Part 1: Groups

0 Preliminaries

0.1 Properties of Integers

Universal Product Code (UPC)

$(a_1, a_2, \cdots, a_{12}) \cdot (3, 1, 3, 1, \cdots, 3, 1) \mod 10 = 0.$

The 10-digit International Standard Book Number (ISBN-10) has the property $(a_1, a_2, \cdots, a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \mod 11 = 0$. As for a_{10}, X stands for 10.

0.2 Modular Arithmetic

Logic Gates & modulo 2 arithmetic

0.3 Complext Numbers

norm of a+bi

Closure under division

conjugation

0.4 Mathematical Induction

e.g. Prove that $2^n 3^{2n} - 1$ is always divisible by 17.

0.5 Equivalence Relations

1. reflexive property: $a \sim a$.
2. symmetric property: $a \sim b \Rightarrow b \sim a$.
3. transitive property: $a \sim b,\ b \sim c \Rightarrow a \sim c$.

e.g.

- $(a, b) \cong (c, d)$ if $ad = bc, b, d \neq 0$.

Partition

0.6 Functions (Mappings)

To verify that a correspondence is a function:

$$x_1 = x_2 \Rightarrow \phi(x_1) = \phi(x_2).$$

One-to-one function:

$$\phi(x_1) = \phi(x_2) \Rightarrow a_1 = a_2.$$

Function from A onto B

Properties

1. associativity: $\gamma(\beta\alpha) = (\gamma\beta)\alpha$.
2. If α and β is one-to-one, then $\beta\alpha$ is one-to-one.
3. If α and β is onto, then $\beta\alpha$ is onto.
4. If α is one-to-one and onto, then there is a function α^{-1} from B onto A such that $(\alpha^{-1}\alpha)(a) = a$ for all a in A and $(\alpha\alpha^{-1})(b) = b$ for all b in B.

0.7 Exercise

1. If a mod st = b mod st, show that a mod s=b mod s and a mod t = b mod t. The converse is true if s and t are relatively prime.
2. If n is an integer greater than 1 and $(n-1)! = 1$ mod n, prove that n is prime.
3. Prove that 3, 5, and 7 are the only three consecutive odd integers that are prime.

1 Introduction to Groups

1.1 Symmetries of a Square

Cayley table

- closure
- identity
- inverse
- associativity

commutative (Abelian)

1.2 The Dihedral Groups

~~cross cancellation~~

1.3 Bibliography of Niels Abel

2 Groups

2.1 Definition and Examples of Groups

Group	Operation	Identity	Form of Element	Inverse	Abelian
$GL(n,F)$	Matrix multiplication	E	$\|A\| \neq 0$		No
$SL(n,F)$	Matrix multiplication	E	$\|A\| = 1$		No
$U(n)$	Mutiplication mod n	1	$\gcd(k,n) = 1$		Yes
$\mathbb{R}^n$	Componentwise addition	$(0,0,\cdots,0)$	$(a_1,a_2,\cdots,a_n)$		Yes

2.2 Elementary Properties of Groups

- Uniqueness of the Identity
- Cancellation
- Uniqueness of Inverses
- Socks-Shoes Property: $(ab)^{-1} = b^{-1}a^{-1}$.

2.3 Historical Note

2.4 Exercises

1. Left-right cancellation implies commutativity, and cross cancellation implies Abelian property.
2. Law of Exponents for Abelian Groups: $(ab)^n = a^n b^n$.
3. $ab = ba \quad \Leftrightarrow \quad (ab)^2 = a^2b^2 \quad \Leftrightarrow \quad (ab)^{-2} = b^{-2}a^{-2}$.
4. Supose F_1 and F_2 are distinct reflections in a dihedral group D_n, Prove that $F_1F_2 \neq R_0$. If $F_1F_2 = F_2F_1$, then $F_1F_2 = R_{180}$.

3 Finite Groups; Subgroups

3.1 Temiology and Notation

Order of a group

Order of an element

Subgroup

Proper subgroup: $H \subset G$.

3.2 Subgroup Tests

- To prove that a subset is a subgroup
  - **One-Step Test**: $ab^{-1} \in H$.
  - **Two-Step Test**: $ab, a^{-1} \in H$.
  - **Finite Subgroup Test**: $ab \in H$.
- To prove that a subset is not a subgroup
  - Show that the identity is not in the set.
  - Exhibit an element of the set whose inverse is not in the set.
  - Exhibit two elements of the set whose product is not in the set.

3.3 Examples of Subgroups

- $\langle a \rangle$ is an Abelian subgroup, where a is called a *generator* of G.
- $\langle S \rangle$ is the smallest subgroup of G containing S.
- Gaussian Integers: $\langle 1, \mathrm{i} \rangle = \{a + b\mathrm{i} \mid a, , b \in \mathbb{Z}\}$.
- Center is a subgroup. $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$.
- For $n \geq 3$,

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\}, & n \text{ is even,} \\ \{R_0\}, & n \text{ is odd.} \end{cases}$$

- Centralizer of a in G is a subgroup: $C(a) = \{g \in G \mid ga = ag\}$.
- Centralizer of H in G is a subgroup: $C(H) = \{g \in G \mid xh = hx \text{ for all } h \in H\}$.
- $Z(G) \in C(a)$, $Z(G) = \bigcap\limits_{a \in G} C(a)$.
- G is Abelian if and only if $C(a) = G$ for all a in G.

3.4 Exercises

1. For elements a, b in group $\mathbb{Z}_n$, $|a + b| = (|a| + |b|) \mod n$.
2. Prove that if a is the only element of order 2 in a group, then a lies in the center of the group.

   Proof. $\left(x^{-1}ax\right)^2 = x^{-1}ax = a \Rightarrow ax = xa$.
3. No group is the union of two proper subgroups, but some groups are the union of three proper subgroups.
4. Let G be a group and let H be a subgroup of G. For any fixed x in G, define the ***conjugate*** of H: $xHx^{-1} = \left\{xhx^{-1} \mid h \in H\right\}$, which preserves structure.
5. Compute the probability that two randomly chosen elements (they can be the same) from D_4 communte:

$$P = \begin{cases} \dfrac{n+3}{4n}, & n \text{ is odd,} \\ \dfrac{n+6}{4n}, & n \text{ is even.} \end{cases}$$

4 Cyclic Groups

4.1 Properties of Cyclic Groups

> If a and b belong to a finite group and $ab = ba$, then $|ab|$ divides $|a|\,|b|$.

- $|ab| = |a|\,|b|$ if and only if $(|a|, |b|) = 1$.

Theorem 4.2 ⭐

> $|a| = n,\ d = \gcd(n, k) \quad \Rightarrow \quad \langle a^k \rangle = \langle a^d \rangle,\ |a^k| = \dfrac{n}{d}.$

- In a finite cyclic group, the order of an element divides the order of the group.

> $\gcd(n, i) = \gcd(n, j) \quad \Leftrightarrow \quad \langle a^i \rangle = \langle a^j \rangle \quad \Leftrightarrow \quad |a^i| = |a^j|.$

- $\gcd(n, j) = 1 \quad \Leftrightarrow \quad \langle a \rangle = \langle a^j \rangle \quad \Leftrightarrow \quad |a| = |\langle a^j \rangle|.$

4.2 Classification of Subgroups of Cyclic Groups

Theorem 4.3 ⭐ Fundamental Theorem of Cyclic Groups

> Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely, $\langle a^{n/k} \rangle$.

Theorem 4.4 Number of Elements of Each Order in a Cyclic Group

> If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

- Notice that for a finite cyclic group of order n, the number of elements of order d for any divisor d of n depends only on d.

Corollary 4.1 Number of Elements of Order d in a Finite Group.

> In a finite group, the number of elements of order d is a mutliple of $\phi(d)$.

$$
\begin{gathered}
\phi\left(p^n\right) = p^n - p^{n-1} \\
\phi(p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \cdots \phi(p_m^{k_m})
\end{gathered}
$$

subgroup lattice

4.3 Exercise

1. If a is a group element of infinite order, then

$$
\begin{gathered}
\langle a^i \rangle \cap \langle a^j \rangle = \left\langle a^{[i,j]} \right\rangle \\
\langle a^i \rangle \cup \langle a^j \rangle = \left\langle a^{(i,j)} \right\rangle
\end{gathered}
$$

2. Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.

4.3 Bibliography of James Joseph Sylvester

5 Permutation Groups

5.1 Definitions and Notation

5.2 Cycle Notation

5.3 Properties of Permutations

Theorem 5.1 Products of Disjoint Cycles

> Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem 5.2 Disjoint Cycles Commute

> If the pair of cycles $\alpha = (a_1, a_2, \cdots, a_m)$ and $\beta = (b_1, b_2, \cdots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Theorem 5.3 Order of a Permutation

> The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Theorem 5.4 Product of 2-Cycles

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

Lemma If $\varepsilon = \beta_1\beta_2 \cdots \beta_r$, where β_i are 2-cycles, then r is even.

Theorem 5.5 Always Even or Always Odd

Therorem 5.6 Even Permutations Form a Group

> The set of even permutations in S_n forms a subgroup of S_n, which is called the alternating group of degree n, A_n.

Theorem 5.7 For $n \geq 1$, A_n has order $n!/2$.

5.4 A Check-Digit Scheme Based on D_5

5.5 Exercise

1. Stabilizer of a in G is a subgroup: $\mathrm{stab}(a) = \{\alpha \in G \mid \alpha(a) = a\}$.
2. Let α belong to S_n, Prove that $|\alpha|$ divides $n!$.

5.5 Bibliography of Augustin Cauchy

5.6 Bibilography of Alan Turing

6 Isomorphisms

6.1 Motivation

6.2 Definition and Examples

Definition Group Isomorphism

> An isomorphism ϕ from a group G_1 to a group G_2 is a one-to-one onto mapping (or function) from G_1 to G_2 that preserves the group operation. That is,
>
> $$\forall a, b \in G_1,\ \phi(ab) = \phi(a)\phi(b).$$
>
> If there is an isomorphism from G_1 onto G_2, we say that G_1 and G_2 are isomorphic and write $G_1 \approx G_2$.

To prove a group G_1 is isomorphic to a group G_2:

1. "Mapping": Define a function ϕ from G_1 to G_2;
2. "1-1": Assume that $\phi(a) = \phi(b)$, prove that $a = b$;
3. "Onto": For any element $\overline{g}$ in G_2, find an element g in G_1 such that $\phi(g) = \overline{g}$;
4. "O.P.": Prove that ϕ is operation-preserving; that is, show that $\phi(ab) = \phi(a)\phi(b)$.

Example

- Conjugation by M: $\phi_M = MAM^{-1}$.

6.3 Properties of Isomorphisms

Theorem 6.1 Properties of Isomorphisms Acting on Elements

> Suppose that ϕ is an isomorphism from a group G_1 onto a group G_2. Then
>
> 1. ϕ carries the identity of G_1 to the identity of G_2.
> 2. For every integer n and for every group element a in G_1, $\phi(a^n) = [\phi(a)]^n$. (Additive form: $\phi(na) = n\phi(a)$.)
> 3. For any elements a and b in G_1, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
> 4. $G_1 = \langle a \rangle$ if and only if $G_2 = \langle \phi(a) \rangle$.
> 5. $|a| = |\phi(a)|$ for all a in G_1 (isomorphisms preserve orders).
> 6. For a fixed integer k and a fixed group element b in G_1, the equation $x^k = b$ has the same number of solutions in G_1 as does the equation $x^k = \phi(b)$ in G_2.
> 7. If G_1 is finite, thenn G_1 and G_2 have exactly the same number of elements of every order.

Theorem 6.2 Properties of Isomorphisms Acting on Groups

> Suppose that ϕ is an isomorphism from a group G_1 onto a group G_2. Then
>
> 1. ϕ^{-1} is an isomorphism from G_2 onto G_1.
> 2. G_1 is Abelian if and only if G_2 is Abelian.
> 3. G_1 is cyclic if and only if G_2 is cyclic.
> 4. If K is a subgroup of G_1, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of G_2.
> 5. If K is a subgroup of G_2, then $\phi^{-1}(K) = \{g \in G_1 \mid \phi(g) \in K\}$ is a subgroup of G_1.
> 6. $\phi(Z(G_1)) = Z(G_2)$.

To prove groups G_1 and G_2 are not isomorphic:

- Observe that $|G_1| \neq |G_2|$.
- Observe that G_1 is cyclic but G_2 is not.
- Observe that G_1 is Abelian but G_2 is not.
- show that the largest order of any element in G_1 is not the same as that in G_2.
- Show that the number of elements of some specific order in G_1 is not the same as G_2.

6.4 Automorphisms

Definition Inner Automorphism Induced by a

> Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is called the **inner** automorphism of G induced by a.

$\mathrm{Aut}(G)$: the set of all automorphisms of G.

$\mathrm{Inn}(D)$: the set of all inner automorphisms of G.

Theorem 6.3 $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups.

Theorem 6.4 $\mathrm{Aut}(Z_n) \approx U(n)$.

6.5 Cayley's Theorem

Theorem 6.5 Cayley's Theorem

> Every group is isomorphic to a group of permutations.

The *left regular representation* of G: $\{T_g \mid T_g(x) = gx,\ g \in G\}$.

6.6 Exercise

1. $U(8) \approx U(12)$.
2. For all finite groups, the order of a subgroup divides the order of the group.
3. $|\mathrm{Aut}(D_n)| = n\,|U(n)|$.
4. Prove that

$$|\mathrm{Inn}(D_n)| = \begin{cases} 2n, & n \text{ is odd,} \\ n, & n \text{ is even.} \end{cases}$$

6.7 Bibliography of Arthur Cayley

7 Cosets and Lagrange's Theorem

7.1 Properties of Cosets

Definition Coset of H in G

> Let G be a group and let H be a noempty subset of G. For any $a \in G$, $aH = \{ah \mid h \in H\}$, which is called the **left coset** of H in G containing a. The element a is called the **coset representative** of aH.

Lemma 7.1 Properties of Cosets

> Let H be a subgroup of G, and $a, b \in G$, then
>
> 1. $a \in aH$.
> 2. $aH = H \quad \Leftrightarrow \quad a \in H$.
> 3. $(ab)H = a(bH),\ H(ab) = (Ha)b$.

4. $aH = bH \quad \Leftrightarrow \quad a \in bH$.
5. $aH = bH$ or $aH \cap bH = \varnothing$.
6. $aH = bH \quad \Leftrightarrow \quad a^{-1}b \in H$.
7. $|aH| = |bH| = |H|$.
8. $aH = Ha \quad \Leftrightarrow \quad H = aHa^{-1} \quad \Leftrightarrow \quad H = a^{-1}Ha$.
9. $aH \subset G \quad \Leftrightarrow \quad a \in H$.

7.2 Lagrange's Theorem and Consequences

Theorem 7.1 Lagrange's Theorem: $|H|$ Divides $|G|$

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left cosets of H in G is $|G|/|H|$.

- The **index** of a subgroup H in G is the number of distinct left cosets of H in G, denoted by $|G : H|$.

Corollary 1 $|G : H| = |G|/|H|$.

Corollary 2 $|a|$ Divides $|G|$.

Corollary 3 Groups of Prime Order Are Cyclic.

Corollary 4 $a^{|G|} = e$.

Corollary 5 Fermat's Little Theorem: $a^p \equiv a \mod p$.

- $a^{p^n} \equiv a \mod p$.

Theorem 7.2 $|HK| = |H||K|/|H \cap K|$.

For two finite subgroups H and K of a group, define the set $HK = \{hk \mid h \in H, k \in K\}$. Then $|HK| = |H||K|/|H \cap K|$.

- HK and hK may not be a subgroup.
- ⭐ HK may not be a subgroup of G, but $HK \in G$, so $|HK| < |G|$, but need not divide $|G|$.

Theorem 7.3 Classification of Groups of Order $2p$.

Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to Z_{2p} or D_p.

- $D_3 \approx S_3 \approx \mathrm{GL}(2, Z_2)$.

7.3 An Application of Cosets to Permutation Groups

Definition Stabilizer of a Point

Let G be a group of permutations of a set S. For each i in S, let $\mathrm{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$. We call $\mathrm{stab}_G(i)$ the **stabilizer** of i in G.

Definition Orbit of a Point

Let G be a group of permutations of a set S. For each i in S, let $\mathrm{orb}_G(i) = \{\phi(i) \mid \phi \in G\}$. The set $\mathrm{orb}_G(i)$ is a subset of S called the **orbit** of i under G.

Theorem 7.4 Orbit-Stabilizer Theorem

Let G be a finite group of permutations of a set S. Then, for any i from S, $|G| = |\text{orb}_G(i)| \cdot |\text{stab}_G(i)|$.

7.4 The Rotation Group of a Cube and a Soccer Ball

Theorem 7.5 The Rotation Group of a Cube

The group of rotations of a cube is isomorphic to S_4.

- The rotation group of a pyraminx is isomorphic to A_4.
- The rotation group of a soccer ball (megaminx) is isomorphic to A_5.

7.5 An Application of Cosets to the Rubik's Cube

7.6 Exercises

1. Let a and b be elements of a group G, and H and K be subgroups of G. If $aH = bK$, prove that $H = K$.
2. Let H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$.
3. If G is a finite group of order n with the property that G has exactly one subgroup of order d for each positive divisor d of n, then G is cyclic.
4. Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $|G : H| = |G : K| \, |K : H|$.
5. If a finite group G has subgroups H and K such that $K \subseteq H \subseteq G$ with $[G : K] = p$ where p is prime, prove that $H = G$ or $H = K$.
6. Prove that if G is a finite gruop, the index of $Z(G)$ cannot be prime.
7. Prove that A_5 has no subgroup of order 15, 20 or 30, and S_5 has no subgroup of order 30.

7.7 Bibliography of Joseph Lagrange

8 External Direct Products

8.1 Definition and Examples

Definition External Direct Product

Let $G_1, G_2, \cdots, G_n$ be a finite collection of groups. The external direct product of them, written as $G_1 \oplus G_2 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the i^{th} component is an element of G_i and the operation is componentwise.

- $|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1| \, |G_2| \cdots |G_n|$.
- $Z_m \oplus Z_n \approx Z_{mn}$ if and only if $\gcd(m, n) = 1$.

8.2 Properties of External Direct Products

Theorem 8.1 Order of an Element in a Direct Product

The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2, \cdots, g_n)| = \text{lcm}(|g_1|, |g_2|, \cdots, |g_n|).$$

- If m and n be positive integers that are divisible by a prime p, then the number of elements of order p in $Z_m \oplus Z_n$ is $p^2 - 1$.

Theorem 8.2 Criterion for $G \oplus H$ to be Cyclic.

> Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

Corollary 1 Criterion for $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ to be Cyclic.

Corollary 2 Criterion for $Z_{n_1 n_2 \cdots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$.

> $Z_{n_1 n_2 \cdots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

$$\begin{aligned} Z_2 \oplus Z_{30} &\approx Z_2 \oplus Z_6 \oplus Z_5 \\ &\approx Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 \\ &\approx Z_2 \oplus Z_6 \oplus Z_5 \\ &\approx Z_2 \oplus Z_3 \oplus Z_2 \oplus Z_5 \\ &\approx Z_6 \oplus Z_{10}. \end{aligned}$$

8.3 The Group of Units Modulo n as an External Direct Product

$U_k(n) \equiv \{x \in U(n) \mid x = 1 \mod k\}$ is a subgroup of $U(n)$.

Theorem 8.3 $U(n)$ as an External Direct Product

> Suppose s and t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. In short,
>
> $$U(st) \approx U(s) \oplus U(t).$$
>
> Moreover, $U_s(st)$ is isomorphic to $U(t)$, and $U_t(st)$ is isomorphic to $U(s)$.

$$\left| \begin{aligned} U(st) &\to U(s) \oplus U(t) \\ x &\mapsto (x \mod s, x \mod t) \end{aligned} \right. \qquad \left| \begin{aligned} U_s(st) &\to U(t) \\ x &\mapsto x \mod (t) \end{aligned} \right.$$

Corollary

> Let $m = n_1 n_2 \cdots n_k$, where $gcd(n_i, n_j) = 1$ for $i \neq j$. Then
>
> $$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k).$$

$$\begin{cases} U(2) \approx \{0\}, & \\ U(4) \approx Z_2, & \\ U(2^n) \approx Z_{2^{n-2}} \oplus Z_2, & \text{for } n \geq 3, \\ U(p^n) \approx Z_{p^n - p^{n-1}}, & \text{for } p \text{ an odd prime}. \end{cases}$$

e.g. $\left|\mathrm{Aut}^4(Z_{27})\right| = 1$.

8.4 RSA Public Key Encryption Scheme

Receiver

1. PIck very large primes p and q and compute $n = pq$.
2. Compute the least common multiple of $p - 1$ and $q - 1$; let us call it m.
3. Pick e relatively prime to m.

4. Find d such that $ed \mod m = 1$.
5. Publicly announce n and e.

Sender

1. Convert the message to a string of digits.
2. Break up the message into uniform blocks of digits; call them $M_1, M_2, \cdots, M_k$. (The integer calue of each M_i must be less than n. In practive, n is so large that this is not a concern.)
3. Check to see that the greatest common divisor of each M_i and n is 1. If not, n can be factored and out code is broken. (In practice, the primes p and q are so large that they exceed all M_i, so this step may be omitted.)
4. Calculate and send $R_i = M_i^e \mod n$.

Receiver

1. For each received message R_i, calculate $R_i^d \mod n$.
2. Covert the string of digits back to a string of characters.

Principles

$U(n) \approx U(p) \oplus U(q) \approx Z_{p-1} \oplus Z_{q-1}$.

$R_i^d = (M_i^e)^d = M_i^{ed} = M_i^{1+km} = M_i$.

8.5 Exercises

1. $G \oplus H$ is Abelian if and only if G and H are Abelian.
2. $G_1 \approx G_2,\ H_1 \approx H_2 \quad \Rightarrow \quad G_1 \oplus H_1 \approx G_2 \oplus H_2$.
3. $A \oplus B \approx A \oplus C \quad \Leftrightarrow \quad B \approx C$.
4. $U(8) \approx U(12),\ U(55) \approx U(75),\ U(144) \approx U(140),\ U_{50}(200) \approx U(4)$.
5. $U_p(p^n) \approx Z_{p^{n-1}}$.
6. For relatively prime positive integeres $s \leq n$ and $t \leq n$, show that $U_{st}(n) = U_s(n) \cap U_t(n)$.

8.6 Bibliography of Leonard Adleman

9 Normal Subgroups and Factor Groups

9.1 Normal Subgroups

Definition Normal Subgroup

> A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all a in G. We denote this by $H \lhd G$.

Theorem 9.1 Normal Subgroup Test

> A subgroup H of G is normal in G if and only if $xHx^{-1} \subseteq H$ for all x in G.

e.g.

- Every subgroup of an Abelian group is normal.
- The center $Z(G)$ of a group is normal.

- A_n is a normal subgroup of S_n.
- Every subgroup of D_n consisting solely of rotations is normal.
- $\mathrm{SL}(2, \mathbb{R})$ is a normal subgroup of $\mathrm{GL}(2, \mathbb{R})$.

Properties:

- If H and K are subgroups of G and H is normal, then HK is a subgroup of G.
- If a group G has a unique subgroup H of some finite order, then H is normal in G.
- Normality is not transitive: $K \lhd L \lhd G \nRightarrow K \lhd G$.
- If N and M are normal, then $N \cap M$ and NM are normal.
- $K/N \lhd G/N \quad \Rightarrow \quad K \lhd G$.

9.2 Factor Groups

Theorem 9.2 Factor (Quoation) Groups

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

- The converse is also true: if $aHbH = abH$ defines a group operation on the set of left cosets of H in G, then H is normal in G.

9.3 Applications of Factor Groups

Theorem 9.3 G/Z Theorem

> Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian, thus $G/Z(G)$ is trivial.

- If G/H is cyclic, where H is a subgroup of $Z(G)$, then G is Abelian.
- If G is non-Abelian, then $G/Z(G)$ is not cyclic.
  - A non-Abelian group of order pq, where p and q are primes, must have a trivial center.
- If $K = \{H, a_1H, a_2H, a_3H\}$ is a subgroup of the factor group G/H, then the set $K = H \cup a_1H \cup a_2H \cup a_3H$ is a subgroup of G of order $4\,|H|$, called the **pull back** of K to G.
- Suppose that G is a finite group and a factor group G/H has an element aH of order n, then G has an element of order n.

Theorem 9.4 $G, G/Z(G)$

> For any group G, $G/Z(G)$ is isomorphic to $\mathrm{Inn}(G)$.

It can be proved by the First Isomorphism Theorem in chapter 10 easily.

- $|Z(D_6)| = 2 \Rightarrow |D_6/Z(D_6)| = 6 \Rightarrow D_6/Z(D_6) \approx D_3 \text{ or } Z_6$. By Theorem 9.3 and 9.4, we know that $\mathrm{Inn}(D_6) \approx D_3$.
- $\mathrm{Inn}(D_{2n}) \approx D_n,\ \mathrm{Inn}(D_{2n+1}) \approx D_{2n+1}$.

Theorem 9.5 Cauchy's Theorem for Abelian Groups

> Let G be a finite Abelian group and let p be a prime that divides the order of G, then G has an element of order p.

9.4 Internal Direct Products

Definition Internal Direct Product of H and K

> We say that G is the internal direct product of H and K and write $G = H \times K$ if H and K are normal subgroups of G and
>
> $$G = HK \text{ and } H \cap K = \{e\}.$$

- If s and t are relatively prime positive integers then $U(st) = U_s(st) \times U_t(st)$.
- $D_6 = \{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\} \times \{R_0, R_{180}\} \approx D_3 \oplus Z_2$.

Definition Internal Direct Product $H_1 \times H_2 \times \cdots H_n$

> Let $H_1, H_2, \cdots, H_n$ be a finite collection of notmal subgroups of G. We say that G is the internal direct product of $H_1, H_2, \cdots, H_n$ and write $G = H_1 \times H_2 \times \cdots \times H_n$, if
>
> 1. $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n \mid h_i \in H_i\}$,
> 2. $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, \cdots, n-1$.

Theorem 9.6 $H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$

> If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \cdots, H_n$, then G is isomorphic to the external direct product of $H_1, H_2, \cdots, H_n$.

- To prove this
  - $\forall h_i \in H_i, h_j \in H_j, h_i h_j = h_j h_i$.
  - Each member of G can be expressed uniquely in the form $h_1 h_2 \cdots h_n$.
  - Mapping: $\phi(h_1 h_2 \cdots h_n) = (h_1, h_2, \cdots, h_n)$.
- If $m = n_1 n_2 \cdots n_k$, $(n_i, n_j) = 1$ for $i \neq j$, then

$$\begin{aligned} U(m) &= U_{m/n_1}(m) \times U_{m/n_2}(m) \times \cdots \times U_{m/n_k}(m) \\ &\approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k) \end{aligned}$$

Classification Theorems

- Classification of subgroups of finite cyclic groups: There is exactly one subgroup for each divisor of the order of the group and no others.
- Classification of groupus of prime order: Every group of prime order p is isomorphic to Z_p.
- Classification of groups of $2p$ where p is an odd prime: Every group of $2p$ is isomorphic to Z_{2p} or D_p.
- Classification of groups of 4: Every group of order 4 is isomorphic to Z_4 or $Z_2 \oplus Z_2$.

Theorem 9.7 Classification of finite Abelian groups of squarefree order

> Every Abelian group of order $p_1 p_2 \cdots p_k$ where p_i are distinct primes is cyclic.

- $G = H_1 \times H_2 \times \cdots \times H_k$.

Theorem 9.8 Classification of Groups of Order p^2

> Every group of order p^2, where p is a prime, is isomorphic to Z_{p^2} or $Z_p \oplus Z_p$.

- Let G be a group of order p^2, then every subgroup of the form $\langle a \rangle$ is normal in G.

Corollary

> If G is a group of order p^2, where p is a prime, then G is Abelian.

9.5 Exercises

1. Prove that if H has index 2 in G, then H is normal in G.

2. Prove that a factor group of a cyclic group is cyclic, a factor group of an Abelian group is Abelian.
3. H is normal in G, a is an element of G. Then the order of the element aH in the factor group G/H is the smallest positive integer n such that a^n is in H. Moreover, $|gH|$ divides $|g|$.
4. $H \approx K \not\Rightarrow G/H \approx G/K$.
5. Groups of order 2 or 4 are all Abelian.
6. Let G be a group and let $S = \left\{x^{-1}y^{-1}xy \mid x, y \in G\right\}$, $G' = [G, G] = \langle S \rangle$. Then
    1. G' is normal in G.
    2. G/G' is Abelian.
    3. If G/N is Abelian, then $G' \subseteq N$.
    4. If H is a subgroup of G and $G' \subseteq H$, then H is normal.
7. $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$.

Question: 66.

9.6 Bibliography of Evariste Galois

10 Group Homomorphisms

10.1 Definition and Examples

Definition Group Homomorphism

> A homomorphism ϕ from a group G_1 to a group G_2 is a mapping from G_1 into G_2 that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Definition Kernel of a Homomorphism

> The **kernel** of a homomorphism ϕ from a group G to a group with identity e is the set $\mathrm{Ker}\, \phi = \{x \in G \mid \phi(x) = e\}$.

- Any isomorphism is a homoporphism that is also onto and one-to-one, the kernel of which is a trivial subgroup.
- Let $\phi : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*,\ A \mapsto \det A$, then $\mathrm{Ker}\, \phi = \mathrm{SL}(n, \mathbb{R})$.
- $U(st) = U_s(st)U_t(st),\ \phi(ab) = a$, then $\mathrm{Ker}\, \phi = U_t(st)$.
- Every linear transformation is a group homomorphism and the null-space is the same as the kernel. An invertible linear transformation is a group isomorphism.

10.2 Properties of Homomorphisms

Theorem 10.1 Properties of Elements Under Homomorphisms

> Let ϕ be a homomorphism from a group G_1 to a group $G_2$and let g be an element of G_1. Then
>
> 1. ϕ carries the identity of G_1 to the identity of G_2.
> 2. $\phi(g^n) = \phi(g)^n$ for all n in $\mathbb{Z}$.

3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$ and if $|G_1|$ is finite, then $|\phi(g)|$ divides $|g|$ and $|\phi(G_1)|$.
4. $\operatorname{Ker}\phi$ is a subgroup of G_1.
5. $\phi(a)=\phi(b)$ if and only if $a\operatorname{Ker}\phi=b\operatorname{Ker}\phi$.
6. If $\phi(g)=g'$, then $\phi^{-1}(g')=\{x\in G_1 \mid \phi(x)=g'\}=g\operatorname{Ker}\phi$.

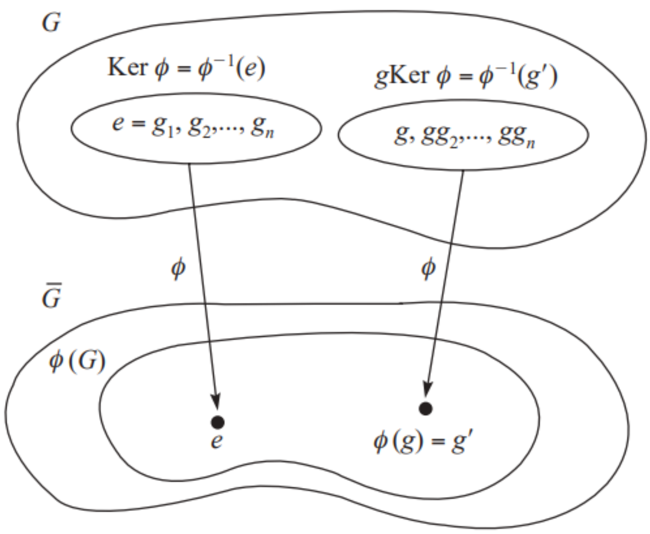
- The particular solution to $Ax=b$ is x_0, the entire solution to $Ax=0$ is S, then the entire solution to $Ax=b$ is x_0+S. It's a special case of property 6.

Theorem 10.2 Properties of Subgroups Under Homomorphisms

Let ϕ be a homomorphism from a group G_1 to a group G_2 and let H be a subgroup of G. Then

1. $\phi(H)=\{\phi(h)\mid h\in H\}$ is a subgroup of G_2.
2. If H is cyclic, then $\phi(H)$ is cyclic.
3. If H is Abelian, then $\phi(H)$ is Abelian.
4. If H is normal in G_1, then $\phi(H)$ is normal in $\phi(G_1)$.
5. If $|\operatorname{Ker}\phi|=n$, then ϕ is an n-to-1 mapping from G_1 onto $\phi(G_1)$.
6. If H is finite, then $|\phi(H)|$ divides $|H|$.
7. $\phi(Z(G_1))$ is a subgroup of $Z(\phi(G_1))$.
8. If K is a subgroup of G_2, then $\phi^{-1}(K)=\{k\in G_1\mid \phi(k)\in K\}$ is a subgroup of G_1.
9. If K is a normal subgroup of G_2, then $\phi^{-1}(K)=\{k\in G_1\mid \phi(k)\in K\}$ is a normal subgroup of G_1.
10. If ϕ is onto and $\operatorname{Ker}\phi=\{e\}$, then ϕ is an isomorphism from G_1 to G_2.

- $\left|\phi^{-1}(H)\right|=|H|\,|\operatorname{Ker}\phi|$.
- The inverse image of an element is a coset of the kernel and that every element in that coset has the same image.



Corollary Kernels are Normal

Let ϕ be a group homomorphism from G_1 to G_2, then $\operatorname{Ker}\phi$ is a normal subgroup of G_1.

- The number of homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$ is $d=\gcd(m,n)$, since such a homomorphism is completely specified by the image a of 1, and $|a|$ divides both m and n, and $d=\sum\phi(a)$ for all divisor a of d.

10.3 The First Isomorphism Theorem

Theorem 10.3 First Isomorphism Theorem

> Let ϕ be a group homomorphism from G_1 to G_2, then the mapping from $G_1/\operatorname{Ker}\phi$ to $\phi(G_1)$, given by $g\operatorname{Ker}\phi \to \phi(g)$, is an isomorphism. In symbols, $G_1/\operatorname{Ker}\phi \approx \phi(G_1)$.

Corollary 1

> If ϕ is a homomorphism from a finite group G_1 to G_2, then $|G_1|/\left|\operatorname{Ker}\phi\right| = |\phi(G_1)|$.

Corollary 2

> If ϕ is a homomorphism from a finite group G_1 to G_2, then $|\phi(G_1)|$ divides $|G_1|$ and $|G_2|$.

The commutative diagram of Theorem 10.3 is:

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\gamma"'] & & \phi(G) \\
& G/\mathrm{Ker}\phi \arrow[ur, "\psi"'] &
\end{tikzcd}$$

$\gamma : G \to G/\operatorname{Ker}\phi,\ g \mapsto g\operatorname{Ker}\phi$ is called the **natural mapping** from G to $G/\operatorname{Ker}\phi$. The diagram is commutative since $\psi\gamma = \phi$.

- $\mathbb{Z}/\langle n\rangle \approx \mathbb{Z}_n$ since $\phi(m) = m \mod n$ is a homomorphism with $\operatorname{Ker}\phi = \langle n\rangle$. Likewise, $\mathbb{Z}[\mathrm{i}]/\{sn + tn\mathrm{i} \mid s,t \in \mathbb{Z}\} \approx \mathbb{Z}_n[\mathrm{i}]$.
- $\mathrm{GL}(2,\mathbb{R})/\mathrm{SL}(2,\mathbb{R}) \approx \mathbb{R}^*$ since $\phi(A) = \det A$ from $\mathrm{GL}(2,\mathbb{R})$ onto $\mathbb{R}^*$ is a homomorphism with $\operatorname{Ker}\phi = \mathrm{SL}(2,\mathbb{R})$. Likewise, $\mathrm{SL}^{\pm}(2,\mathbb{R}) = \{A \in \mathrm{GL}(2,\mathbb{R}) \mid \det A = \pm 1\} \approx \mathbb{R}^+$ since we have $\phi(A) = (\det A)^2$.
- For an Abelian group G and a positive integer k, let G^k denote the subgroup $\left\{x^k \mid x \in G\right\}$ and $G^{(k)}$ the subgroup $\left\{x \in G \mid x^k = e\right\}$. Then $G/G^{(k)} \approx G^k$ since we have $\phi(x) = x^k$, but $G/G^k \not\approx G^{(k)}$ since $\phi(x^k) = x$ may be not well-defined.

Theorem N/C Theorem

> Let H be a subgroup of a group G. Noting that the normalizer of H in G, $N(H) = \left\{x \in G \mid xHx^{-1} = H\right\}$, and the centralizer of H in G, $C(H) = \left\{x \in G \mid \forall h \in H,\ xhx^{-1} = h\right\}$, are subgroups of G, consider the mapping from $N(H)$ to $\mathrm{Aut}(H)$ given by $g \mapsto \phi_g$, where $\phi_g(h) = ghg^{-1}$. This mapping is a homomorphism with $\operatorname{Ker}\phi_g = C(H)$. So, $N(H)/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$, in fact, $N(H)/C(H) \approx \mathrm{Inn}(H)$.

Theorem 10.4 Normal Subgroups Are Kernels

> Every normal subgroup N of a group G is the kernel of a **natural homomorphism** of G defined by $\phi : G \to G/N,\ g \mapsto gN$.

10.4 Exercieses

1. $G \xrightarrow{\phi} H \xrightarrow{\sigma} K$, then $\operatorname{Ker}\phi$ is a normal subgroup of $\operatorname{Ker}\sigma\phi$, and $[\operatorname{Ker}\sigma\phi : \operatorname{Ker}\phi] = |H|/|K|$.
2. $U(st)/U_s(st) \approx U(s)$.
3. If $G = \langle S\rangle$ and ϕ is a homomorphism from G to some group, prove that $\phi(G) = \langle\phi(S)\rangle$.
4. Let N be a normal subgroup of a group G. Prove that every subgroup of G/N has the form H/N, where H is a subgroup of G.
5. For any two primes p and q with $p < q$ where $p \nmid q - 1$, a group of order pq is cyclic.

Theorem First Isomorphism Theorem

> Let ϕ be a group homomorphism from G_1 onto G_2, then the mapping ψ from $G_1/\operatorname{Ker}\phi$ to G_2, given by $g\operatorname{Ker}\phi \to \phi(g)$, is an isomorphism. In symbols, $G_1/\operatorname{Ker}\phi \approx G_2$.

Proof $\psi(x\operatorname{Ker}\phi y\operatorname{Ker}\phi) = \psi(xy\operatorname{Ker}\phi) = \phi(xy) = \phi(x)\phi(y) = \psi(x\operatorname{Ker}\phi)\psi(y\operatorname{Ker}\phi)$. $\square$

Theorem Second Isomorphism Theorem

> If K is a subgroup of G and N is a normal subgroup of G, then $K/(K\cap N) \approx KN/N$.

Proof Let $\phi: K \to KN/N,\ k \mapsto kN$, then $\operatorname{Ker}\phi = K\cap N$. $\square$

Theorem Third Isomorphism Theorem

> If M and N are normal subgroups of G and $N \subseteq M$, then $(G/N)/(M/N) \approx G/M$.

Proof Let $\phi: G/N \to G/M,\ gN \mapsto gM$, then $\operatorname{Ker}\phi = M/N$. $\square$

10.5 Bibliography of Camile Jordan

11 Fundamental Theorem of Finite Abelian Groups

11.1 The Fundamental Theorem

Theorem 11.1 Fundamental Theorem of Finite Abelian Groups

> Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Writing an Abelian group G in the form $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$, is called determining the isomorphism class of G.

- If $k = n_1 + n_2 + \cdots + n_t$, then $\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}}$ is an Abelian group of order p^k.

11.2 The Isomorphism Classes of Abelian Groups

Corollary Existence of Subgroups of Abelian Groups

> If m divides the order of a finite Abelian group G, then G has a subgroup of order m.

11.3 Proof of the Fundamental Theorem

Lemma 1

> Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where $H = \left\{x \in G \mid x^{p^n} = e\right\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.

- Given an Abelian group G with $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, where p's are distinct primes, let $G(p_i) = \left\{x \in G \mid x^{p_i^{n_i}} = e\right\}$, then $G = G(p_i) \times G(p_2) \times \cdots \times G(p_k)$ and $|G(p_i)| = p_i^{n_i}$.

Lemma 2

> Let G be an Abelian group of prime-power order and let a be an element of maximum order in G, then G can be written in the form $\langle a\rangle \times K$.

Lemma 3

> A finite Abelian group of prime-order is an internal direct product of cyclic groups.

Lemma 4

> Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the H's and K's are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

11.4 Exercises

1. The number of elements in $\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}$ of order p is $p^{n-1} + p^{n-2} + \cdots + p + 1 = \dfrac{p^n - 1}{p - 1}$.
2. Dirichlet's Theorem says that, for every pair of relatively prime integers a and b, there are infinitely many primes of the form $at + b$. Use **Dirichlet's Theorem** to prove that every finite Abelian group is isomorphic to a subgroup of a U-group. (Hint: $U(p_i^{n_i}t + 1) \approx \mathbb{Z}_{p_i^{n_i}t}$)