \qquad\qquad \varphi(x^a) \longmapsto y^a$$

2. If $\langle x \rangle$ is an infinite group, then

$$\psi : \mathbb{Z} \longrightarrow \langle x \rangle \qquad\qquad \psi(n) \longmapsto x^n$$

is an isomorphism.

Theorem 2.18. Let $H = \langle x \rangle$ be a cyclic group. Then every subgroup of H is cyclic, and is generated by x^a where a is the smallest possible integer such that $x^a \in K$ (or $K = \{1\}$).

Additionally, if $|H| = \infty$, then the subgroups generated by distinct powers of x are not equal.

If $|H| = n < \infty$ then for every $d|n$, there is a unique subgroup of H of order d: $\langle x^{nd^{-1}} \rangle$.

2.4 Subgroups Generated by Subsets of a Group

Example 2.19. If $A = \{x\}$, then $\langle A \rangle = \langle x \rangle$

Lemma 2.20 (The Intersection of Subgroups)**.** If $\{H_i : i \in I\}$ is a collection of subgroups of a group $(G, \cdot, 1)$, then $H = \bigcap\{H_i : i \in I\}$ is a subgroup of G.

Definition 2.21. If $A \subseteq G$ for some group $(G, \cdot, 1)$, the subgroup generated by A is the intersection of all subgroups of G that contain A:

$$\langle A \rangle := \bigcap_{H \leqslant G,\ A \subseteq H} H$$

We write

$$\langle A \rangle = \langle a_1, \ldots, a_k \rangle$$

if $\{a_1, \ldots, a_k\}$ and

$$\langle A \cup B \rangle = \langle A, B \rangle$$

Theorem 2.22. Define

$$\overline{A} = \{a_1^{\varepsilon_1} \cdot \cdots \cdot a_n^{\varepsilon_n} | n \in \mathbb{Z}, \varepsilon_i \in \mathbb{Z}, a_i \in A\ \forall i\}$$

The set of all products of finite powers of a_i. Then $\overline{A} = \langle A \rangle$.

2.5 The Lattice of Subgroups of a Group

Definition. A lattice is a partially ordered set $(L, \leq)$ where every two-element subset of L has both a least upper bound (supremum/join) and a greatest lower bound (infimum/meet).

Naturally, it follows via induction that all finite subsets of L have suprema and infima.

Definition 2.23. The lattice of subgroups of a group G is a lattice which has subgroups of G as elements and set inclusion as a partial order. The join of two subgroups is the subgroup generated by their union, and the meet of two subgroups is their intersection.

3 Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Consider the map $\varphi : \mathbb{Z} \to Z_n$, the cyclic group of order n. For any $x^a \in \mathbb{Z}$, we have $\varphi^{-1}(x^a) = a + nm$ for all $m \in \mathbb{Z}$. We also have that $\varphi^{-1}(1) = nm$ and all other fibers are translates of this by elements of $\mathbb{Z}$.

Definition 3.1. The kernel of a group homomorphism $\varphi : G \to H$ is the set of elements that map to the identity:

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

This is a subgroup of G.

Definition 3.2. If G, H are groups and $\varphi : G \to H$ is a group homomorphism, then we can make a group out of the fibers (preimages) of elements of G:

- The elements are "fibers", or preimages of elements a of G under φ, denoted $\varphi^{-1}(a)$.
- The operation is defined by

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

we inherit associativity and identity for free from G.

If $K := \ker(\varphi)$, we call the above group the quotient group G/K (pronounced $G \mod K$).

Definition 3.3. Let $(H, \cdot, 1_H)$ be a subgroup of $(G, \cdot, 1_G)$ and $g \in G$. Then a left coset of H is

$$gH := \{gn | n \in H\}$$

and the right coset of H is

$$Hg := \{ng | n \in H\}$$

The set of left cosets of H in G is G/H

Theorem 3.4. Let $\varphi : G \to H$ be a group homomorphism with $K = \ker(\varphi)$ and let $\varphi^{-1}(a) \in G/K$ be the fiber above a. Then

1. For any $g \in \varphi^{-1}(a)$,

$$\varphi^{-1}(a) = \{gu | u \in K\} = gK$$

2. For any $g \in \varphi^{-1}(a)$,

$$\varphi^{-1}(a) = \{ug | u \in K\} = Kg$$

Definition 3.5. If $\varphi : G \to H$ is a group homomorphism and $\varphi^{-1}(x)$ is the preimage of some element $x \in H$, then an element $g \in \varphi^{-1}(x)$ is called a representative of $\varphi^{-1}(x)$, and we write $gK = \varphi^{-1}(x)$. Any element in a coset is called a representative of that coset.

Definition 3.6. Let $(G, \cdot, 1_G)$ be a group and A be a G-set. We can define an equivalence relation $\sim$ where

$$a \sim b \iff a = gb$$

for some $g \in G$. Then the equivalence class of $a \in A$ is the orbit of a under the action of G.

Theorem 3.7 (Left Cosets and Quotient Groups)**.** If

a. $(G, \star, 1_G), (H, \diamond, 1_H)$ are groups,

b. $\varphi : G \to H$ is a group homomorphism,

c. $K = \ker(\varphi)$

then the set G/K with the operation defined by

$$(gK) \bullet (hK) := (g \star h)K$$

for $g, h \in G$ forms a group.

Example 3.8. • Consider the groups $(\mathbb{Z}, +, 0)$ and Z_n, the cyclic group of order n. Then $\ker(\varphi) = n\mathbb{Z}$, all the multiples of n. So the quotient is $\mathbb{Z}/n\mathbb{Z}$.

- Consider the quotient of just one group: If we have $\varphi : G \to H$ where $\varphi(g) = 1$, then $\ker(\varphi) = G$, so $G/G \cong \{1\}$.
- What about the identity morphism $\varphi : G \to G, \varphi(g) = g$? Then $\ker(\varphi) = 1$, and $G/\{1\} \cong G$.
- How about the map $\varphi : \mathbb{R}^2 \to \mathbb{R}, \varphi(x, y) = x$? Then $\ker\varphi = \{(0, y) | y \in \mathbb{R}\} = \{0\} \times \mathbb{R}$ so our quotient group is $\mathbb{R}^2/\mathbb{R} \cong \mathbb{R}$.

Lemma 3.9 (Cosets of a Subgroup)**.** Let N be a subgroup of G. Then the set of left cosets of N forms a partition of G. Furthermore, for all $u, v \in G$, we have

$$uN = vN \iff v^{-1}u \in N$$

Lemma 3.10. If $(N, \cdot, 1_G)$ is a subgroup of $(G, \cdot, 1_G)$, then

1. The operation on the set of left cosets given by $uN \star gN = (uv)N$ is well-defined if and only if $gng^{-1} \in N$ for all $g \in G, n \in N$.
2. If this operation is well-defined, then the set of left cosets is a group under this operation with identity $1_G N$ and inverses $(gN)^{-1} = g^{-1}N$.

Definition 3.11. For a group $(G, \cdot, 1_G)$ and subgroup $(N, \cdot, 1_G)$ and elements $g \in G, n \in N$, the element gng^{-1} is called the conjugate of n by g. The set gNg^{-1} is the conjugate of N by g. If $gNg^{-1} = N$, then we say that g normalizes N. A subgroup N of a group G is normal if every element of G normalizes it: $\left\{gNg^{-1} | g \in G\right\} = N$, i.e. the left cosets of N form a group. We write this $N \trianglelefteq G$.

Lemma 3.12 (When is a Subgroup Normal?)**.** A subgroup N of a group G is normal if and only if it is the kernal of some homomorphism from G to some other group.

Definition 3.13. The map

$$\pi : G \longrightarrow N \qquad \text{defined by} \qquad \pi(g) := gN$$

is a group homomorphism, called the natural projection. Its kernel is N.

Definition 3.14. If $\overline{H}$ is a subgroup of G/N, the complete preimage of $\overline{H}$ is the preimage of H under the natural projection. It is a subgroup of G: $\pi^{-1}(\overline{H}) \leqslant G$, and contains N: $N \leqslant \pi^{-1}(H)$.

Note. For a group G, what is G/G?

$$G/G \cong 1_G$$

Note. For a group G, what is $G/1$?

$$G/1 \cong G$$

Note. All subgroups of an Abelian group are __.
All subgroups of an Abelian group are normal.

3.2 More on Cosets and Lagrange's Theorem

Another intro to cosets:

Definition 3.15. Let $(G, \cdot, 1)$ be a group and H a subgroup. Define a relation on a G by $x \sim y$ iff $y^{-1}x \in H$. This is an equivalence.

The left coset of H containing x is the equivalence class containing x under $\sim$, denoted xH.

Theorem 3.16 (Lagrange's Theorem)**.** If $(G, \cdot, 1)$ is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$, and the number of cosets of H in G is $|G|/|H|$.

Definition 3.17. If G is a finite group and H is a subgroup, then the positive integer

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

guaranteed by Lagrange's Theorem is the index of H in G.

More generally, the index of H in G is the number of left cosets of H in G.

Definition 3.18. If H, K are subgroups of G, then

$$HK := \{hk | h \in H, k \in K\} \subseteq G$$

and

$$hK := \{hk | k \in K\} \subseteq G$$

Lemma 3.19.

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

Lemma 3.20. If G is a group with subgroups of K, H, then HK is a subgroup of G if and only if $HK = KH$.

Theorem 3.21 (Cauchy's Theorem)**.** If

a. G is a finite group

b. $p \in \mathbb{N}$ is a prime dividing G

then G has an element of order p.

Theorem 3.22 (Groups of Prime Order)**.** If $(G, \cdot, 1)$ is a group of prime order, then G is cyclic.

Corollary: all groups of a given prime order are isomorphic.

Proof. Let $x \in G, x \neq 1$. Then $|x| = |\langle x \rangle| > 1$ and $|x| \big| |G|$. Since $|G|$ is prime, $|x| = p$ so $G = \langle x \rangle$. $\square$

Lemma 3.23 (Subgroup Products and the Normalizer)**.** Let $H, K \leqslant G$ with $H \leqslant N_G(K)$. Then $HK \leqslant G$.

3.3 The Isomorphism Theorems

Theorem 3.24 (First Isomorphism Theorem for Groups)**.** If $\varphi : G \to H$ is a group homomorphism, then $\ker \varphi \trianglelefteq G$ and $G / \ker \varphi \cong \varphi(G)$.

Corollary 3.25. If $\varphi : G \to H$ is a group homomorphism, then φ is injective if and only if $\ker \varphi = \{1\}$.

Theorem 3.26 (Second Isomorphism Theorem)**.** If

a. A, B, G are groups,

b. A, B are subgroups of G,

c. A is a subgroup of $N_G(B)$,

then $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and

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

Theorem 3.27 (Third Isomorphism Theorem)**.** Let $K \trianglelefteq H \trianglelefteq G$ and $K \trianglelefteq H$. Then

$$H / K \trianglelefteq G / K$$

and

$$(G/K) \Big/ (H/K) \cong G/H$$

Note. When does a group homomorphism $\Phi : G \to H$ factor through G/N? What does that even mean?
If $N \leqslant \ker\Phi$, then we can define a homomorphism

$$\varphi : G/N \longrightarrow H \qquad\qquad \varphi(gN) := \Phi(g)N.$$

This homomorphism is well-defined and unique. It is called the induced homomorphism. If we let

$$\pi : G \longrightarrow G/N \qquad\qquad \pi(g) := gN$$

be the natural projection, than for any Φ, the following diagram commutes:

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\Phi"] & G/N \arrow[d, dashed, "\varphi"] \\ & H \end{tikzcd}$$

3.4 The Hölder Program and Simple and Solvable Groups

Lemma 3.28 (Finite Groups and Elements of Prime Order)**.** Let $(G, \cdot, 1_G)$ be a finite commutative group and p a prime dividing $|G|$. Then $\exists g \in G$ such that $|g| = p$.

Definition 3.29. A group $(G, \cdot, 1)$ is simple if the only normal subgroups of G are the trivial ones $(\{1\}, G)$.

Theorem 3.30 (Feit-Thompson)**.** If G is an odd-order simple group, then $G \cong Z_p$ for some prime p. This result was ∼250 pages.

Definition 3.31. A group G is solvable if there is a chain of subgroups $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$ such that G_{i+1}/G_i is commutative for $i = 0, \ldots, s-1$.

Theorem 3.32. If

a. G is a group with normal subgroup N,

b. N is solvable, and

c. G/N is solvable,

then G is solvable.

3.5 Transpositions and the Alternating Group

Definition 3.33. A two-cycle in the symmetric group S_n is also called a transposition. We can write a general cycle $(a_1\ \dots\ a_m) \in S_n$ as

$$(a_1\ \dots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1}) \cdots (a_1 a_2)$$

i.e. the product of two-cycles. Thus, the symmetric group is generated by transpositions.

Definition 3.34. The alternating group is the subgroup of S_n containing all permutations that can be written as the product of an even number of transpositions.

Example 3.35. The alternating group is the subgroup of S_n that is made of permutations that are the product of an even number of transpositions.

Theorem 3.36 (The Order of $|S_n/A_n|$)**.** For all $n \geq 2$, $|S_n/A_n| = 2$.

4 Group Actions

4.1 Group Actions and Permutation Representations

Theorem 4.1. Let G be a finite group and p the smallest prime dividing $|G|$. Then any subgroup $H \subseteq G$ of index p is normal.

Note. The kernel of a group action $\cdot : G \times A \to A$ is the same as _.
The kernel of the associated permutation representation

$$\sigma_g : A \longrightarrow A \qquad\qquad \sigma_g(a) \coloneqq g \cdot a,$$

or the intersection of the stabilizers of all the $a \in A$.

Example 4.2. Consider S_n where $n \geq 3$. We have $A_n \leqslant S_n$ with $|S_n : A_n| = 2$. By the above theorem, $A_n \trianglelefteq S_n$, so S_n is not simple for $n \geq 3$.

Theorem 4.3 (Orbit-Stabilizer Coset Correspondence)**.** Let G act on A. Then the relation $a \sim b \iff \exists g \in G$ such that $a = gb$ is an equivalence relation on A. Let $G_a = \{g \in G | ga = a\}$ the stabilizer of a in G, and $G \cdot a = \{g \cdot a | g \in G\}$ the orbit of a in G. Then $|G \cdot a| = |G : G_a|$.

Definition 4.4. A group action is transitive if it has only one orbit.

4.2 Groups Acting on Themselves by Left Multiplication—Cayley's Theorem

Theorem 4.5 (Cayley's Theorem)**.** Every group G is isomorphic to some subgroup of a symmetric group. Specifically, if $|G| = n$, then G is isomorphic to a subgroup of S_n.

4.3 Groups Acting on Themselves by Conjugation—The Class Equation

Definition 4.6. For $a, b \in G$, we say that a is conjugate to b if $\exists g \in G$ such that $a = gbg^{-1}$. In fact, G acts on itself via conjugation:

$$\cdot : G \times G \longrightarrow G \qquad\qquad (g, a) \overset{\cdot}{\longmapsto} gag^{-1}$$

The orbits of this action are called conjugation classes, often denoted $[a] = \{gag^{-1} : g \in G\}$.

Two sets are conjugate if $\exists g \in G$ such that $S = gTg^{-1}$.

Note. What is the conjugation class of $c \in C_G(G) = Z(G)$?
$\{c\}$, since it commutes with everything, $gcg^{-1} = c$, $\forall g$.

Note. A normal subgroup is conjugate to _.
itself.

Theorem 4.7. The number of conjugates of $S \subseteq G$ is $|G : N_G(S)|$. In particular, the number of conjugates of $s \in G$ is $|G : C_G(s)|$.

Theorem 4.8 (The Class Equation)**.** Let G be a finite group and $g_1, \ldots, g_r \in G$ be representatives of the conjugacy classes of G not contained in $C_G(G)$. Then

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

Theorem 4.9. If G is a group with order p^a for some prime p, then $C_G(G)$ is non-trivial.

Proof. Since $|G|$ is p^a, if $g_i \notin C_G(G)$, then $|G : C_G(G)| = p^b$ for some $b < a$. Then the class equation gives

$$p^a = |C_G(G)| + pn$$

for some $0 < n < a$, so $p \big| |C_G(G)|$. $\square$

Corollary 4.10. If $|G| = p^2$ for some prime p, then G is commutative. Moreover, G is isomorphic to Z_{p^2} or $Z_p \times Z_p$.

4.3.1 Conjugacy in S_n

Lemma 4.11. If $\sigma, \tau \in S_n$ and

$$(a_1\ a_2\ a_3\ \dots)(b_1\ b_2\ b_3\ \dots)$$

then

$$\tau \circ \sigma \circ \tau^{-1} = (\tau a_1\ \tau a_2\ \tau a_3\ \dots)(\tau b_1\ \tau b_2\ \tau b_3\ \dots)$$

Definition. Let $\sigma \in S_n$ and assume σ can be written as disjoint cycles of lengths $n_1 \leq n_2 \leq \dots \leq n_k$. Then $n_1, \dots, n_k$ is the cycle type of σ.

4.4 Automorphisms

Definition 4.12. An isomorphism of a group onto itself is an automorphism. The set of automorphisms of a group G is itself a group under composition, denoted $\mathrm{Aut}(G)$.

Theorem 4.13 (Conjugating a normal subgroup)**.** If H is a normal subgroup of G, then G acts on H by conjugation:

$$G \times H \longrightarrow H \qquad\qquad (g, h) \longmapsto ghg^{-1}$$

and for each $g \in G$, conjugation by g is an automorphism of H. The permutation representation of this action is a homomorphism of G into $\mathrm{Aut}(H)$.

Definition 4.14. If G is a group, then conjugation of G by g is an inner automorphism. The subgroup of $\mathrm{Aut}(G)$ consisting of all inner automorphisms is denoted $\mathrm{Inn}(G)$.

Definition 4.15. A subgroup H of a group G is characteristic if every automorphism of G maps H to itself, i.e. $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(G)$.

Theorem 4.16 (Properties of characteristic subgroups)**.**

1. Characteristic subgroups are normal.
2. If H is the unique subgroup of G of a given order, then H is characteristic in G.
3. If K is characteristic in H and $H \trianglelefteq G$, then $K \trianglelefteq G$.

4.5 The Sylow Theorems

Definition 4.17. A group G of prime order p is a p-group, a subgroup of G of prime order p is a p-subgroup, and if G is of order $p^a m$ where p is prime and $p \nmid m$, then a subgroup of order p^a is a Sylow p-subgroup of G.

Theorem 4.18 (Sylow's theorem (simplified))**.** If

a. $(G, \cdot, 1)$ is a group,

b. $|G| = p^a m$ for prime p with $p \nmid m$,

then there are Sylow p-subgroups of G, they are all conjugate to one another, and the number of Sylow p-subgroups is of the form $1 + kp$ for $k \in \mathbb{N}$.

Corollary 4.19. If P is a Sylow p-subgroup of G, then the following are equivalent:

1. P is the unique p-subgroup of G,
2. P is normal in G, and
3. P is characteristic in G.