2021 UChicago Math REU Notes: Final Paper

Steven Labalme

July 23, 2021

Contents

Part I

Dummit and Foote

Chapter 0

Preliminaries

0.1 Basics

7/9:
- Know the basics of set theory.
- **Order** (of a set A): The cardinality of A.
- $\mathbb{Z}$ denotes the integers because the German word for numbers is "Zahlen."
- $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ denote the positive nonzero elements of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, respectively.
- **Fiber** (of f over b): The preimage of $\{b\}$ under f.
- **Left inverse** (of f): A function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A.
- **Right inverse** (of f): A function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B.

7/10:
- f is injective $\iff$ f has a left inverse.
- f is surjective $\iff$ f has a right inverse.
- f is a bijection $\iff$ f has a 2-sided inverse (or simply inverse).
- **Permutation** (of a set A): A bijection from A to itself.
- **Extension** (of g to B): The function $f : B \to C$ where $A \subset B$, $g : A \to C$, and $f|_A = g$.

0.2 Properties of the Integers

- "The connection between the greatest common divisor d and the least common multiple l of two integers a and b is given by $dl = ab$."
- **Euclidean algorithm**: A procedure for finding the greatest common divisor of two integers a and b by iterating the division algorithm:

$$\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
r_0 &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

  This yields $\gcd(a,b) = r_n$.

- Note that $(a, b) = ax + by$ as a consequence of the Euclidean algorithm (write r_n in terms of the other quantities iteratively).
  - x and y are not unique for any two integers a, b.
- If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.
- **Fundamental Theorem of Arithmetic**: If $n \in \mathbb{Z}$ and $n > 1$, then n can be factored uniquely into the product of primes, i.e., there are distinct primes $p_1, p_2, \dots, p_s$ and positive integers $\alpha_1, \alpha_2, \dots, \alpha_s$ such that
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$
- Let a, b be positive integers such that
$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \qquad\qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$
are their prime factorizations (we let $\alpha_i, \beta_j \geq 0$ so that we can express both as the product of the same primes). Then
$$\begin{aligned}\gcd(a, b) &= p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_s^{\min(\alpha_s,\beta_s)}\\ \operatorname{lcm}(a, b) &= p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_s^{\max(\alpha_s,\beta_s)}\end{aligned}$$
- **Euler $\boldsymbol{\varphi}$-function**: The function $\varphi : \mathbb{Z}^+ \to \mathbb{N}$ defined by $\varphi(n)$ is the number of positive integers $a \leq n$ such that $(a, n) = 1$.
  - If p prime, then $\varphi(p) = p - 1$.
  - If p prime and $a \geq 1$, then $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1)$.
  - If $(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.
  - If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, then
$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s})\\ &= p_1^{\alpha_1-1}(p_1 - 1)p_2^{\alpha_2-1}(p_2 - 1) \cdots p_s^{\alpha_s-1}(p_s - 1)\end{aligned}$$

0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

- Define $\sim$ on $\mathbb{Z}$ by $a \sim b \iff n \mid (b - a)$.
  - $\sim$ is an equivalence relation.
  - If $a \sim b$, we write $a \equiv b \bmod n$[1].
- **Congruence class** (of a): The equivalence class $\bar{a}$ of a mod n. *Also known as* **residue class**.
$$\begin{aligned}\bar{a} &= \{a + kn \mid k \in \mathbb{Z}\}\\ &= \{a, a \pm n, a \pm 2n, a \pm 3n, \dots\}\end{aligned}$$
  - There are n distinct equivalence classes mod$n$.
- **Integers modulo $\boldsymbol{n}$**: The set of equivalence classes $\mathbb{Z}/n\mathbb{Z}$[2] under the equivalence relation $\sim$. *Also known as* **integers mod $\boldsymbol{n}$**.
- **Reducing $\boldsymbol{a}$ mod $\boldsymbol{n}$**: The process of finding the equivalence class mod$n$ of some integer a.
- **Least residue** (of a mod n): The smallest nonnegative number congruent to a mod n.

[1] a is congruent to $b \mod n$.
[2] The motivation for this notation will become clear in the discussion of quotient groups and quotient rings.

- **Modular arithmetic** (on $\mathbb{Z}/n\mathbb{Z}$): The addition and multiplication operations defined by

$$\bar{a} + \bar{b} = \overline{a+b} \qquad\qquad \bar{a} \cdot \bar{b} = \overline{ab}$$

  for all $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$.

- $(\mathbb{Z}/n\mathbb{Z})^\times$ is the collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$, i.e.,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists\, \bar{c} \in \mathbb{Z}/n\mathbb{Z} : \bar{a} \cdot \bar{c} = \bar{1}\}$$

  - It can be proven that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of residue classes whose representatives are relatively prime to n.
  - Thus, $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}$.
  - Let a be an integer that is relatively prime to n. Then the Euclidean algorithm generates integers x, y such that $ax + ny = 1$. But this implies that $ax = 1 + (-y)n$, i.e., $ax \equiv 1 \bmod n$, so that $\bar{x}$ is the multiplicative inverse of $\bar{a}$.

Chapter 1

Introduction to Groups

1.1 Group Theory

- "One of the essential characteristics of mathematics is that after applying a certain algorithm or method of proof, one then considers the scope and limits of the method. As a result, properties possessed by a number of interesting objects are frequently abstracted and the question raised; can one determine *all* the objects possessing these properties? Attempting to answer such a question also frequently adds considerable understanding of the original objects under consideration."
- Motivation?

1.2 Basic Axioms and Examples

7/12:

- **Binary operation** (on a set G): A function $\star : G \times G \to G$.
- **Closed** (subset $H \subset G$ under $\star$): A subset $H \subset G$ such that $a \star b \in H$ for all $a, b \in H$, where $\star$ is a binary operation on G.
  - Alternatively, we can require that $\star|_H$ be a binary operation on H.
- If $\star$ is an associative (respectively, commutative) binary operation on G and $\star|_H$ is a binary operation on $H \subset G$, then $\star$ is associative (respectively, commutative) on H as well.
- **Group**: An ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
  (i) Associativity: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.
  (ii) Identity: There exists an element $e \in G$ such that for all $a \in G$, $a \star e = e \star a = a$.
  (iii) Inverse: For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.
- **Abelian** (group): A group $(G, \star)$ such that for all $a, b \in G$, $a \star b = b \star a$. *Also known as* **commutative**.
- Axiom (ii) implies that G is nonempty.
- **Direct product** (of $(A, \star)$ and $(B, \diamond)$): The group $A \times B$ whose elements are those in the Cartesian product
  $$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$
  and whose operation is defined component-wise by
  $$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$
- Let G be a group under the operation $\star$.

Proposition 1.1.

(1) *The identity of G is unique.*

(2) *For each $a \in G$, a^{-1} is uniquely determined.*

(3) $(a^{-1})^{-1} = a$ *for all* $a \in G$.

(4) $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$.

(5) *Generalized associative law: For any $a_1, \dots, a_n \in G$, the value of $a_1 \star \cdots \star a_n$ is independent of how the expression is bracketed.*

- Let G be a group and let $a, b \in G$.

  Proposition 1.2. *The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in G, i.e.,*

  (1) *If $au = av$, then $u = v$;*

  (2) *If $ub = vb$, then $u = v$.*

- **Order** (of an object $x \in G$): The smallest positive integer n such that $x^n = 1$. *Denoted by* $|\boldsymbol{x}|$.
  - We say x is of order n.
  - If no such n exists, the order of x is defined to be infinity and x is said to be of infinite order.
- $|g| = 1 \iff g = e$.
- Is $|\bar{x}|$ for $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ equal to $\gcd(x, n)$?
- **Multiplication table** (of a finite group G): The $n \times n$ matrix whose i, j entry is the group element $g_i g_j$, where $G = \{g_1, \dots, g_n\}$ and $g_1 = e$. *Also known as* **group table**.

Exercises

5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

Proof. Let n be an arbitrary natural number such that $n > 1$. Consider $\bar{0} \in \mathbb{Z}/n\mathbb{Z}$. Since $\bar{x} \cdot \bar{0} = \bar{0}$ for all $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$, there is no element $\bar{0}^{-1} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{0} \cdot \bar{0}^{-1} = \bar{1}$. Thus, there is clearly no multiplicative inverse for $\bar{0}$ in $\mathbb{Z}/n\mathbb{Z}$, contradicting axiom (iii). □

6. Determine which of the following sets are groups under addition:

(a) The set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd.

Answer. Yes.
Closure: Let $\frac{a}{b}, \frac{c}{d}$ be two such rational numbers. Then since the product of two odd numbers is odd, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ is also an element of this set.
Axiom (i): As stated in the text, the associativity of a closed subset of a group under the same operation follows from the associativity of the original group.
Axiom (ii): Identity is 0.
Axiom (iii): Inverse of $\frac{a}{b}$ is $-\frac{a}{b}$, which is also clearly in the set since b is consistently odd. □

(b) The set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even.

Answer. Yes.
Symmetric to (a). □

(c) The set of rational numbers of absolute value < 1.

Answer. No.
Not closed: $|\frac{2}{3}+\frac{2}{3}|=|\frac{4}{3}|\geq 1$, for instance. $\square$

(d) The set of rational numbers of absolute value ≥ 1 together with 0.

Answer. No.
Not closed: $|\frac{3}{2}+(-\frac{1}{1})|=|-\frac{1}{2}|=\frac{1}{2}<1$, for instance. $\square$

(e) The set of rational numbers with denominators equal to 1 or 2.

Answer. Yes.
Closed: $\text{lcm}(1,1)=1$, $\text{lcm}(1,2)=2$, and $\text{lcm}(2,2)=2$, so the denominator stays within the constraints of the set.
Axioms (i-iii): Symmetric to (a). $\square$

(f) The set of rational numbers with denominators equal to 1, 2, or 3.

Answer. No.
Not closed: $\text{lcm}(2,3)=6\notin\{1,2,3\}$, so $\frac{1}{2}+\frac{1}{3}=\frac{5}{6}$, for instance. $\square$

8. Let $G=\{z\in\mathbb{C}\mid z^n=1\text{ for some }n\in\mathbb{Z}^+\}$.

(a) Prove that G is a group under multiplication (called the group of **roots of unity** in $\mathbb{C}$).

Proof. Closed: Let $z_1,z_2\in G$ such that $z_1^n=1$ and $z_2^m=1$. Consider these complex numbers in the forms $z_1=r_1\mathrm{e}^{i\theta_1}$ and $z_2=r_2\mathrm{e}^{i\theta_2}$ (note that $r_1=r_2=1$ since if not, repeated exponentiation would change the magnitude of z^n vs. z^{2n}, etc.[1]). It follows that $z_1^n=\mathrm{e}^{in\theta_1}=1$ and $z_2^m=\mathrm{e}^{im\theta_2}=1$. Thus, $n\theta_1\equiv 0\bmod 2\pi$ and $m\theta_2\equiv 0\bmod 2\pi$. Consequently, $nm\theta_1\equiv 0\bmod 2\pi$ and $nm\theta_2\equiv 0\bmod 2\pi$. But this implies that $nm(\theta_1+\theta_2)\equiv 0\bmod 2\pi$, i.e., that nm is an integer such that $(z_1z_2)^{nm}=\mathrm{e}^{i(nm(\theta_1+\theta_2))}=1$, as desired.
Axiom (i): As stated in the text, the associativity of a closed subset of a group under the same operation follows from the associativity of the original group.
Axiom (ii): Clearly, $1=1+0i\in\mathbb{C}$ and $1^1=1$, so $1\in G$. Additionally, by the definition of 1, $z\cdot 1=1\cdot z=z$, as desired.
Axiom (iii): Let $z\in G$ be arbitrary. Choose $z^{-1}=z^{n-1}$. Then

$$\begin{aligned}z\cdot z^{-1}&=z\cdot z^{n-1}\\&=z^n\\&=1\\&=z^n\\&=z^{n-1}\cdot z\\&=z^{-1}\cdot z\end{aligned}$$

as desired. $\square$

(b) Prove that G is not a group under addition.

Proof. By part (a), $1\in G$. However, $1+1=2\notin G$ since 2^n grows exponentially and never equals 1. $\square$

15. Prove that $(a_1a_2\cdots a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\cdots a_1^{-1}$ for all $a_1,a_2,\dots,a_n\in G$.

[1] This notion can be formalized in a contradiction argument.

Proof. We induct on n. For the base case $n = 2$, we have by Proposition 1.4 that $(a_1a_2) = a_2^{-1}a_1^{-1}$, as desired. Now suppose inductively that we have proven the claim for n; we now seek to prove it for $n+1$. But we have that

$$\begin{aligned}(a_1a_2\cdots a_{n+1})^{-1} &= a_{n+1}^{-1}(a_1a_2\cdots a_n)^{-1} && \text{Proposition 1.4}\\ &= a_{n+1}^{-1}a_n^{-1}\cdots a_1^{-1} && \text{Hypothesis}\end{aligned}$$

as desired. ☐

24. If a and b are commuting elements of G, prove that $(ab)^n = a^nb^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]

Proof. We divide into three cases ($n = 0$, $n \in \mathbb{N}$, $n \in -\mathbb{N}$).

If $n = 0$, then $(ab)^0 = 1 = 1 \cdot 1 = a^0b^0$, as desired.

If $n \in \mathbb{N}$, we induct on n. For the base case $n = 1$, we have that $(ab)^1 = ab = a^1b^1$ trivially, as desired. Now suppose inductively that we've proven the claim for n; we now seek to prove it for $n+1$. But we have that

$$\begin{aligned}(ab)^{n+1} &= (ab)^n(ab)\\ &= a^nb^nab\\ &= a^nab^nb\\ &= a^{n+1}b^{n+1}\end{aligned}$$

as desired.

If $n \in -\mathbb{N}$, then $-n \in \mathbb{N}$. Therefore, by the above,

$$\begin{aligned}(ab)^n &= \frac{1}{(ab)^{-n}}\\ &= \frac{1}{a^{-n}b^{-n}}\\ &= \frac{1}{a^{-n}} \cdot \frac{1}{b^{-n}}\\ &= a^nb^n\end{aligned}$$

as desired. ☐

1.3 Dihedral Groups

- **Dihedral group**: A group whose elements are symmetries of geometric objects.
- D_{2n} denotes the group of symmetries of a regular n-gon.
- Note that $|D_{2n}| = 2n$.
- D_{2n} is related to S_n by labeling the vertices of the n-gon 1 through n.
- "Since symmetries are rigid modtions, one sees that once the position of the ordered pair of vertices 1,2 has been specified, the action of the symmetry on all remaining vertices is completely determined."
- Fix a regular n-gon centered at the origin in the xy-plane and label the vertices consecutively from 1 to n in a clockwise manner. Let r be the rotation clockwise about the origin through $\frac{2\pi}{n}$ radians. Let s be the reflection about the line of symmetry through vertex 1 and the origin. Then
  (1) $1, r, r^2, \dots, r^{n-1}$ are distinct and $r^n = 1$, so $|r| = n$.

(2) $|s| = 2$.

(3) $s \neq r^i$ for any i.

(4) $sr^i \neq sr^j$ for all $0 \leq i,\ j \leq n-1$ with $i \neq j$, so

$$D_{2n} = \{1, \dots, r^{n-1}, s, \dots, sr^{n-1}$$

In other words, each element of D_{2n} can be writen uniquely in the form $s^k r^i$ for some $k = 0, 1$ and $0 \leq i \leq n-1$.

(5) $rs = sr^{-1}$. Thus, r, s do not commute so D_{2n} is non-abelian.

(6) $r^i s = sr^{-i}$ for all $0 \leq i \leq n$. This indicates how to commute s with powers of r.

- Note that r, s in the above example are **generators**, which will only be rigorously introduced later but are useful now and thus used informally.
- **Generators** (of G): A subset $S \subset G$ with the property that every element in G can be written as a (finite) product of elements of S and their inverses. *Denoted by* $G = \langle \boldsymbol{S} \rangle$.
  - We write that "G is generated by S" or "S generates G."
  - Examples: $\mathbb{Z} = \langle 1 \rangle$ and $D_{2n} = \langle r, s \rangle$.
- **Relation**: An equation in a general group G that the generators satisfy.
  - Example: In D_{2n}, we have $r^n = 1$, $s^2 = 1$, and $rs = sr^{-1}$.
- **Presentation** (of G): The set S of generators of G along with the relations $R_1, \dots, R_m$, where each R_i is an equation in the elements from $S \cup \{1\}$, such that any relation among the elements of S can be deduced from these. *Denoted by* $G = \langle \boldsymbol{S} \mid \boldsymbol{R_1, \dots, R_m} \rangle$.
  - Example: $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$.
- List examples and works with **collapsing** presentations, i.e., ones in which some important relations are consequences of others.

1.4 Symmetric Groups

- **Symmetric group** (on the set Ω): The group $(S_\Omega, \circ)$, where S_Ω is the set of all bijections from a nonempty set Ω to itself and $\circ$ is function composition. *Also known as* **permutations** (of Ω).
  - We write $\sigma \in S_\Omega$ and let $1 \in S_\Omega$ be the identity function defined by $1(a) = a$ for all $a \in \Omega$.
  - If $\Omega = [n]$, then we denote S_Ω by S_n.
- $|S_n| = n!$.
- **Cycle**: A string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers).
  - The cycle $(a_1\ a_2\ \dots\ a_m)$ is the permutation which sends a_i to a_{i+1} for all $1 \leq i \leq m-1$ and sends a_m to a_1.
- **Cycle decomposition** (of σ): The product of all cycles, often written in the form

$$(a_1\ a_2\ \dots\ a_{m_1})(a_{m_1+1}\ a_{m_1+2}\ \dots\ a_{m_2}) \dots (a_{m_{k-1}+1}\ a_{m_{k-1}+2}\ \dots\ a_{m_k})$$

- Cycle decomposition algorithm:
  1. To start a new cycle, pick the smallest element of $[n]$ which has not yet appeared in a previous cycle — call it a (if you are just starting, choose $a = 1$); begin the new cycle: "$(a$".

2. Read off $\sigma(a)$ from the given description of σ — call it b. If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle — return to step 1. If $b \neq a$, write b next to a in this cycle: "$(a\ b$".
3. Read off $\sigma(b)$ from the given description of σ — call it c. If $c = a$, close the cycle with a right parenthesis to complete the cycle — return to step 1. If $c \neq a$, write c next to b in this cycle: "$(a\ b\ c$". Repeat this step using the number c as the new value for b until the cycle closes.
4. Remove all cycles of **length** 1.

- Example:

$$\begin{array}{cccc} \sigma(1) = 12 & \sigma(2) = 2 & \sigma(3) = 3 & \sigma(4) = 1 \\ \sigma(5) = 11 & \sigma(6) = 9 & \sigma(7) = 5 & \sigma(8) = 10 \\ \sigma(9) = 6 & \sigma(10) = 4 & \sigma(11) = 7 & \sigma(12) = 8 \end{array}$$

  becomes
$$\sigma = (1\ 12\ 8\ 10\ 4)(5\ 11\ 7)(6\ 9)$$

- **Length** (of a cycle): The number of integers which appear in it.
- ***t*-cycle**: A cycle of length t.
- **Disjoint** (cycles): Two cycles that have no numbers in common.
- The convention of removing all cycles of length 1 makes it so that any cyclic decomposition essentially represents a function $\sigma : \mathbb{N} \to \mathbb{N}$.
- For any $\sigma \in S_n$, the cyclic decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order.
  - Continuing with the above example, $\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(7\ 11\ 5)(9\ 6)$.
- S_n is a non-abelian group for all $n \geq 3$.
- Disjoint cycles commute.
- The order of a permutation is the lcm of the lengths of the cycles in its cycle decomposition.

1.5 Matrix Groups

- Since $\mathbb{Z}/p\mathbb{Z}$, p prime, is a finite field, we denote it $\mathbb{F}_p$.
- **Field**: A set F together with two binary operations $+$ and $\cdot$ on F such that $(F, +)$ is an abelian group (call its identity 0), $(F - \{0\}, \cdot)$ is also an abeilan group, and the following distributive law holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in F$.
- $\boldsymbol{F^\times}$: The set $F - \{0\}$ where F is a field.
- **General linear group of degree *n***: The set of all $n \times n$ matrices, where $n \in \mathbb{Z}^+$, whose entities come from the field F and whose determinant is nonzero. *Denoted by* $\boldsymbol{GL_n(F)}$.

1.6 The Quaternion Group

- **Quaternion group**: The group
$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$
with product $\cdot$ computed as follows:
$$\begin{aligned} 1 \cdot a = a \cdot 1 &= a && \text{for all } a \in Q_8 \\ (-1) \cdot (-1) &= 1 \\ (-1) \cdot a = a \cdot (-1) &= -a && \text{for all } a \in Q_8 \\ i \cdot i = j \cdot j = k \cdot k &= -1 \end{aligned}$$
$$\begin{aligned} i \cdot j &= k & j \cdot k &= i & k \cdot i &= j \\ j \cdot i &= -k & k \cdot j &= -i & i \cdot k &= -j \end{aligned}$$
- Q_8 is a non-abelian group of order 8.

1.7 Homomorphisms and Isomorphisms

- **Homomorphism**: A map $\varphi : G \to H$ such that $\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$ for all $x, y \in G$, where $(G, \star)$ and $(H, \diamond)$ are groups.
  - Intuitively, a map is a homomorphism if it respects the group structures of its domain and codomain.
- **Isomorphism**: A map $\varphi : G \to H$ such that φ is a homomorphism and a bijection.
  - If such a φ exists, we write that G and H are isomorphic, are of the same isomorphism type, and that $G \cong H$.
  - Intuitively, such a map implies that G and H are the same group; they simply have relabeled elements.
- The existence of an isomorphism between two groups implies that any property of G that can be derived from the group axioms also holds for H, and vice versa.
- $\cong$ is an equivalence relation.
- **Isomorphism class**: An equivalence class of a nonempty collection $\mathcal{G}$ of groups under $\cong$.
- $|\triangle| = |\Omega| \iff S_\triangle \cong S_\Omega \iff |S_\triangle| = |S_\Omega|$.
- **Classification theorem**: A theorem stating what properties of a structure specify its isomorphism type.
  - For example, a general classification theorem would assert that if G is an object with some structure (such as a group) and G has property $\mathcal{P}$, then any other similarly structured object (group) X with property $\mathcal{P}$ is isomorphic to G.
- If $\varphi : G \to H$ is an isomorphism, then
  1. $|G| = |H|$.
  2. G is abelian iff H is abelian.
  3. For all $x \in G$, $|x| = |\varphi(x)|$.
- Let G be a finite group of order n for which we have a presentation and let $S = \{s_1, \dots, s_m\}$ be the generators. Let H be another group and $\{r_1, \dots, r_m\}$ be elements of H. Suppose that any relation satisfied in G by the s_i is also satisfied in H when each s_i is replaced by r_i. Then there is a unique homomorphism $\varphi : G \to H$ which sends $s_i \mapsto r_i$.

1.8 Group Actions

- **Group action** (of a group G on a set A): A map $\cdot : G \times A \to A$ such that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$, and such that $1 \cdot a = a$ for all $a \in A$.
- What is a group action?
- Let G act on A, and for each $g \in G$, define $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. Then
  1. For each fixed $g \in G$, σ_g is a permutation of A;

     Proof. We prove that σ_g has a two-sided inverse; it follows that σ_g is a permutation. Let $g \in G$ be arbitrary. Then by Axiom (iii), there exists g^{-1}. Therefore,

     $$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= g^{-1} \cdot (g \cdot a) \\ &= (g^{-1} \cdot g) \cdot a \\ &= 1 \cdot a \\ &= 1\end{aligned}$$

     We can prove something similar in the other direction. □
  2. The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

     Proof. Let $\varphi : G \to S_A$ be defined by $\varphi(g) = \sigma_g$ for all $g \in G$. To prove that φ is a homomorphism, it will suffice to show that $\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2)$ for all $g_1, g_2 \in G$. To verify the equality of functions, we must show that for all $a \in A$, $\varphi(g_1 \cdot g_2)(a) = (\varphi(g_1) \circ \varphi(g_2))(a)$. Let a be an arbitrary element of A. Then

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

     □
- Intuitively, a group action of G on A means that every element $g \in G$ acts as a permutation on A in a manner consistent with the group operations in G.
- **Permutation representation** (associated to the group action $\cdot$): The homomorphism $\varphi : G \to S_A$ defined by $\varphi(g) = \sigma_g$ for all $g \in G$, defined by $\varphi(g)(a) = \sigma_g(a) = g \cdot a$ for all $a \in A$.
- Getting into what a representation is?

Chapter 2

Subgroups

2.1 Definition and Examples

- Two way of unraveling the structure of an axiomatically defined mathematical object are to study subsets of the object that satisfy the same axioms, and to study quotients (which, roughly speaking, collapse one group onto a smaller one).
- **Subgroup** (of G): A subset $H \subset G$ that is nonempty and closed under products and inverses. *Denoted by* $H \leq G$.
  - In other words, we require that $x^{-1} \in H$ for all $x \in H$, and $xy \in H$ for all $x, y \in H$.
  - Alternatively, a subgroup of $(G, \cdot)$ is a subset of G that is a group in its own right under $\cdot$.
- $H \leq G$ and $H \neq G$ imply $H < G$.
- **Trivial subgroup**: The subgroup $H = \{1\}$, henceforth denoted by 1.
- $\leq$ is transitive: $K \leq H \leq G \Longleftarrow K \leq G$.
- Let G be a group.

  Proposition 2.1 (The Subgroup Criterion). *A subset $H \subset G$ is a subgroup iff*

  (1) $H \neq \emptyset$;

  (2) *For all $x, y \in H$, $xy^{-1} \in H$.*

  Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Exercises

7/13: **1.** In each of a-e, prove that the specified subset is a subgroup of the given group.

(a) The set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition).

Proof. Let $H = \{a + ai \mid a \in \mathbb{R}\} \subset \mathbb{C}$.
Criterion 1: Let $a = 1$. Then $1 + i \in H \subset \mathbb{C}$, so $H \neq \emptyset$, as desired.
Criterion 2: Let $a + ai, b + bi \in H$ be arbitrary. Then $(a + ai) + (-b - bi) = (a - b) + (a - b)i \in H$, as desired. □

(b) The set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication).

Proof. Let $H = \{e^{i\theta} \mid \theta \in \mathbb{R}\} \subset \mathbb{C}$.
Criterion 1: Let $\theta = 0$. Then $e^{i(0)} = 1 \in H$, so $H \neq \emptyset$, as desired.
Criterion 2: Let $e^{i\theta_1}, e^{i\theta_2} \in H$ be arbitrary. Then $e^{i\theta_1}e^{i\theta_2} = e^{i(\theta_1+\theta_2)} \in H$, as desired. ☐

(c) For fixed $n \in \mathbb{Z}^+$, the set of rational numbers whose denominators divide n (under addition).

Proof. Let $n \in \mathbb{Z}^+$ be arbitrary, and let $H = \{\frac{p}{q} \in \mathbb{Q} : q \mid n\}$.
Criterion 1: Let $p = q = 1$. Then $\frac{1}{1} \in H$ since 1 divides all n, so $H \neq \emptyset$, as desired.
Criterion 2: Let $\frac{p}{q}, \frac{r}{s} \in H$ be arbitrary. Then since $q, s \mid n$, we can add the fractions with common denominator n, i.e., $\frac{p}{q} + \frac{r}{s} = \frac{pn/q}{n} + \frac{rn/s}{n} = \frac{pn/q+rn/s}{n} \in H$, as desired. ☐

(d) For fixed $n \in \mathbb{Z}^+$, the set of rational numbers whose denominators are relatively prime to n (under addition).

Proof. Symmetric to part (c) — the lcm of two numbers coprime to n will not contain any factors of n. ☐

(e) The set of nonzero real numbers whose square is a rational number (under multiplication).

Proof. Let $H = \{x \in \mathbb{R} \mid x^2 \in \mathbb{Q}\}$.
Criterion 1: Let $x = \sqrt{2}$. Then $x^2 = 2 \in \mathbb{Q}$, so $x \in H$, i.e., $H \neq \emptyset$, as desired.
Criterion 2: Let $x, y \in H$ be arbitrary. Since $x^2, y^{-2} \in \mathbb{Q}$, it follows that $x^2y^{-2} = (xy^{-1})^2 \in \mathbb{Q}$. Therefore, $xy^{-1} \in H$, as desired. ☐

4. Give an explicit example of a group G and an infinite subset $H \subset G$ that is closed under the group operation but is not a subgroup of G.

5. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Proof. Suppose for the sake of contradiction that $H < G$ satisfies $|H| = |G| - 1 \geq 2$. Let $g \in G$ be the unique element of G satisfying $g \notin H$. Since H is a subgroup, we know that $xy^{-1} \in H$, i.e., $xy^{-1} \neq g$ for any $x, y \in H$. It follows that $gy \neq x$ for any $x, y \in H$. However, since gy must be an element of G, we therefore have that $gy = yg = g$ for all $y \in H$. Thus, $y = e$ for all $y \in H$, i.e., that $H = \{e\}$. But then $|H| = 1 < 2$, a contradiction. ☐

8. Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup iff either $H \subseteq K$ or $K \subseteq H$.

Proof. Suppose first that $H \cup K$ is a subgroup. Suppose for the sake of contradiction that $H \not\subseteq K$ and $K \not\subseteq H$. Thus, there exists $h \in H$ such that $h \notin K$, and $k \in K$ such that $k \notin H$. Since $H \cup K$ is a subgroup, $hk \in H \cup K$. Thus, $hk \in H$ or $hk \in K$. We divide into two cases. If $hk \in H$, then $h^{-1}hk = k \in H$, a contradiction. The same contradiction in the other case exists. Since we have a contradiction in every case, we must have that $H \subseteq K$ or $K \subseteq H$, as desired.

Now suppose that $H \subseteq K$ or $K \subseteq H$. We divide into two cases. If $H \subseteq K$, then $H \cup K = K$ is a subgroup of G. The argument is symmetric in the other case. ☐

2.2 Centralizers and Normalizers, Stabilizers and Kernels

- **Centralizer** (of A in G): The set $\{g \in G \mid gag^{-1} = a \ \forall \ a \in A\}$. *Denoted by* $\boldsymbol{C_G(A)}$.
  - Where A is a nonempty subset of G, $C_G(A)$ is the set of all elements in G which commute with every element of A, since $gag^{-1} = a$ is an equivalent condition to $ga = ag$.
- $C_G(A) \leq G$:

Proof. Criterion 1: Since $1a1 = a$ for all $a \in A$, $1 \in C_G(A)$. Thus, $C_G(A)$ is nonempty.

Criterion 2: Let $x, y \in C_G(A)$ be arbitrary. To prove that $xy^{-1} \in C_G(A)$, it will suffice to show that for all $a \in A$, $(xy^{-1})a(xy^{-1})^{-1} = a$. Let a be an arbitrary element of A. Since $x, y \in C_G(A)$, we know that $xax^{-1} = a$ and $yay^{-1} = a$. It follows from the latter condition via multiplication on the left by y^{-1} and multiplication on the right by y that $a = y^{-1}ay$. Combining the last two results, we have that

$$\begin{aligned}(xy^{-1})a(xy^{-1})^{-1} &= x(y^{-1}ay)x^{-1} \\ &= xax^{-1} \\ &= a\end{aligned}$$

as desired. □

- **Center** (of G): The set $\{g \in G \mid gx = xg \ \forall \ x \in G\}$. *Denoted by* $\boldsymbol{Z(G)}$.
- Since $Z(G) = C_G(G)$, $Z(G) \leq G$ by the above argument.
- **Normalizer** (of A in G): The set $\{g \in G \mid gAg^{-1} = A\}$, where $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. *Denoted by* $\boldsymbol{N_G(A)}$.
- Note that $g \in C_G(A)$ implies $g \in N_G(A)$, so $C_G(A) \leq N_G(A)$.

7/15:

- **Stabilizer** (of s in G): The set $\{g \in G \mid g \cdot s = s\}$. *Denoted by* $\boldsymbol{G_s}$.
- $G_s \leq G$.
- **Kernel** (of the action of G on S): The set $\{g \in G \mid g \cdot s = s \ \forall \ s \in S\}$.

Exercises

1. Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \ \forall \ a \in A\}$.

Proof.

$$\begin{aligned}C_G(A) &= \{g \in G \mid gag^{-1} = a \ \forall \ a \in A\} \\ &= \{g \in G \mid g^{-1}gag^{-1}g = g^{-1}ag \ \forall \ a \in A\} \\ &= \{g \in G \mid a = g^{-1}ag \ \forall \ a \in A\} \\ &= \{g \in G \mid g^{-1}ag = a \ \forall \ a \in A\}\end{aligned}$$

□

2. Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Proof. Suppose first that $g \in C_G(Z(G))$. Then by the definition of the centralizer, $g \in G$. Now suppose that $g \in G$. To prove that $g \in C_G(Z(G))$, it will suffice to show that $ghg^{-1} = h$ for all $h \in Z(G)$. Let h be an arbitrary element of $Z(G)$. Then $hx = xh$ for all $x \in G$. It follows that $h = xhx^{-1}$ for all $x \in G$, notably including g. Therefore, we have shown that $ghg^{-1} = h$, as desired.

The proof is symmetric in the other case. □

3. Prove that if A and B are subsets of G with $A \subseteq B$, then $C_G(B) \leq C_G(A)$.

Proof. To prove that $C_G(B) \leq C_G(A)$, it will suffice to show that $C_G(B) \subset C_G(A)$, $C_G(B) \neq \emptyset$, and for all $x, y \in C_G(B)$, $xy^{-1} \in C_G(B)$.

Subsets: Let g be an arbitrary element of $C_G(B)$. Then $gbg^{-1} = b$ for all $b \in B$. Thus, since $A \subset B$, $gag^{-1} = a$ for all $a \in A \subset B$. Therefore, $g \in C_G(A)$, as desired.

Criterion 1: Since $1b1^{-1} = b$ for all $b \in B \subset G$, $1 \in C_G(B)$, so $C_G(B) \neq \emptyset$, as desired.

Criterion 2: Let x, y be arbitrary elements of $C_G(B)$. Then $xbx^{-1} = b$ and $yby^{-1} = b$ for all $b \in B$. It follows from the latter condition that $b = y^{-1}by$. Therefore,

$$\begin{aligned}(xy^{-1})b(xy^{-1})^{-1} &= xy^{-1}byx^{-1} \\ &= xbx^{-1} \\ &= b\end{aligned}$$

as desired. ☐

5. In each of parts a-c, show that for the specified group G and subgroup A of G that $C_G(A) = A$ and $N_G(A) = G$.

(a) $G = S_3$ and $A = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$.

Proof. $1a1^{-1} = a$ for all $a \in A$.

$$\begin{aligned}(1\ 2\ 3) \cdot 1 \cdot (1\ 2\ 3)^{-1} &= (1\ 2\ 3) \cdot (1\ 2\ 3)^{-1} \\ &= 1\end{aligned} \qquad \begin{aligned}(1\ 2\ 3) \cdot (1\ 2\ 3) \cdot (1\ 2\ 3)^{-1} &= (1\ 2\ 3) \cdot 1 \\ &= (1\ 2\ 3)\end{aligned}$$

$$\begin{aligned}(1\ 2\ 3) \cdot (1\ 3\ 2) \cdot (1\ 2\ 3)^{-1} &= 1 \cdot (1\ 2\ 3)^{-1} \\ &= (1\ 3\ 2)\end{aligned}$$

Etc. in each case. ☐

(b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.

(c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

2.3 Cyclic Groups and Cyclic Subgroups

- **Cyclic** (group): A group H that can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).
- A cyclic group may have more than one generator (e.g., we can have $H = \langle x \rangle = \langle x^{-1} \rangle$).
- Let $H = \langle x \rangle$.

  Proposition 2.2. *Then $|H| = |x|$ (where if one side of this equality is infinite, so is the other). More specifically,*

  (1) *If $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \dots, x^{n-1}$ are all the distinct elements of H;*

  (2) *If $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$.*

- Let G be an arbitrary group, let $x \in G$, and let $m, n \in \mathbb{Z}$.

  Proposition 2.3. *If $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.*

  Proof. If $d = \gcd(m, n)$, then by the Euclidean algorithm, there exist integers r, s such that $d = mr + ns$. Thus,

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

  as desired.

  We divide into two cases for the second assertion ($m = 0$ and $m \neq 0$). If $m = 0$, then clearly $|x|$ divides $0 = m$, as desired. On the other hand, if $m \neq 0$, then we continue. Let $d = (m, |x|)$. By the first part, $x^d = 1$. By definition, $0 < d \leq |x|$. But since $|x|$ is the smallest positive integer such that $x^{|x|} = 1$, we must have $d = |x|$. Thus, by the definition of d, $|x| = d \mid m$. ☐

- Cyclic group isomorphisms:

  Theorem 2.4. *Any two cyclic groups of the same order are isomorphic. More specifically,*

  (1) *If $n \in \mathbb{Z}$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map*

  $$\begin{aligned}\varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k\end{aligned}$$

  is well defined and is an isomorphism.

  Proof. To prove that φ is well defined, it will suffice to show that if $x^r = x^s$, then $\varphi(x^r) = \varphi(x^s)$. Let $x^r = x^s$. Then $x^{r-s} = 1$. Thus, by Proposition 2.3, $n \mid r - s$. It follows that $r - s = nt$, i.e., that $r = nt - s$ for some $t \in \mathbb{Z}$. Consequently,

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

  as desired.

  To prove that φ is an isomorphism, it will suffice to show that it is a homomorphism and a bijection. The following shows that φ is a homomorphism.

  $$\varphi(x^a x^b) = \varphi(x^{a+b}) = y^{a+b} = y^a y^b = \varphi(x^a)\varphi(x^b)$$

  As to proving that φ is a bijection, we have by hypothesis that $\langle x \rangle$ and $\langle y \rangle$ are finite groups of the same order, and we know that φ is a surjection since each y^k is the image of an x^k. These two facts prove that it is a bijection (equivalently, φ has an obvious two-sided inverse). □

  (2) *If $\langle x \rangle$ is an infinite cyclic group, the map*

  $$\begin{aligned}\varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k\end{aligned}$$

  is well defined and is an isomorphism.

  Proof. φ is automatically well-defined since $\mathbb{Z}$ is well-defined.

  By Proposition 2.2, $a \neq b$ implies $x^a \neq x^b$ for all distinct $a, b \in \mathbb{Z}$. Thus, φ is injective. By the definition of a cyclic group, φ is surjective. Thus, it is bijective. Additionally, laws of exponents prove that it is a homomorphism, as above. □

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

  Proposition 2.5.

  (1) *If $|x| = \infty$, then $|x^a| = \infty$.*

  Proof. Suppose for the sake of contradiction that $|x^a| = m < \infty$. Then $x^{am} = (x^a)^m = 1$ and $x^{-am} = ((x^a)^m)^{-1} = 1^{-1} = 1$. Thus, since either am or $-am$ is a positive integer (neither are 0 since $a \neq 0 \neq m$), $|x| = \pm am < \infty$, a contradiction. □

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

  (3) *In particular, if $|x| = n < \infty$, and a is a positive integer dividing n, then $|x^a| = \frac{n}{a}$.*

Chapter 4

Group Actions

4.1 Group Actions and Permutation Representations

- **Faithful** (group action): A group action whose kernel is the identity.

Part II

Serre

Chapter 1

Generalities on Linear Representations

1.1 Definitions

7/15:

- ***GL*(*V*)**: The group of isomorphisms of V onto itself, where V is a vector space over the field $\mathbb{C}$ of complex numbers.
- If (e_i) is a finite basis of n elements for V, then each linear map $a : V \to V$ is defined by a square matrix (a_{ij}) of order n.
- The coefficients a_{ij} are complex number derived from expressing the images $a(e_j)$ in terms of the basis (e_i) and solving, i.e., we know that each $a(e_j) = \sum_i a_{ij} e_i$.
- a is an isomorphism $\iff \det(a) = \det(a_{ij}) \neq 0$.
- We can thus identify $GL(V)$ with the group of invertible square matrices of order n.
- **Linear representation** (of G in V): A homomorphism $\rho : G \to GL(V)$, where G is a finite group.
- **Representation space** (of G): The vector space V, given a homomorphism ρ. *Also known as* **representation**.
- **Degree** (of a representation V): The dimension of the representation space.
- **Similar** (representations): Two representations ρ, ρ' of the same group G in vector spaces V and V' such that there exists a linear isomorphism $\tau : V \to V'$ which satisfies the identity $\tau \circ \rho(s) = \rho'(s) \circ \tau$ for all $s \in G$. *Also known as* **isomorphic**.
  - When $\rho(s), \rho'(s)$ are given in matrix form by R_s, R'_s, respectively, this means that there exists an invertible matrix T such that $T \cdot R_s = R'_s \cdot T$ for all $s \in G$.

1.2 Basic Examples

- **Unit representation**: The representation ρ of G defined by $\rho(s) = 1$ for all $s \in G$. *Also known as* **trivial representation**.
- **Regular representation**: The representation ρ defined by $\rho(s) = f : V \to V$ where $f : e_t \mapsto e_{st}$, where V is a vector space of dimension $g = |G|$ with basis $(e_t)_{t \in G}$.
- **Permutation representation**: The representation ρ defined by $\rho(s) = f : V \to V$, where $f : e_x \to e_{sx}$, $x \in X$ being the set acted upon by G.

1. So ρ is the representation of a group, technically. But it seems like we more often treat V as the representation. So which is it, because it seems like they are distinct concepts?
2. What is the utility of representation theory in mathematics? Does mapping group elements onto automorphisms that obey similar properties in the more well-defined vector space allow us to prove certain results about groups, for instance? Is it the other way around, in that representation theory allows us to prove results about vector spaces from what we know about groups? Is representation theory purely a way of linking group theory and linear algebra so that results in one field may be applied to the other and vice versa? I'm just trying to wrap my head around the motivation for creating and studying homomorphism from groups to vector space automorphisms/linear transformations.
3. Subrepresentations and blocks of block-diagonal matrices?
4. Can you explain kernel to me?
5. What about stability under subgroups of G?
6. Equivalence between representation and group actions?
7. Are linear automorphisms a generalization of permutations?
8. It seems like the general linear group is a group, and all that representation theory does is maps an arbitrary group onto a general linear group in a manner that preserves the group operation. But why bother? If we wanted to study the group-like characteristics of the general linear group, couldn't we just do that directly? Or is the point to have a common reference point for a whole bunch of groups?
9. We define a permutation to be a function because the "original set" and the "final set" are both critical to understanding the nature of what a permutation is. We do the same for a representation for the same reason?

Part III

Pinter

Chapter 3

The Definition of Groups

Exercises

D. A Checkerboard Game

1	2
3	4

Our checkerboard has only 4 squares, numbered 1, 2, 3, and 4. There is a single checker on the board, and it has four possible moves:

V: Move vertically; that is, move from 1 to 3, or from 3 to 1, or form 2 to 4, or from 4 to 2.

H: Move horizontally; that is, move from 1 to 2 or vice versa, or from 3 to 4 or vice versa.

D: Move diagonally; that is, move from 2 to 3 or vice versa, or from 1 to 4 or vice versa.

I: Stay put.

We may consider an operation on the set of these four moves, which consists of performing moves successively. For example, if we move horizontally and then vertically, we end up with the same result as if we had moved diagonally:

$$H * V = D$$

If we perform two horizontal moves in succession, we end up where we started: $H * H = I$. And so on. If $G = \{V, H, D, I\}$, and $*$ is the operation we have just described, write the table of G. Granting associativity, explain why $\langle G, * \rangle$ is a group.

Chapter 4

Elementary Properties of Groups

7/19: • Let G be a group, and let $a, b \in G$.

Theorem 4.2. *If* $ab = e$*, then* $a = b^{-1}$ *and* $b = a^{-1}$*.*

Chapter 9

Isomorphism

7/20: • **Isomorphism** (between groups G_1, G_2): A bijective function $f : G_1 \to G_2$ with the property that for any $a, b \in G_1$, $f(ab) = f(a)f(b)$. *Denoted by* $\boldsymbol{G_1 \cong G_2}$.

Exercises

A. Isomorphism Is an Equivalence Relation among Groups

1 Let G be any group. If $\varepsilon : G \to G$ is the identity function, $\varepsilon(x) = x$, show that ε is an isomorphism.

Proof. To prove that ε is an isomorphism, it will suffice to show that ε is a bijection and that $\varepsilon(ab) = \varepsilon(a)\varepsilon(b)$ for all $a, b \in G$. Let $a, b \in G$ be arbitrary. By the definition of ε, $\varepsilon(a) = \varepsilon(b)$ implies $a = b$. Thus, ε is injective. Additionally, we have that $\varepsilon(b) = b$, so ε is surjective. Therefore, it is bijective. Lastly,

$$\varepsilon(ab) = ab = \varepsilon(a)\varepsilon(b)$$

as desired. □

2 Let G_1, G_2 be groups, and $f : G_1 \to G_2$ be an isomorphism. Show that $f^{-1} : G_2 \to G_1$ is an isomorphism.

Proof. Since f is a bijection, f^{-1} exists and is a bijection. Additionally, let $c, d \in G_2$ be arbitrary. Then $f^{-1}(c) = a$ and $f^{-1}(d) = b$ for some $a, b \in G_1$. Thus, since $f(ab) = f(a)f(b) = cd$, we have that $f^{-1}(cd) = f^{-1}(f(ab)) = ab = f^{-1}(c)f^{-1}(d)$, as desired. □

3 Let G_1, G_2, G_3 be groups, and let $f : G_1 \to G_2$ and $g : G_2 \to G_3$ be isomorphisms. Prove that $g \circ f : G_1 \to G_3$ is an isomorphism.

Proof. Since f, g are bijections, $g \circ f$ is a bijection. Now let $a, b \in G_1$ be arbitrary. Thus, $f(ab) = f(a)f(b)$, where $f(a), f(b) \in G_2$. It follows that $g(f(a)f(b)) = g(f(a))g(f(b))$. Therefore,

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$$

as desired. □

B. Elements Which Correspond under an Isomorphism

1 If e_1 denotes the neutral element of G_1 and e_2 denotes the neutral element of G_2, prove that $f(e_1) = e_2$.

Proof. For all $x \in G_1$, $e_1 x = x = x e_1$. Thus, by the definition of an isomorphism, $f(e_1)f(x) = f(e_1 x) = f(x)$ and $f(x)f(e_1) = f(x e_1) = f(x)$. It follows by their definition that $f(e_1)$ is a neutral element of G_2. Therefore, since neutral elements are unique, $f(e_1) = e_2$, as desired. □

2 Prove that for each element $a \in G_1$, $f(a^{-1}) = [f(a)]^{-1}$.

Proof. Let $a \in G_1$ be arbitrary. Then $e_2 = f(e_1) = f(aa^{-1}) = f(a)f(a^{-1})$. It follows by Theorem 4.2 that $f(a^{-1}) = [f(a)]^{-1}$, as desired. $\square$

3 If G_1 is a cyclic group with generator a, prove that G_2 is also a cyclic group, with generator $f(a)$.

Proof. Suppose G_1 is a cyclic group of order n with generator a. We wish to show that G_2 is a cyclic group of order n with generator $f(a)$. By the definition of an isomorphism,

$$f(a^t) = f(\underbrace{aa\cdots a}_{t \text{ times}}) = \underbrace{f(a)f(a)\cdots f(a)}_{t \text{ times}} = f(a)^t$$

for all $t \in \mathbb{Z}$. As a special case, $e_2 = f(e_1) = f(a^n) = f(a)^n$, so G_2 is of order *at most* n. Now suppose for the sake of contradiction that there exists a positive integer $0 < t < n$ such that $f(a)^t = e_2$. Then $f(a^t) = e_2$, i.e., $a^t = e_2$. But this means that G_1 is of order t, a contradiction. $\square$

C. Isomorphism of Some Finite Groups

1 G is the checkerboard game group of Chapter 3, Exercise D. H is the group of the complex numbers $\{i, -i, 1, -1\}$ under multiplication.

Proof. Suppose for the sake of contradiction that an isomorphism $f : G \to H$ exists. Since $-i^1 = -i$, $-i^2 = -1$, $-i^3 = i$, and $-i^4 = 1$, $H = \langle -i \rangle$. Thus, by Exercise 9.B.3, G is a cyclic group with generator $f^{-1}(-i)$. However, no element $x \in G$ suffices as a generator ($I^1 = I$, $V^2 = I$, $H^2 = I$, and $D^2 = I$), a contradiction. $\square$

Chapter 13

Counting Cosets

7/22:

- **Left coset** (of H in G): The set of all products ah, where H is a subgroup of G, $a \in G$ is fixed, and h ranges over H. *Denoted by* $\boldsymbol{aH}$.
- **Right coset** (of H in G): The set of all products ha, where H is a subgroup of G, $a \in G$ is fixed, and h ranges over H. *Denoted by* $\boldsymbol{Ha}$.
- In this book, we choose to focus on right cosets.
- If $a \in Hb$, then $Ha = Hb$.

  Proof. Let $x \in Ha$ be arbitrary. Then there exists $h \in H$ such that $x = ha$. Similarly, since $a \in Hb$, there exists $h' \in H$ such that $a = h'b$. Thus, we have that $x = h(h'b) = (hh')b$ by the associative law. But since H is a subgroup of G, $hh' \in H$. Therefore, $x \in Hb$, as desired. The proof is symmetric in the other direction. $\square$

- Let G be a group and let H be a fixed subgroup of G.

  Theorem 13.1. *The family of all the cosets Ha, as a ranges over G, is a partition of G.*

  Proof. To prove that the collection of all cosets of H is a partition of G, it will suffice to show that any two cosets are either disjoint or equal, and every element of G is in some coset. We take this one constraint at a time.

  Let Ha, Hb be arbitrary cosets of H in G. We divide into two cases (Ha, Hb are disjoint and Ha, Hb are not disjoint). If they are disjoint, we are done. On the other hand, if they are not disjoint, then there exists $x \in Ha \cap Hb$. Since $x \in Ha$, $x = h_1a$ for some $h_1 \in H$. Similarly, $x = h_2b$ for some $h_2 \in H$. It follows that $a = (h_1^{-1}h_2)b$. But since $h_1^{-1}h_2 \in H$ by the definition of a subgroup, the above fact implies that $Ha = Hb$, as desired.

  Let $x \in G$ be arbitrary. Since $e \in H$ by the definition of a subgroup, $x = ex \in Hx$, as desired. $\square$

- Let G be a finite group, let H be be a fixed subgroup of G, and let $a \in G$ be arbitrary.

  Theorem 13.2. *If Ha is any coset of H, there is a one-to-one correspondence from H to Ha.*

  Proof. Let $f : H \to Ha$ be defined by $f(h) = ha$ for all $h \in H$. To prove that f is bijective, it will suffice to show that it is injective and surjective. To begin, let $f(h_1) = f(h_2)$. Then $h_1a = h_2a$. But by the cancellation law, $h_1 = h_2$, as desired. Now let $x \in Ha$ be arbitrary. By the definition of Ha, $x = ha$ for some $h \in H$. Therefore, $f(h) = ha = x$, as desired. $\square$

  - This implies that if G is finite, all cosets of H have the same number of elements.

- Let G be a finite group, and H any subgroup of G.

Theorem 13.3 (Lagrange's Theorem)**.** *The order of G is a multiple of the order of H.*

Proof. By Theorem 13.1, we may let the cosets of H divide G into n partitions. By Theorem 2, each of these n partitions has the same cardinality $\text{ord}(H)$. Therefore, since the elements in the group are divided into n partitions of size $\text{ord}(H)$, $\text{ord}(G) = n\,\text{ord}(H)$, as desired. □

- Let G be a group.

  Theorem 13.4. *If G has a prime number p of elements, then G is a cyclic group. Furthermore, any element $a \neq e$ in G is a generator of G.*

  Proof. Let a be an arbitrary non-neutral element of G. As we know, $\langle a \rangle$ is a subgroup of G. Thus, by Lagrange's theorem, $\text{ord}(\langle a \rangle) \mid \text{ord}(G)$. However, since $\text{ord}(G) = p$ is prime, either $\text{ord}(\langle a \rangle) = 1$ or $\text{ord}(\langle a \rangle) = p$. But since $a \neq e$, $\text{ord}(\langle a \rangle) \neq 1$. Therefore, $\text{ord}(\langle a \rangle) = p$, and we have that G is a cyclic group with generator a, as desired. □

- Theorem 13.4 gives us complete information on all groups of prime order; in other words, every group of prime order is isomorphic to the well-behaved $\mathbb{Z}/p\mathbb{Z}$.
- Let G be a finite group and $a \in G$.

  Theorem 13.5. *The order of a divides the order of G.*

  Proof. Clearly, $\text{ord}(a) = \text{ord}(\langle a \rangle)$. But since $\langle a \rangle$ is a subgroup of G, Lagrange's theorem implies that $\text{ord}(\langle a \rangle) = \text{ord}(a) \mid \text{ord}(G)$, as desired. □

- **Index** (of H in G): The number of cosets of H in G. *Denoted by* $\boldsymbol{(G : H)}$.
- By Theorems 13.1 and 13.2,
$$(G : H) = \frac{\text{ord}(G)}{\text{ord}(H)}$$

Exercises

A. Examples of Cosets in Finite Groups

In parts 1-5, list the cosets of H. For each coset, list the elements of the coset.

1 $G = S_3$, $H = \{\epsilon, \beta, \delta\}$.

Answer.
$$H\epsilon = H\beta = H\delta = \{\epsilon, \beta, \delta\}$$
$$H\alpha = H\kappa = H\gamma = \{\alpha, \kappa, \gamma\}$$
□

2 $G = S_3$, $H = \{\epsilon, \alpha\}$.

Answer.
$$H\epsilon = H\alpha = \{\epsilon, \alpha\}$$
$$H\beta = H\gamma = \{\beta, \gamma\}$$
$$H\delta = H\kappa = \{\delta, \kappa\}$$
□

3 $G = \mathbb{Z}/15\mathbb{Z}$, $H = \langle 5 \rangle$.

Answer. If $H = \langle 5 \rangle$, then $H = \{0, 5, 10\}$. Therefore,

$$\begin{aligned} H+0 &= H+5 = H+10 = \{0,5,10\} \\ H+1 &= H+6 = H+11 = \{1,6,11\} \\ H+2 &= H+7 = H+12 = \{2,7,12\} \\ H+3 &= H+8 = H+13 = \{3,8,13\} \\ H+4 &= H+9 = H+14 = \{4,9,14\} \end{aligned}$$

□

4 $G = D_4$, $H = \{R_0, R_4\}$.

Answer.

$$\begin{aligned} HR_0 &= HR_4 = \{R_0, R_4\} \\ HR_1 &= HR_7 = \{R_1, R_7\} \\ HR_2 &= HR_5 = \{R_2, R_5\} \\ HR_3 &= HR_6 = \{R_3, R_6\} \end{aligned}$$

□

5 $G = S_4$, $H = A_4$.

Answer. If $H = A_4$, then

$$\begin{aligned} H = \{&\left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\1&3&4&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\1&4&2&3\end{smallmatrix}\right), \\ &\left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\2&3&1&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\2&4&3&1\end{smallmatrix}\right), \\ &\left(\begin{smallmatrix}1&2&3&4\\3&1&2&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\3&2&4&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right), \\ &\left(\begin{smallmatrix}1&2&3&4\\4&1&3&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\4&2&1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right)\} \end{aligned}$$ [1]

Therefore,

$$\begin{aligned} Hx = A_4 &\implies x \in A_4 \\ Hx = S_4 \setminus A_4 &\implies x \notin A_4 \end{aligned}$$

□

6 Indicate the order and index of each of the subgroups in parts 1-5.

Answer.
1: $\operatorname{ord}(H) = 3$, $(G : H) = 2$.
2: $\operatorname{ord}(H) = 2$, $(G : H) = 3$.
3: $\operatorname{ord}(H) = 3$, $(G : H) = 5$.
4: $\operatorname{ord}(H) = 2$, $(G : H) = 4$.
5: $\operatorname{ord}(H) = 12$, $(G : H) = 2$. □

B. Examples of Cosets in Infinite Groups

Describe the cosets of the subgroups described in parts 1-5.

1 The subgroup $H = \langle 3 \rangle$ of $\mathbb{Z}$.

[1] For all $n \in \mathbb{N}$, $\operatorname{ord}(S_n) = 2\operatorname{ord}(A_n) = 2\operatorname{ord}(S_n \setminus A_n)$. In A_n, there are $n!/n/2 = (n-1)!/2$ permutations that send $1 \mapsto 1$. In A_n, for all $m \in [n]$, there are an equal number of permutations that send $1 \to m$. Generalization of this one may be more complicated: In A_4, if $1 \mapsto m$ odd, then the remaining three numbers are an increasing cycle; similarly, if $1 \mapsto m$ even, then the remaining three numbers are a decreasing cycle. Relation to determinants of matrices? Minimum number of transpositions? – every permutation in A_4 can be written as the product of 0 or 2 transpositions. In general, the coset of any element in H is H.

Answer. If $x \in \langle 3 \rangle$, then $H + x = \langle 3 \rangle$.
If $x \in \{1 + n \mid n \in \langle 3 \rangle\}$, then $H + x = \{1 + n \mid n \in \langle 3 \rangle\}$.
If $x \in \{2 + n \mid n \in \langle 3 \rangle\}$, then $H + x = \{2 + n \mid n \in \langle 3 \rangle\}$. □

2 The subgroup $H = \mathbb{Z}$ of $\mathbb{R}$.

Answer. If $x \in \mathbb{R}$, let $\tilde{x}$ be the greatest integer less than or equal to x. Let $x \in \mathbb{R}$ Then $H + x = \{p \in \mathbb{R} \mid p - \tilde{p} = x - \tilde{x}\}$. □

3 The subgroup $H = \langle 2^n : n \in \mathbb{Z} \rangle$ of $\mathbb{R}^*$.

Answer. The coset of any element in H is H. Otherwise, its a scaled version of H. □

C. Elementary Consequence of Lagrange's Theorem

Let G be a finite group. Prove the following.

1 If G has order n, then $x^n = e$ for every $x \in G$.

Proof. $\langle x \rangle$ is a cyclic subgroup of G. Thus, $x^{\mathrm{ord}(\langle x \rangle)} = e$. Additionally, by Lagrange's theorem, $\mathrm{ord}(\langle x \rangle) \mid n$. Thus, let $n = m\,\mathrm{ord}(\langle x \rangle)$. Therefore, $x^n = (x^{\mathrm{ord}(\langle x \rangle)})^m = e^m = e$, as desired. □

2 Let G have order pq, where p, q are primes. Either G is cyclic, or every element $x \neq e$ in G has order p or q.

Proof. Let $x \in G$ such that $x \neq e$. We know that $\langle x \rangle$ is a cyclic subgroup of G, and that $\mathrm{ord}(x) = \mathrm{ord}(\langle x \rangle)$. Thus, by Lagrange's theorem, $\mathrm{ord}(x) \mid pq$. This combined with the hypothesis that $x \neq e$ implies the $\mathrm{ord}(x) \in \{p, q, pq\}$. We divide into two cases ($\mathrm{ord}(x) = pq$, and $\mathrm{ord}(x) \neq pq$). If $\mathrm{ord}(x) = pq$, then G is cyclic with generator x, as desired. On the other hand, if $\mathrm{ord}(x) = p$ or $\mathrm{ord}(x) = q$, then every element $x \neq e$ in G has order p or q (for if one did not, it would have order pq; but then G would be cyclic, contradicting the fact that $\mathrm{ord}(x) \in \{p, q\}$). □

E. Elementary Properties of Cosets

Let G be a group, and H a subgroup of G. Let a, b denote elements of G. Prove the following:

1 $Ha = Hb$ iff $ab^{-1} \in H$.

I. Conjugate Elements

If $a \in G$, a **conjugate** of a is any element of the form xax^{-1}, where $x \in G$. (Roughly speaking, a conjugate of a is any product consisting of a sandwiched between any element and its inverse.) Prove each of the following:

1 The relation "a is equal to the conjugate of b" is an equivalence relation in G. (Write $a \sim b$ for "a is equal to the conjugate of b.")

Proof. Criterion 1: Let $x = a$. Then $a = ae = aaa^{-1} = xax^{-1}$. Therefore, $a \sim a$.
Criterion 2: Let $a \sim b$. Then $a = xbx^{-1}$ for some $x \in G$. It follows that $b = x^{-1}ax = (x^{-1})a(x^{-1})^{-1}$. Therefore, $b \sim a$.
Criterion 3: Let $a \sim b$ and $b \sim c$. Then $a = xbx^{-1}$ and $b = ycy^{-1}$. It follows that $a = xycy^{-1}x^{-1} = (xy)c(xy)^{-1}$. Therefore, $a \sim c$. □

This relation $\sim$ partitions any group G into classes called **conjugacy classes**. (The conjugacy class of a is $[a] = \{xax^{-1} : x \in G\}$.)

For any element $a \in G$, the **centralizer** of a, denoted by C_a, is the set of all the elements in G which commute with a. That is,

$$C_a = \{x \in G \mid xa = ax\} = \{x \in G \mid xax^{-1} = a\}$$

Prove the following:

2 For any $a \in G$, C_a is a subgroup of G.

3 $x^{-1}ax = y^{-1}ay$ iff xy^{-1} commutes with a iff $xy^{-1} \in C_a$.

Proof. First, suppose that $x^{-1}ax = y^{-1}ay$. Then

$$axy^{-1} = xx^{-1}axy^{-1} = xy^{-1}ayy^{-1} = xy^{-1}a$$

as desired.
Second, suppose that xy^{-1} commutes with a. Then by the definition of the centralizer, $xy^{-1} \in C_a$.
Third, suppose that $xy^{-1} \in C_a$. Then $xy^{-1}ayx^{-1} = a$. Then $x^{-1}ax = x^{-1}xy^{-1}ayx^{-1}x = y^{-1}ay$, as desired. □

4 $x^{-1}ax = y^{-1}ay$ iff $C_ax = C_ay$.

Proof. Suppose first that $x^{-1}ax = y^{-1}ay$. Then by Exercise 13.I.3, $xy^{-1} \in C_a$. Therefore, by Exercise 13.E.1, $C_ax = C_ay$, as desired.
The proof is symmetric in the other direction. □

5 There is a one-to-one correspondence between the set of all the conjugates of a and the set of all the cosets of C_a.

J. Group Acting on a Set

Let A be a set, and let G be any subgroup of S_A. G is a group of permutations of A; we say it is a **group acting** (on the set A). Assume here that G is a finite group. If $u \in A$, the **orbit** (of u with respect to G) is the set

$$O(u) = \{g(u) : g \in G\}$$

1 Define a relation $\sim$ on A by $u \sim v$ iff $g(u) = v$ for some $g \in G$. Prove that $\sim$ is an equivalence relation on A, and that the orbits are its equivalence classes.

Proof. Criterion 1: Let u be an arbitrary element of A. Since G is a subgroup of S_A, G contains the identity permutation ϵ. Under this element of G, we know that $\epsilon(u) = u$. Therefore, $u \sim u$.
Criterion 2: Let $u \sim v$. Then there exists $g \in G$ such that $g(u) = v$. Since G is a subgroup of S_A, $g^{-1} \in G$. Thus, $g^{-1}(v) = g^{-1}(g(u)) = u$. Therefore, $v \sim u$.
Criterion 3: Let $u \sim v$ and $v \sim w$. Then there exist $g, h \in G$ such that $g(u) = v$ and $h(v) = w$. It follows that $(hg)(u) = h(g(u)) = w$. But since $hg \in G$ because G is closed under products, $u \sim w$.

To prove that the orbits are equivalence classes, it will suffice to show that any two orbits are either disjoint or equal. Let $O(u), O(v)$ be arbitrary orbits. If they are disjoint, we are done. However, if they are not, then there exists $w \in O(u) \cap O(v)$. It follows that $w = g(u) = h(v)$ for some $g, h \in G$. But then $w \sim u$ and $w \sim v$. It follows since $\sim$ is an equivalence relation that $u \sim v$. Thus, there exists $f \in G$ such that $f(u) = v$. □