Math 417: Abstract Algebra

Lanxiao Hermite Bai

December 12, 2016

Contents

1 Algebraic Themes

1.1 Symmetry

Definition 1.1.1 (Symmetry) *A **symmetry** is an undetectable motion. An object is symmetric if it has symmetries.*

1.2 Multiplication Table

Example of Multiplication Table Example of rectangle

	e	r	r^2	r^3	a	b	c	d
e	e	r	r^2	r^3	a	b	c	d
r	r	r^2	r^3	e	d	c	a	b
r^2	r^2	r^3	e	r	b	a	d	c
r^3	r^3	e	r	r^2	c	d	b	a
a	a	c	b	d	e	r^2	r	r^3
b	b	d	a	c	r^2	e	r^3	r
c	c	b	d	a	r^3	r	e	r^2
d	d	a	c	b	r	r^3	r^2	e

Table 1: Table of Multiplication for Rectangle

Property of Symmetry

1. The product of symmetries is independent of how they are associated,

$$s(tu) = (st)u$$

2. The *nonmotion* e compose with any other symmetry (in either order) is the second symmetry,

$$eu = ue = u$$

3. For each symmetry there is an inverse, such that the composition of the symmetry with its inverse (in either order) is the *nonmotion* e,

$$uu^{-1} = u^{-1}u = e$$

1.3 Symmetries and Matrices

Definition 1.3.1 (Isometry) *A transformation $\tau : R \to R$ is called an* ***isometry*** *if for all points $\mathbf{a}, \mathbf{b} \in R$, we have $d(\tau(\mathbf{a}), \tau(\mathbf{b})) = d(\mathbf{a}, \mathbf{b})$, where d demotes the usual Euclidean distance function.*

Proposition 1.3.1 *Let R denote a polygon or a polyhedron in three-dimensional space, locate with its centroid at the origin of coordinates. Then every symmetry if R is the restriction to R of a linear isometry of $\mathbb{R}^3$.*

1.4 Permutations

Definition 1.4.1 (Permutation) *The symmetries of a configuration of identical objects are called* ***permutations****. There are $n!$ permutations for n objects. The set of all the permutations is denoted by $Sym(X) = S_n$.*

qq

1. The multiplication of permutation is associative.
2. There is an identity permutation e, which leaves each object in its original position.
3. For each permutation σ, there is an inverse permutation σ^{-1}.

Definition 1.4.2 (Cycle) *A permutation that permutes several numbers cyclically and leave all other. numbers fixed is call a* ***cycle****.*

Definition 1.4.3 (Disjoint) *Two cycles are* ***disjoint*** *if each leaves the fixed numbers moved by each other.*

Definition 1.4.4 (Order) *A permutation π is said to have* ***order*** *k if k^{th} power of π is the identity and no lower power of π is the identity.* ***A k-cycle has order k.***

Theorem 1.4.1 *Every permutation of a finite set can be written uniquely as a product of disjoint cycles.*

1.5 Divisibility in the Integers

Definition 1.5.1 (Integer) *We denote the set of* ***integers*** $\{0, \pm 1, \pm 2, \ldots\}$ *by* $\mathbb{Z}$.

Definition 1.5.2 (Natural Number) *We denote the set of natural numbers* $\{1, 2, 3, \ldots\}$ *by* $\mathbb{N}$.

Proposition 1.5.1 *: Addition and Multiplication*

1. *Addition on* $\mathbb{Z}$ *is commutative and associative.*
2. *0 is an identity element for addition;* $\forall a \in \mathbb{Z}, 0 + a = a$.
3. *Every element* a *of* $\mathbb{Z}$ *has an additive inverse* $-a$ *that* $a + (-a) = 0$.
4. *Multiplication on* $\mathbb{Z}$ *is commutative and associative.*
5. *1 is is an identity element for multiplication;* $\forall a \in \mathbb{Z}, 1a = a$.
6. *The distribute law holds;* $a(b + c) = ab + ac$.
7. $\mathbb{N}$ *is closed under addition and multiplication.*
8. *The product of non-zero integers is non-zero.*

Definition 1.5.3 (Divisibility) *We say that an interger* a ***divides*** b, *(or that* b *is divisible by* a*), if there is an interger* q *such that* $aq = b$*; we write* $a|b$ *for "*a *divides* b*"*

Proposition 1.5.2 *Properties of Divisibility:*

Let a, b, c, u, and v denote integers.

1. *If* $uv = 1$, *then* $u = v = 1$ *or* $u = v = -1$.
2. *If* $a|b$ *and* $b|a$, *then* $a = \pm b$.
3. *Divisibility is transitive; if* $a|b$, $b|c$, *then* $a|c$.
4. *If* $a|b$ *and* $a|c$, *then* $a|(sb + tc)$, *where* s *and* t *are integers.*

Definition 1.5.4 (Prime) *A natural number is **prime** if it is greater than 1 and not divisible by any natural number other than 1 and itself.*

Proposition 1.5.3 *Any natural number other than 1 can be written as a product of prime numbers.*

Theorem 1.5.1 *There are infinitely many prime numbers.*

Proposition 1.5.4 *Given integers a and b, with $d \geq 1$, there exist unique intergers q and r[1] such $a = qd + r$ and $0 \leq r < d$.*

Definition 1.5.5 (Greatest Common Divisor) *A natural number d is the greatest common divisor of nonzero integers m and n if*

1. *$d|m$ and $d|n$;*
2. *whenever $x \in \mathbb{N}$ divides m and n, then x also divides d.*

Proposition 1.5.5 *For integers m and n, let*

$$I(m, n) = \{am + bn : a, b \in \mathbb{Z}\}. \tag{1}$$

1. *For $x, y \in I(m, n)$, $x + y \in I(m, n)$ and $-x \in I(m, n)$.*
2. *$\forall x \in \mathbb{Z}, xI(m, n) \subseteq I(m, n)$*
3. *If $b \in \mathbb{Z}$ divides m and n, then b divides all elements of $I(m, n)$.*

Lemma 1.5.1 *Let m and n be nonzero integers. If a natural number d is a common divisor of m and n and an element of $I(m, n)$, then d is the greatest common divisor of m and n.*

Proposition 1.5.6 *Let $m, n, n_1, ..., n_k..., q_1, q_2, ...q_k \in \mathbb{Z}$*

$$m = q_1 n + n_1 \tag{2}$$

$$n = q_2 n_1 + n_2 \tag{3}$$

[1]The q is called **quotient** and the r is called **remainder**.

$$\dots$$

$$n_{k-2} = q_k n_{k-1} + n_k \tag{4}$$

$$\dots$$

$$n_{r-1} = q_{r+1} n_r \tag{5}$$

The natural number n_r is the greatest common divisor of m and n, and furthermore $n_r \in I(m, n)$.

Corollary 1.5.1 *Let m and n be nonzero integers, and write $d = g.c.d.(m, n)$*

1. *d is the least element of $\mathbb{N} \cap I(m, n)$.*
2. *$I(m, n) = \mathbb{Z}d$, the set of all integer multiples of d.*

Definition 1.5.6 (Relatively Prime) *Nonzero integers m and n are **relatively prime** if $g.c.d.(m, n)$.*

Corollary 1.5.2 *Two nonzero integers m and n are relatively prime if and only if there exist integers s and t such that $1 = sm + tn$.*

Corollary 1.5.3 *Suppose that a and b are relatively prime natural numbers, that x is an integer, and that both a and b divide x. Then ab divides x.*

Proposition 1.5.7 *If p is a prime number and a is any nonzero integer, then either p divides a or p and a are relatively prime.*

Proposition 1.5.8 *Let p be a prime number, and a and b nonzero integers. If $p|ab$, then $p|a$ or $p|b$.*

Corollary 1.5.4 *Suppose that a prime number $p|a_1a_2...a_r$, which for $r \in [1, r], a_n \neq 0$, then p divides one of the factors.*

Theorem 1.5.2 *The prime factorization of a natural number is unique.*

Definition 1.5.7 *Greatest common Divisor of Several Numbers A natural nnumber d is the greatest common divisor of nonzero integers $a_1, a_2, ..., a_n$, if*

1. *d divides each a_i and*

2. *whenever $x \in \mathbb{N}$ divides each a_i, then x also divides d.*

Lemma 1.5.2 *Given nonzero integers $a_1, a_2, ..., a_n (n \leq 2)$, there is a natural number d and an n-by-n integer matrix Q such that Q is invertible, Q^-1 also has integer entries, and*

$$(d, 0, ..., 0) = (a_1, a_2, ..., a_n)Q \tag{6}$$

Proposition 1.5.9 *The greatest common divisor of nonzero integers $a_1, a_2, ..., a_n$ exists, and is an integer linear combination of $a_1, a_2, ..., a_n$.*

Definition 1.5.8 (Relatively Prime) *We say that nonzsro integers $a_1, ..., a_n$ are **relatively prime** if their greatest common divisor is 1. We say that they are **pairwise relatively prime** if a_i and a_j are relatively prime whenever $i \neq j$.*

1.6 Modular Arithmetic

Definition 1.6.1 (Congruence) *Given integers a and b, and a natural number n, we say that "a is congruent to b modulo n" and we write $a \equiv b \mod n$ if $n|(a - b)$.*

Lemma 1.6.1 *Properties of Mod*

1. *$\forall a \in \mathbb{Z}, a \equiv a \mod n$(Reflexive)*
2. *$\forall a, b \in \mathbb{Z}$, if $a \equiv b \mod n$ if and only if $b \equiv a \mod n$.(Symmetric)*
3. *$\forall a, b, c \in \mathbb{Z}$, if $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv v \mod n$.(Transitive)*

Lemma 1.6.2 *For $a, b \in \mathbb{Z}$, the following are equivalent:*

- *$a \equiv b \mod n$.*
- *$[a] = [b]$.*[2]
- *$rem_n(a) = rem_n(b)$.*[3]

[2]The set a is called the residue class or congruence class of a modulo n.

[3]Denote by $rem_n(a)$ the unique number r such that $0 \leq r < n$ and $a - r$ is divisible by n.

- $[a] \cap [b] \neq \varnothing$

Corollary 1.6.1 *There exist exactly n distinct residue classes modulo n, namely $[0], [1], ...[n-1]$. These classes are mutually disjoint.*

Lemma 1.6.3 *Let a, a', b, b' be integers with $a \equiv a' \mod n$ and $b \equiv b \mod n$. Then $a + b \equiv a' + b' \mod n$ and $ab \equiv a'b' \mod n$.*

Proposition 1.6.1 *Properties of Modulo Congruence:*

1. *Addition on $\mathbb{Z}_n$ is commutative and associative, $\forall [a], [b], [c] \in \mathbb{Z}_n$*
$$[a] + [b] = [b] + [a] \tag{7}$$
and,
$$[a] + [b] + [c] = [a] + ([b] + [c]) \tag{8}$$
0 is an identity element for addition, $\forall [a] \in \mathbb{Z}_n$,
$$[0] + [a] = [a] \tag{9}$$
2. *Every element $[a]$ of $\mathbb{Z}_n$ has an additive inverse $[-a]$, that*
$$[a] + [-a] = [0] \tag{10}$$
3. *Muktiplication on $\mathbb{Z}_n$ is commutative and associative; $\forall [a], [b], [c] \in \mathbb{Z}_n$,*
$$[a][b] = [b][a] \tag{11}$$
,and
$$[a][b][c] = [a]([b][c]) \tag{12}$$
4. *$[1]$ is an identity for multiplication; $\forall [a] \in \mathbb{Z}_n$,*
$$[1][a] = [a][1] \tag{13}$$
5. *The distributive law hold; $\forall [a], [b], [z] \in \mathbb{Z}_n$,*
$$[a]([b] + [c]) = [a][b] + [a][c] \tag{14}$$

Proposition 1.6.2 (Chinese Reminder Theorem) *Suppose a and b are relatively prime natural numbers, and α and beta are integers. There exists an integer x such that $x \equiv \alpha \mod a$ and $x \equiv \beta \mod b$. Moreover, x is unique up to congruence modulo ab.*

1.7 Polynomials

Denotation Denote set of rational numbers by $\mathbb{Q}$, and denote set of real numbers by $\mathbb{R}$ and denote set of complex numbers by $\mathbb{C}$.

Addition and Multiplication

$$(\sum_j a_j x^j) + (\sum_j b_j x^j) = \sum_j (a_j + b_j) x^j \tag{15}$$

and,

$$(\sum_i a_i x^i)(\sum_j b_j x^j) = \sum_i \sum_j (a_i b_j) x^{i+j} \tag{16}$$

$$= \sum_k (\sum_{i,j:i+j=k} a_i b_j) x^k = \sum_k (\sum_i a_i b_{k-i}) x^k \tag{17}$$

Proposition 1.7.1 *Basic Properties:*

1. *Addition in $K[x]$ is commutative and associative; $f + g = g + f$ and $\forall f, g, h \in K[x], f + g + h = f + (g + h)$.*
2. *0 is an identity element for addition; $0 + f = f$.*
3. *Every element f of $K[x]$ has an additive inverse $-f$; $f + (-f) = 0$.*
4. *Multiplication in $K[x]$ is commutative and associative; that is, for all $f, g, h \in K[x]$, $fg = gf$, and $f(gh) = (fg)h$.*
5. *1 is an identity for multiplication; $\forall f \in K[x], 1f = f$.*
6. *The distributed law holds; $\forall f, g, h \in K[x], f(g + h) = fg + fh$.*

Definition 1.7.1 (Degree) *The **degree** of a polynomial $\sum_k a_k x^k$ is the largest k that $a_k \neq 0$. If $p = \sum_j a_j x^j$ is a nonzero polynomial of degree k, denoted $deg(p)$, the **leading coefficient** of p is a_k and leading term of p is $a_k x^k$. A polynomial is said to be **monic** if its leading coefficient is 1.*

Proposition 1.7.2 *Let $f, g \in K[x]$.*

1. *$deg(fg) = deg(f) + deg(g)$; in particular, if f and g are both nonzero, then $fg \neq 0$.*

2. $deg(f+g) \leq \max\{deg(f), deg(g)\}$

Proposition 1.7.3 *Let f, g, h, u, v denote polymonials like in $K[x]$.*

1. *If $uv = 1$, then $u, v \in K$.*
2. *If $f|gandg|f$, then there is a $k \in K$ such that $g = kf$.*
3. *Divisibility is transitive*
4. *If $f|g$ and $f|h$, then $\forall s, t \in K[x], f|(sg+th)$.*

Definition 1.7.2 (Irreducible) *We say that a polymonial in $K[x]$ is **irreducible** if its degree is positive and it cannot be written as a product of two polynomials each of strictly smaller (positive)degree.*

Proposition 1.7.4 *Any polynomial in $K[x]$ of positive degree can be written as a product of irrecucible polynomials.*

Proposition 1.7.5 *$K[x]$ contains infinitely many irreducible polynomials.*

Lemma 1.7.1 *Let p and d be elements of $K[x]$, with $deg(p) \geq deg(d) \geq 0$. Then there is a monomial $m = bx^k \in K[x]$ and a polynomial $p' \in K[x]$ such that $p = md + p'$, and $deg(p') < deg(p)$.*

Proposition 1.7.6 *Let $p, d \in K[x]$, with $deg(d) \geq 0$. Then there exist polynommials q and r in $K[x]$ such that $p = dq + r$ and $deg(r) < deg(d)$.*

Definition 1.7.3 (Great Common Divisor of Polynomials) *A polynomial $f \in K[x]$ is a greatest common divisor of nonzero polynomials $p, q \in K[x]$ if*

1. *$f|p$ and $f|q$ in $K[x]$ and*
2. *whenever $g \in K[x]$ divides p and q, then g also divides f.*

Proposition 1.7.7 *For polynomials $f, g \in K[x]$, let*

$$I(f,g) = af + bg : a, b \in K[x] \tag{18}$$

1. *$\forall p, q \in I(f,g), p+q \in I(f,g)$ and $-p \in I(f,g)$*

2. *$\forall p \in K[x]$, $pI(f,g) \subseteq I(f,g)$.*

3. *If $p \in K[x]$ divides f and g, then p divides all elements in $I(f,g)$.*

Theorem 1.7.1 *ANy two nonzero polynomials $f, g \in K[x]$ have a greatest common divisor $\in I(f,g)$.*

Definition 1.7.4 (Relatively Prime) *Two polynomials $f, g \in K[x]$ are **relatively prime** if g.c.d.$(f,g) = 1$.*

Proposition 1.7.8 *Two polynomials $f, g \in K[x]$ are relatively prime if and only if $1 \in I(f,g)$.*

Proposition 1.7.9 *Properties of irreducible polynomial*

1. *Let p be an irreducible polynomial in $K[x]$ and $f, g \in K[x]$ nonzero polynomials. If $p|fg$, then $p|f$ or $p|g$.*

2. *Suppose that irreducible polynomial $p \in K[x]$ divides a product $f_1 f_2 ... f_s$ of nonzero polynomials. Then p divides one of the factors.*

Theorem 1.7.2 *The factorization of a polynomial in $K[x]$ into irreducible factors is essentially unique.*

Proposition 1.7.10 *Let $p \in K[x]$ and $a \in K$. Then there is a polynomial q such that $p(x) = q(x)(x-a) + p(a)$. Consequently, $p(a) = 0$ if and only if $(x-a)|p$.*

Definition 1.7.5 (Root) *An element $\alpha \in K$ is a **root** of a polynomial $p \in K[x]$ if $p(\alpha) = 0$. The **multiplication of the root** α is k if $x - \alpha$ appears exactly k times in the irreducible pfactorization of p.*

Corollary 1.7.1 *A polynomial $p \in K[x]$ of degree n has at most n roots in K, counting with multiplicities.*

1.8 Counting

Proposition 1.8.1 *A set with n elements has 2^n subsets.*

Proof:

$$N = \sum_{i=0}^{n} \binom{n}{i} = 2^n$$

Proposition 1.8.2 *Let n be a natural number and let k be an integer in $[0, n]$. Let $\left(\begin{array}{c} n \\ k \end{array}\right)$ denote the number of the number of k-element subsets of a set with n elements. Then*

$$\left(\begin{array}{c} n \\ k \end{array}\right) = \frac{n!}{k!(n-k)!} \tag{19}$$

If $k < 0$ or $k > n$,

$$\left(\begin{array}{c} n \\ k \end{array}\right) = 0 \tag{20}$$

and,

$$\left(\begin{array}{c} 0 \\ 0 \end{array}\right) = 1 \tag{21}$$

$$\left(\begin{array}{c} 0 \\ k \end{array}\right) = 0 \tag{22}$$

if $k \neq 0$

Lemma 1.8.1 *Let n be a natural number and $k \in \mathbb{Z}$.*

1. $\left(\begin{array}{c} n \\ k \end{array}\right)$ *is a nonnegative integer.*
2. $\left(\begin{array}{c} n \\ k \end{array}\right) = \left(\begin{array}{c} n \\ n-k \end{array}\right)$.
3. $\left(\begin{array}{c} n \\ k \end{array}\right) = \left(\begin{array}{c} n-1 \\ k \end{array}\right) + \left(\begin{array}{c} n-1 \\ k-1 \end{array}\right)$

Proposition 1.8.3 (Binomial Theorem) *Let x and y be numbers. For $n \geq 0$, we have*

$$(x+y)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array}\right) x^k y^{n-k} \tag{23}$$

Corollary 1.8.1 *Basic Properties:*

1.

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \tag{24}$$

2.

$$0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \tag{25}$$

3.

$$2^{n-1} = \sum_{k=0, k \ odd}^{n} \binom{n}{k} = \sum_{k=0, k \ even}^{n} \binom{n}{k} \tag{26}$$

Lemma 1.8.2 *Let p be a prime number.*

1. *If $0 < k < p$, then $\binom{p}{k}$ is divisible by p.*
2. $\forall a, b \in \mathbb{Z}, (a+b)^p \equiv a^p + b^p \mod p$.

Proposition 1.8.4 .

1. *Let $n \geq 2$ be a natural number. An element $[a] \in \mathbb{Z}_n$ has a multiplicative inverse if and only if a is relatively prime to n.*
2. *If p is a prime, then every nonzero element of $\mathbb{Z}_p$ is invertible.*

Proposition 1.8.5 (Fermat's Little Theorem) *Let p be a prime number.*

1. $\forall a \in \mathbb{Z}, a^p \equiv a \mod p$.
2. *If $p \nmid a, a^{p-1} \equiv 1 \mod p$.*

Definition 1.8.1 (Characteristic Function of X) *Let U be any set, for a subset $X \subseteq U$, the **characteristic function** of X is the function $\boldsymbol{1}_X : U \to 0, 1$ defined by*

$$\boldsymbol{1}_X(u) = \begin{cases} 1 & \text{if } u \in X \\ 0 & \text{if } u \notin X \end{cases} \tag{27}$$

Denotation Denote The relative copmplement of a subset $X \subseteq U$ by X'.

Proposition 1.8.6 *Let $A_1, A_2, ..., A_n \subseteq U$, then*

1.

$$\mathbf{1}_{A_1' \cap A_2' \cap ... \cap A_n'} = 1 - \sum_i \mathbf{1}_{A_i} + \sum_{i<j} \mathbf{1}_{A_i \cap A_j} - \sum_{i<j<k} \mathbf{1}_{A_i \cap A_j \cap A_k} + ... + (-1)^n \mathbf{1}_{A_1 \cap ... \cap A_n} \tag{28}$$

2.

$$\mathbf{1}_{A_1 \cup A_2 \cup ... \cup A_n} = \sum_i \mathbf{1}_{A_i} - \sum_{i<j} \mathbf{1}_{A_i \cap A_j} + \sum_{i<j<k} \mathbf{1}_{A_i \cap A_j \cap A_k} - ... + (-1)^n \mathbf{1}_{A_1 \cap ... \cap A_n} \tag{29}$$

Corollary 1.8.2 *Suppose that U is a finite set and that $A_1, A-2, ..., A_n$ are subsets of U. Then*

1.

$$|A_1' \cap A_2' \cap ... \cap A_n'| = |U| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \sum_{i<j<k} |A_i \cap A_j \cap A_k| + ... + (-1)^n |A_1 \cap ... A_n| \tag{30}$$

2.

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - ... + (-1)^n |A_1 \cap ... A_n| \tag{31}$$

Definition 1.8.2 (Cardinality) *For each natural number n, $\varphi(n)$ is defined to be the cardinality of the set of natural numbers $k < n$ such that k is relatively prime to n.*

Lemma 1.8.3 *Let $k, n \in \mathbb{N}$, with $k|n$. The number of natural numbers $j \leq n$ such that $k|j$ is n/k.*

Corollary 1.8.3 *If p is a prime, then $\forall k \geq 1$, $\varphi(p^k) = p^{k-1}(p-1)$.*

Proposition 1.8.7 *Let n be a natural number with prime factorization $n = p_1^{k_1}...p_s^{k_s}$. Then,*

1.
$$\varphi(n) = n\prod_{i=1}^{s}(1-\frac{1}{p_i}) \tag{32}$$

2.
$$\varphi(n) = \prod_{i=1}^{s}\varphi(p_i^{k_i}) \tag{33}$$

Corollary 1.8.4 *If m, n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Theorem 1.8.1 (Euler's Theorem) *Fix a natural number n. If $a \in \mathbb{Z}$ is relatively prime to n, then*

$$a^{\varphi(n)} \equiv 1 \mod n. \tag{34}$$

1.9 Groups

Operation An *operation* or a *product* on a set G is a function from $G \times G$ to G.

Definition 1.9.1 (Group) *A **group** is a nonempty set G with a product, denoted by juxtaposition, satisfying:*

1. *Associativity: The product is associative: $\forall a, b, c \in G, (ab)c = a(bc)$.*
2. *Identity element: There is an identity element $e \in G, a \in G, ea = ae = a$.*
3. *Inserse element: For each $a \in G$, there is $a^{-1} \in G, aa^{-1} = a^{-1}a = e$.*
4. *Closure: For any $a, b \in G$, $ab \in G$.*

Isomorphic Groups G and H is said to be **isomorphic** if there is a biject map $\varphi : H \to G$ between them that makes the multiplication table match up, namely, $\forall g_1, g_2 \in G$, $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$.[4]

[4] Denote as $H \cong G$

Subgroup If $G \subseteq H$, G is said to be the **subgroup** of H.

Homomorphism A map $f : H \to G$ is said to be **homomorphism** if f take products to products, identity to identity, and inverses to inverses, $f(a \cdot b) = f(a) \cdot f(b)$.

Lemma 1.9.1 *The set $\Phi(n)$ of elements in $\mathbb{Z}_n$ prossessing a multiplicative inverse forms a group (of cardinality $\varphi(n)$) under multiplication, with identity element* [1].

1.10 Rings and Fields

Definition 1.10.1 *A **ring** is a nonempty set R with two operations: addition, donated by + and multiplication, donated by juxtaposition that satisfy:*

1. *Under addition, R is an **Abelian group**.*[5]
2. *Multiplication is associative.*
3. *Multiplication distributes over addition:$\forall a, b, c \in R, a(b + c) = ab + ac$ and $(b + c)a = ba + ca$* [6]

Subring If $G \subseteq H$, G is said to be the **subring** of H.

Proposition 1.10.1 (Chinese Remainder Theorem) *Let a and b be relatively prime natural numbers, each then there is an isomorphism of rings*

$$\mathbb{Z}_{ab} \cong \mathbb{Z}_a \oplus \mathbb{Z}_b \tag{35}$$

defined by $[x]_{ab} \mapsto ([x]_a, [x]_b)$.

Definition 1.10.2 *A **field** is a commutative ring with multiplicative identity element $1 \neq 0$ which every nonzero element is a unit.*[7]

[5] Abelian group is a group that holds communitative law; For $a, b \in R$, $ab = ba$.
[6] If multiplication is commutative, the ring is called a **commutative ring**.
[7] Unit in ring means the multiplicationally invertible elements

1.11 An application to cryptology

Lemma 1.11.1 *For all integers a and h, if $h \equiv 1 \mod m$, then $a^h \equiv a \mod n$.*

Lemma 1.11.2 *$\forall a \in \mathbb{Z}$, if $b \equiv a^r \mod n$, then $b^s \equiv a \mod n$.*

2 Basic Theory of Groups

2.1 First Results

Proposition 2.1.1 (Uniqueness of the identity) *Let G be a group and suppose e and e' are both identity elements in G, then $e = e'$.*

Proposition 2.1.2 (Uniqueness of the inverse) *Let G be a group and $h, g \in G$. If $hg = e$, then $h = g^{-1}$, and if $gh = e$, then $h = g^{-1}$.*

Corollary 2.1.1 *Let $g \in G$, then $g = (g^{-1})^{-1}$.*

Proposition 2.1.3 *Let G be a group and $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.*

Proposition 2.1.4 *Let G be a group and $a \in G$, The map $L_a : G \to G$ defined by $L_a(x) = ax$ is a bijectiion. Similarly $R_a(x) = xa$ is a bijection.*

Corollary 2.1.2 *Let G be a group and $a, b \in G$. The equation $ax = b$ has a unique solution x in G, and likewise the equation $xa = b$ has a unique solution in G.*

Corollary 2.1.3 (Cancellation) *Suppose $a, x, y \in G$. If $ax = ay$, then $x = y$. If $xa = ya$, then $x = y$.*

Corollary 2.1.4 *If G is a finite group, each row and each column of the multiplication table of G contains each element of G exactly once.*

Definition 2.1.1 (Order) *The **order** of a group is its size or cardinality, denote by $|G|$.*

Definition 2.1.2 (Isomorphic) *We say that two groups G and H are **isomorphic** if there is a bijection $\varphi : G \to H$ such that for all $g_1, g_2 \in G$, $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. The map is called an **isomorphism**.*

Definition 2.1.3 (Abelian) *A A group G is called* ***abelian (or commutative)*** *if for all elements $a, b \in G$, the products in the two orders are equal: $ab = ba$.*

Proposition 2.1.5 *Properties of isomorphism:*

1. *Up to isomorphism, $\mathbb{Z}_1$ is the unique group of order 1.*
2. *Up to isomorphism, $\mathbb{Z}_2$ is the unique group of order 2.*
3. *Up to isomorphism, $\mathbb{Z}_3$ is the unique group of order 3.*
4. *Up to isomorphism, there are exactly two groups of order 4, namely $\mathbb{Z}_4$, and the group of rotational symmetries of the rectangular card.*
5. *Up to isomorphism, $\mathbb{Z}_5$ is the unique group of order 5.*
6. *All groups of order no more than 5 are abelian.*
7. *There are at least two nonisomorphic groups of order 6, one abelian and one nonabelian.*

Proposition 2.1.6 (General associative law) *Let M be a set with an associative operation, $M \times M \to M$, denoted by juxtaposition. FOr every $n \geq 1$, there is a unique product $M^n \to M$,*

$$(a_1, a_2, ..., a_n) \mapsto a_1 a_2 ... a_n,$$

such that

1. *The product of one element is that element $(a) = a$.*
2. *The product of two elements agrees with the given operation $(ab) = ab$*
3. $a_1 a_2 ... a_n = (a_1 ... a_k)(a_{k+1} ... a_n)$.

2.2 Subgroup and Cyclic Groups

Definition 2.2.1 (Subgroup) *A nonempty subset H of a group G is called a subgroup if H is itself a group with the group operation inherited from G. We write $H \leq G$ to indicate that H is a subgroup of G.*

Proposition 2.2.1 *Let G be a group and let $H_1, H_2, \cdots, H_n$ be subgroups of G. Then $H_1 \cap H_2 \cap \cdots \cap H_n$ is a subgroup of G. More generally, if $\{H_\alpha\}$ is any collection of subgroups, then $\cap_\alpha H_\alpha$ is a subgroup.*

Proposition 2.2.2 *Let a be an element of a group G. The subgroup $\langle a \rangle$ generated by a is $\{a^k : k \in \mathbb{Z}\}$*[8]

Definition 2.2.2 (Cyclic Group) *Let a be an element of a group G. The set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ of powers of a is called the cyclic subgroup generated by a. If there is an element $a \in G$ such that $\langle a \rangle = G$, we say that G is a cyclic group. We say that a is a generator of the cyclic group.*

Definition 2.2.3 (Order) *The order of the cyclic subgroup generated by a is called the order of a. We denote the order of a by $o(a)$.*

Proposition 2.2.3 *If G is a cyclic group and $g \in G$, $o(g) = |G|/g.c.d(g, |G|)$*

Proof In $\mathbb{Z}_n$, $g \in \mathbb{Z}_n$, $kg \equiv 0 \mod n \Leftrightarrow kg = ln = \mathrm{lcm}(g, n)$.
Since $g.c.d(g, n) \cdot l.c.m(g, n) = gn$, $o(g) = n = |G|/g.c.d(g, |G|)$.■

Proposition 2.2.4 *If the order of a is finite, then it is the least positive integer n such that $a^n = e$. Furthermore, $\langle a \rangle = \{a^k : 0 \leq k < o(a)\}$.*

Proposition 2.2.5 *Let H be a subgroup of $\mathbb{Z}$. Then either $H = 0$, or there is a unique $d \in \mathbb{N}$ such that $H = \langle d \rangle = d\mathbb{Z}$.*

Proposition 2.2.6 *If $d \in \mathbb{N}$, then $d\mathbb{Z} \cong \mathbb{Z}$.*

Proposition 2.2.7 *If $a, b \in \mathbb{N}$, then $a\mathbb{Z} \subseteq b\mathbb{Z}$ if and only if $b|a$.*

Corollary 2.2.1 *Every subgroup of $\mathbb{Z}$ other than 0 is isomorphic to $\mathbb{Z}$.*

Lemma 2.2.1 *Let $n \geq 2$ and let d be a positive divisor of n. The cyclic subgroup $\langle [d] \rangle$ generated by $[d]$ in $\mathbb{Z}_n$ has cardinality $|\langle [d] \rangle| = n/d$*

Proposition 2.2.8 *Let H be a subgroup of $\mathbb{Z}_n$.*

1. *Either $H = [0]$, or there is a $d > 0$ such that $H = \langle [d] \rangle$.*

---

[8] For any group G and any subset $S \subseteq G$, there is a smallest subgroup of G that contains S, which is called the subgroup generated by S.

2. *If d is the smallest of positive intefers s such that $H = \langle [s] \rangle$, then $d|H| = n$.*

Corollary 2.2.2 *Fix a natural number $n \geq 2$.*

1. *Any subgroup of $\mathbb{Z}_n$ is cyclic.*
2. *Any subgroup of $\mathbb{Z}_n$ has cardinality dividing n.*

Corollary 2.2.3 *Fix a natural number $n \geq 2$.*

1. *For any positive divisor q of n, there is a unique subgroup of $\mathbb{Z}_n$ of cardinality q, namely $\langle [n/q] \rangle$.*
2. *For any two subgroups H and H' of $\mathbb{Z}_n$, we have $H \subseteq H' \Leftrightarrow |H|$ divides $|H'|$.*

Proposition 2.2.9 *Every subgroup of a cyclic group is cyclic.*

Proposition 2.2.10 *Let a be an element of finite order n in a group. Then $\langle a^k \rangle = \langle a \rangle$, if and only if k is relatively prime to n. The number of generators of $\langle a \rangle$ is $\varphi(n)$.*

Proposition 2.2.11 *Let a be an element of finite order n in a group. For each positive integer q dividing n, $\langle a \rangle$ has a unique subgroup of order q.*

Proposition 2.2.12 *Let a be an element of finite order n in a group. For each nonzero integer s, as has order $n = g.c.d.(n, s)$.*

2.3 The Dihedral Groups

Definition 2.3.1 (Dihedral Group) *Group consists of n rotational symmetries and n reflection symmetries is a **dihedral group**, denoted by D_n.*

Proposition 2.3.1 $D_n =< r, a | r^n = e, a^2 = e, ra = ar^{-1} >$

Properties:

1. $jr_t = r_{-t}j$ and $j_t = r_{2t}j = jr_{-2t}$.
2. All products in D can be computed using these relations.
3. The symmetry group D of the disk consists of the rotations r_t for $t \in \mathbb{R}$ and the flips $j_t = r_{2t}j$. Writing $N = r_t : t \in \mathbb{R}$, we have $D = N \cup Nj$.
4. The subgroup N of D satisfies $aNa^{-1} = N$ for all $a \in D$.

2.4 Homomorphisms and Isomorphisms

Definition 2.4.1 (Homomorphism) *A map between groups $\varphi : G \to H$ is called a* ***homomorphism*** *if it preserves group multiplication, $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$. And An endomorphism of G is a homomorphism $\varphi : G \to G$.*

Proposition 2.4.1 *If $\varphi : G \to H$ and $\psi : H \to K$ are both group hom, then $\varphi \circ \psi : H \to K$ is a group hom.*

Proposition 2.4.2 *If $\varphi : G \to H$ be a homomorphism of groups.*

- $\varphi(e_G) = e_H$
- $\forall g \in G, \varphi(g^{-1}) = (\varphi(g))^{-1}$

Proposition 2.4.3 *Let $\varphi : G \to H$ be a homomorphism of groups.*

1. *For each subgroup $A \subseteq G$, $\varphi(A) \subseteq H$. (Image of A)*
2. *For each subgroup $B \subseteq G$,*
$$\varphi^{-1}(B) = g \in G : \varphi(g) \in B$$
is a subgroup of G. (Inverse image of B)

2.4.1 The Kernel of a Homomorphism

Definition 2.4.2 (Normal) *A subgroup N of a group G is said to be* ***normal*** *if $\forall g \in G$, $gNg^{-1} = N$. Here gNg^{-1} means $gng^{-1} : n \in N$.*[9][10]

Corollary 2.4.1
$$A_n \trianglelefteq S_n$$

Proposition 2.4.4 *If a subgroup N of a group G is its* ***normal subgroup****, then $\forall g \in G$, $gN = Ng$.*

Proposition 2.4.5 *Any subgroup of Abelian group is normal.*

Definition 2.4.3 (Kernel) *Let $\varphi : G \to H$ be a homomorphism of groups. The* ***kernel*** *of the homomorphism φ, denoted $ker(\varphi)$, is $\varphi^{-}1(e_H) = \{g \in G : \varphi(g) = e_H\}$.*[11]

[9] gng^{-1} is called conjugate if n by g
[10] Denote as $N \trianglelefteq G$
[11] e_H is the identity of group H.

e.g.1 $\varphi : \mathbb{Z} \to \mathbb{Z}_2$,

$$\ker(\varphi) = \{a \in \mathbb{Z} | [a] = [0]\}$$

e.g.2 $\det : GL(\alpha, \mathbb{R}) \to \mathbb{R}^*$

$$\ker(\det) = \mathrm{SL}(\alpha, \mathbb{R})$$

Proposition 2.4.6 *A homomorphism $\varphi : G \to H$ is injective if and only if $ker(\varphi) = e_G$.*

Proposition 2.4.7 *Let $\varphi : G \to H$ be a homomorphism of groups. Then $ker(\varphi)$ is a normal subgroup of G.*

2.4.2 Parity of Permutations

Definition 2.4.4 (Sign, Parity) *The homomorphism ϵ is called the **sign** (or **parity**) homomorphism. A permutation π is said to be even if $\epsilon(\pi) = 1$, that is, if π is in the kernel of the sign homomorphism. Otherwise, π is said to be odd. The subgroup of even permutations (that is, the kernel of ϵ) is generally denoted A_n. This subgroup is also referred to as the alternating group.*[12]

Proposition 2.4.8 *A permutation π is even if and only if π can be written as a product of an even number of 2-cycles.*

Corollary 2.4.2 *The set of odd permutations in S_n is $(12)A_n$, where A_n denotes the subgroup of even permutations.*

Corollary 2.4.3 *A k-cycle is even if k is odd and odd if k is even.*

2.5 Cosets and Lagranges Theorem

Definition 2.5.1 (Coset) *Let H be subgroup of a group G. A subset of the form gH, where $g \in G$, is called a left coset of H in G. A subset of the form Hg, where $g \in G$,is called a right coset of H in G.*

[12] $(a_1 a_2 \cdots a_{l-1} a_l) = \prod_{i=0}^{l-2} (a_1 a_{l-i})$

2.5.1 Properties of Cosets

Proposition 2.5.1 *Let H be a subgroup of a group G, and let a and b be elements of G. The following conditions are equivalent:*

1. $a \in bH$.
2. $b \in aH$
3. $aH = bH$.
4. $b^{-1}a \in H$.
5. $a^{-1}b \in H$.

Proposition 2.5.2 *Let H be a subgroup of a group G.*

1. *Let a and b be elements of G. Either $aH = bH$ or $aH \cap bH = \emptyset$.*
2. *Each left coset aH is nonempty and the union of left cosets is G.*
3. *All cosets have the same size.*[13]

Theorem 2.5.1 (Lagrange's Theorem) *Let G be a finite group and H a subgroup. Then $|H|$ divides $|G|$ and $\frac{|G|}{|H|}$ is the number of left cosets of H in G.*

Definition 2.5.2 (Index) *For a subgroup H of a group G, the index of H in G is the number of left cosets of H in G. The index is denoted $[G : H]$.*

Corollary 2.5.1 *Let p be a prime number and suppose G is a group of order p. Then:*

1. *G has no subgroups other than G and e.*
2. *G is cyclic, and in fact, for any nonidentity element $a \in G$, $G = \langle a \rangle$.*
3. *Every homomorphism from G into another group is either trivial (i.e., every element of G is sent to the identity) or injective.*

Corollary 2.5.2 *Let G be any finite group, and let a 2 G. Then the order $o(a)$ divides the order of G.*

[13]Coset is a partition of G

Proposition 2.5.3 *Suppose $K \subseteq H \subseteq G$ are subgroups, then*

$$[G : K] = [G : H][H : K].$$

Definition 2.5.3 (Center) *For any group G, the **center** $Z(G)$ of G is the set of elements that commute with all elements of G,*

$$Z(G) = \{a \in G : ag = ga, \forall g \in G\}$$

2.6 Equivalence Relations and Set Partitions

Definition 2.6.1 (Equivalence) *An equivalence relation $\sim$ on a set X is a binary relation with the properties:*

1. *Reflexivity: For each $x \in X, x \sim x$.*
2. *Symmetry: For $x, y \in X, x \sim y \Leftrightarrow y \sim x$.*
3. *Transitivity: For $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.*

Definition 2.6.2 (Partition) *A **partition** of a set X is a collection of mutually disjoint nonempty subsets whose union is X.*

Definition 2.6.3 (Equivalence class) *If $\sim$ is an equivalence relation on X, then for each $x \in X$, the **equivalence class** of x os the set*

$$[x] = \{y \in X : x \sim y\}$$

Proposition 2.6.1 *Let $\sim$ be an equivalence relation on X. For $x, y \in X$, $x \sim y$ if, and only if $[x] = [y]$.*

Corollary 2.6.1 *Let $\sim$ be an equivalence relation on X. Either $[x] \cap [y] = \emptyset$ or $[x] = [y]$.*

Proposition 2.6.2 *Let X be any set. There is a one to one correspondence between equivalence relations on X and set partitions of X.*

2.6.1 Equivalence Relations and Surjective Maps

Proposition 2.6.3 *Let $\sim$ be an equivalence relation on X. Then there exists a set Y and a surjective map $\pi : X \to Y$ such that $\sim$ is equal to the equivalence relation $\sim_\pi$.*

Definition 2.6.4 (Similar) *Two surjective maps $f : X \to Y$ and $f' : X \to Y'$ are similar if there exists a bijection $s : Y \to Y'$ such that $f' = s \circ f$.*

$$\begin{tikzcd}
X \arrow[r, "f'"] \arrow[d, "f"'] & Y' \\
Y \arrow[ur, "\cong"', "s"] &
\end{tikzcd}$$

Figure 1: Similar two surjective maps

Proposition 2.6.4 *Two surjective maps $f : X \to Y$ and $f' : X \to Y'$ determine the same equivalence relation X if and only if f and f' are similar.*

Definition 2.6.5 (Canonical projection) *The set of left cosets of H in G is denoted G/H . The surjective map $\pi : G \to G/H$ defined by $\pi(a) = aH$ is called the* ***canonical projection*** *or* ***quotient map*** *of G onto G/H.*

Proposition 2.6.5 *The fibers of the canonical projection $\pi : G \to G/H$ are the left cosets of H in G. The equivalence relation $\sim_\pi$ on G determined by π is the equivalence relation $\sim_H$.*

2.6.2 Conjugacy

Definition 2.6.6 (Conjugate) *Let a and b be elements of a group G. We say that b is conjugate to a if there is a $g \in G$ such that $b = gag^{-1}$.*

Definition 2.6.7 (Conjugacy classes) *The equivalence classes for conjugacy are called conjugacy classes.*

2.7 Quotient Groups and Homomorphism Theorems

Theorem 2.7.1 *Let N be a normal subgroup of a group G. The set of cosets G/N has a unique product that makes $G=N$ a group and that makes the quotient map $\pi : G \to G/N$ a group homomorphism, $ker(\pi) = N$.*

Proposition 2.7.1 *Let $a, b, c \in G$ and $N \trianglelefteq G$, we have:*

- *Closure: $aNbN = abN$*
- *Associativity: $aN(bNcN) = aNbNcN$*
- *Identity: $aN(N) = (N)aN = aN$*
- *Inverse: $(a^{-1}N)(aN) = (aN)(a^{-1}N) = N$*

2.7.1 Homomorphism Theorems

Theorem 2.7.2 (Homomorphism theorem) *Let $\varphi : G \to \bar{G}$ be a surjective homomorphism with kernel N. Let $\pi : G \to G/N$ be the quotient homomorphism. There is a group isomorphism $\tilde{\varphi} : G/N \to \bar{G}$ satisfying $\tilde{\varphi} \circ \pi = \varphi$.*

$$G/Ker(\phi) \cong \phi(G)$$

Theorem 2.7.3 (Correspondence Theorem) *Let $\varphi : G \to \bar{G}$ be a homomorphism of G and $\bar{G}$, and let N denote the kernel of φ.*

1. *The map $\bar{B} \mapsto \varphi^{-1}(\bar{B})$ is a bijection between subgroups of $\bar{G}$ and subgroups of G containing N.*
2. *Under this bijection, normal subgroups of $\bar{G}$ correspond to normal subgroups of G.*

Proposition 2.7.2 (Third Isomorphism Theorem) *Let $\varphi : G \to \bar{G}$ be a surjective homomorphism with kernel N. Let $\bar{K}$ be a normal subgroup of $\bar{G}$ and let $K = \varphi^{-1}(\bar{K})$. Then $G = K \cong \bar{G} = \bar{K}$. Equivalently, $G/K \cong (G/N)(K/N)$.*

Theorem 2.7.4 (Factorization Theorem) *Let $\varphi : G \to \bar{G}$ be a surjective homomorphism of groups with kernel K. Let $N \subseteq K$ be a subgroup that is normal in G, and let $\pi : G \to G/N$ denote the quotient map. Then there is a surjective homomorphism $\tilde{\varphi} : G/N \to G$ such that $\tilde{\varphi} \circ \pi = \varphi$. The kernel of $\tilde{\varphi}$ is $K/N \subseteq G/N$.*

Corollary 2.7.1 *Let $N \subseteq K \subseteq G$ be subgroups with both N and K normal in G. Then $xN \mapsto xK$ defines a homomorphism of G/N onto G/K with kernel K/N.*

Theorem 2.7.5 (Second Isomorphism Theorem(Diamond)) *Let $\varphi : G \to \bar{G}$ be a surjective homomorphism with kernel N. Let A be a subgroup of G. Then*

1. $\varphi^{-1}(\varphi(A)) = AN = \{an : a \in A \text{ and } n \in N\}$,
2. *AN is a subgroup of G containing N.*
3. $AN/N \cong \varphi(A) \cong A/(A \cap N)$.

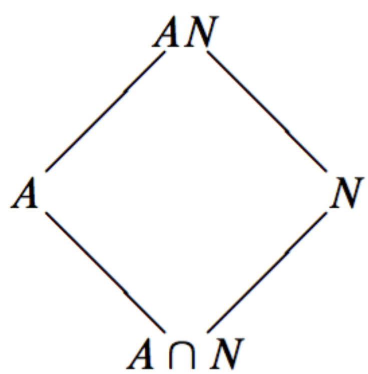

Figure 2: Diamond Isomorphism Theorem

Corollary 2.7.2

$$gcd(m,n)\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/lcm(m,n)\mathbb{Z}$$

Proposition 2.7.3 (Fourth Isomorphism Theorem(Lattice)) *Let $\varphi : G \to H$ be a surjective group homomorphism, $N \ker(\varphi)$ we have*

1. *There is a bijection*

$$\{\textit{subgroups of } G \textit{ containing } N\} \leftrightarrow \{\textit{subgroups of } H \cong G/N\}$$

2. *Normalness is preserved by this bijection*

Proposition 2.7.4 *If $H \subseteq G$ and $|G|/|H| = 2$, $H \trianglelefteq G$.*

3 Products of Groups

3.1 Direct Products

Definition 3.1.1 (Direct Product) *$A \times B$, with this group structure, is called the direct product of A and B.*

Proposition 3.1.1 *Properties:*

1. *Suppose M and N are normal subgroups of G, and $M \cap N = \{e\}$. Then for all $m \in M$ and $n \in N$, $mn = nm$.*
2. *$MN = \{mn : m \in M, n \in N\}$ is a subgroup and $(m, n) \mapsto mn$ is an isomorphism of $M \times N$ onto MN.*
3. *If $MN = G$, then $G \cong M \times N$.*

Definition 3.1.2 (Direct Product) *$A_1 \times A_2 \times \cdots \times A_n$, with the coordinate-by-coordinate multiplication, is called the **direct product** of $A_1, A_2, ..., A_n$.*

Proposition 3.1.2 *Suppose $N_1, N_2, ..., N_r$ are normal subgroups of a group G such that for all i,*

$$N_i \cap (N_1 ... N_{i-1} N_{i+1} ... N_r) = e.$$

Then $N_1 N_2 ... N_r$ is a subgroup of G and $(n_1, n_2, ..., n_r) \mapsto n_1 n_2 ... n_r$ is a subgroup of $P = N_1 \times N_2 \times \cdots \times N_n$ onto $N_1 N_2 ... N_r$. In particular, if $N_1 N_2 ... N_r = G$, then $G \cong N_1 \times N_2 \times \cdots \times N_n$.

Corollary 3.1.1 *Let $N_1, N_2, ..., N_r$ be normal subgroups of a group G such that $N_1 N_2 \cdots N_r = G$. Then G is the **internal direct product** of $N_1, N_2, ..., N_r$ if and only if whenever $x_i \in N_i$ for $1 \leq i \leq r$ and $x_1 x_2 \cdots x_r = e$, then $x_1 = x_2 = \cdots = x_r = e$.*

Definition 3.1.3 (Direct Sum) *The **direct sum** of several rings $R_1, R_2, ..., R_n$ is the Cartesian product $R_1 \times R_2 \times \cdots \times R_n$, endowed with the coordinate-by-coordinate operations*

$$(r_1, r_2, ..., r_n) + (r'_1, r'_2, ..., r'_s) = (r_1 + r'_1, r_2 + r'_2, ..., r_n + r'_n)$$

and

$$(r_1, r_2, ..., r_n)(r'_1, r'_2, ..., r'_s) = (r_1 r'_1, r_2 r'_2, ..., r_n r'_n).$$

The direct sum of $R_1, R_2, ..., R_n$ is denoted $R_1 \oplus R_2 \oplus ... \oplus R_n$.

Proposition 3.1.3 *If $m, n \in \mathbb{N}$, $g.c.d(m, n) = 1$, then*

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Proposition 3.1.4 (Chinese Remainder Theorem) *Let $n \geq 2$ and let $a_1, ..., a_n$ be pairwise relatively prime natural numbers. Write a $a = a_1 a_2 ... a_n$. Then*

$$[x]_a \mapsto ([x]_{a_1}, [x]_{a_2}, ..., [x]_{a_n})$$

defines a ring isomorphism

$$\mathbb{Z}_a \cong \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus ... \oplus \mathbb{Z}_{a_n}.$$

Proposition 3.1.5 (Chinese Remainder Theorem) *Let $n \geq 2$ and let $a_1, a_2, ..., a_n$ be pairwise relatively prime natural numbers. Write $a = a_1 a_2 \cdots a_n$. For any integers $x_1, x_2, ..., x_s$, there exists an integer x such that*

$$x \equiv x_i \mod a_i, for\ 1 \leq i \leq n.$$

Moreover, x is unique up to congruence mod a.

3.2 Semidirect Products

Definition 3.2.1 (Semidirect Product) *If we have groups N and A, and we have a homomorphism $\alpha : a \mapsto \alpha_a$ from A into the automorphism group Aut(N) of N, we can build from these data a new group $N \rtimes_\alpha A$, called the* ***semidirect product*** *of A and N . The semidirect product $N \rtimes_\alpha A$ has the following features: It contains (isomorphic copies of) A and N as subgroups, with N normal; the intersection of these subgroups is the identity, and the product of these subgroups is $N \rtimes_\alpha A$; and we have the commutation relation $an = \alpha_a(n)a$ for $a \in A$ and $n \in N$.*

Proposition 3.2.1 *Let N and A be groups, and $\alpha : A \to Aut(N)$ a homomorphism of A into the automorphism group of N. The Cartesian product $N \times A$ is a group under the multiplication $(n, a)(n', a') = (n\alpha_a(n'), aa')$. This group is denoted $N \rtimes_\alpha A$. This group is denoted $N \rtimes_\alpha A$. $\tilde{N} = \{(n, e) : n \in N\}$ and $\tilde{A} = \{(e, a) : a \in A\}$ are subgroups of $N \rtimes_\alpha A$, with $\tilde{N} \cong N$ and $\tilde{A} \cong A$, and $\tilde{N}$ is normal in $N \rtimes_\alpha A$. We have $(e, a)(n, e) = (\alpha_a(n), e) = (\alpha_a(n), a)$ for all $n \in N$ and $a \in A$.*

Corollary 3.2.1 *Suppose G is a group, N and A are subgroups with N normal, $G = NA = AN$, and $A \cap N = e$. Then there is a homomorphism $\alpha : A \to Aut(N)$ such that G is isomorphic to the semidirect product $N \rtimes_\alpha A$.*

3.3 Vector Spaces

Definition 3.3.1 (Vector Space) *A **vector space** V over a field K is an abelian group with a product $K \times V \to V$, $(\alpha, v) \mapsto \alpha v$ satisfying the following conditions:*

1. $\forall v \in V, 1v = v$.
2. $\forall \alpha, \beta \in K, v \in V, (\alpha\beta)v = \alpha(\beta v)$.
3. $\forall \alpha \in K, v, w \in V, \alpha(v + w) = \alpha v + \alpha w$.
4. $\forall \alpha, \beta \in K, v \in V, (\alpha + \beta)v = \alpha v + \beta v$.

Lemma 3.3.1 *Let V be a vector space over the field K, then $\forall \alpha \in K, v \in V$,*

1. $0v = \alpha 0 = 0$.
2. $\alpha(-v) = -(\alpha v) = (-\alpha)v$.
3. $(-1)v = -v$.
4. $If \alpha \neq 0$ *and* $v \neq 0$, *then* $\alpha v \neq 0$.

Definition 3.3.2 (Linear Transformation) *Let V and W be vector spaces over K. A map $T : V \to W$ is called a **linear transformation** or **linear map** if $\forall x, y \in V, T(x + y) = T(x) + T(y)$ and $\forall \alpha \in K and x \in V, T(\alpha x) = \alpha T(x)$. An endomorphism of a vector space V is a linear transformation $T : V \to V$.*

Definition 3.3.3 (Subspace) *A subspace of a vector space V is a (nonempty) subset that is a vector space with the operations inherited from V.*

Proposition 3.3.1 *For a nonempty subset of a vector space to be a subspace, it suffices that the subset be closed under addition and under scalar multiplication.*

Proposition 3.3.2 *Let $T : V \to W$ be a linear map between vector spaces. Then the range of T is a subspace of W and the kernel of T is a subspace of V.*

3.3.1 Quotients and homomorphism theorems

Theorem 3.3.1 (Homomorphism theorem for vector spaces) *If W is subspace of a vector space V over K, then V/W has the structure of a vector space, and the quotient map $\pi : v \mapsto v + W$ is a surjective linear map from V to V/W with kernel equal to W.*

Proposition 3.3.3 (Correspondence theorem for vector spaces) *Let $T : V \to \bar{V}$ be a surjective linear map, with kernel N. Then $\bar{M} \mapsto T^{-1}(\bar{M})$ is a bijection between subspaces of V and subspaces of $\bar{V}$ containing N.*

Proposition 3.3.4 *Let $T : V \to \bar{V}$ be a surjective linear transformation with kernel N. Let $\bar{M}$ be a subspace of V and let $M = T^{-1}(barM)$. Then $x + M \mapsto T(x) + \bar{M}$ defines a linear isomorphism of V/M to $\bar{V}/\bar{M}$. Equivalently,*

$$(V/N)(M/N) \cong V/M,$$

as vector spaces.

Proposition 3.3.5 (Factorization Theorem for Vector Spaces) *Let V and $\bar{V}$ be vector spaces over a field K, and let $T : V \to \bar{V}$ be a surjective linear map with kernel M. Let $N \subseteq M$ be a vector subspace and let $\pi : V \to V/N$ denote the quotient map. Then there is a surjective homomorphism $\tilde{T} : V/N \to \bar{V}$ such that $\tilde{T} \circ \pi = T$. The kernel is $M/N \subseteq V/N$.*

Proposition 3.3.6 (Diamond Isomorphism Theory for Vector Spaces) *Let A and N be subgroups of a vector space V. Let π denote the quotient map $\pi : V \to V/N$. Then $\pi^{-1}(\pi(A)) = A + N$ is a subspace of V containing both A and N. Furthermore, $(A + N)/N \cong \pi(A) \cong A/(A \cap N)$.*

3.4 Finitely Generated Abelian Groups

Definition 3.4.1 *S generates G if $\mathbb{Z}S = G$.*

Definition 3.4.2 *G is **finitely generated** if there is a finite set $S \subseteq G$ so that $\mathbb{Z}S = G$.*

Definition 3.4.3 *G is **finitely generated** if there is $S \subseteq G$ that is finite and $\mathbb{Z}S = G$.*

Definition 3.4.4 *If S generates G and is linearly independent, say S is a* ***basis*** *of G.*

Definition 3.4.5 *If G has a basis, then call G a free group.*

Proposition 3.4.1 *Let G be an abelian group and let $x_1, \cdots, x_n$ be distinct nonzero elements of G, the set $B = \{x_1, \cdots, x_n\}$ is a basis of G if and only if $G \equiv \mathbb{Z}^n$.*

Theorem 3.4.1 (Fundamental Theorem of Finitely Generated Abelian Groups) *Let G be a finitely generated abelian group.*

1. *G is a direct product of cyclic groups,*

$$G \cong \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_S} \times \mathbb{Z}^k$$

Definition 3.4.6 *Let $g \in G$, if there is $n \neq 0$ so that $ng = 0$, call g a torsion element.*

Proposition 3.4.2 *If $x + G_{tor} \in G/G_{tor}$, $G/G_{tor} = 0 + G_{tor}$*

4 Group Actions

Definition 4.0.1 *An action of a group G on a set X, a group action is a map $G \times X \to X$, denote as $gx_1 = x_2$*

- $(g_1 g_2) \cdot x = g_1(g_2 x)$
- $ex = x$
- $x(g_1 g_2) = x g_1 g_2$
- $xe = x$

Definition 4.0.2 *Let G act on $X, x \in X$. The orbit of x denoted $G \cdot x$ or $\mathcal{O}(x)$, is the set $\{g \cdot x | g \in G\}$.*

Definition 4.0.3 *$x \sim y \Leftrightarrow y = g \cdot x$ for some $g \in G$. $\sim$ is an equivalent relation.*

Eg 1. G acts on itself by left multiplication: $g \cdot a = ga$.

Definition 4.0.4 *If $G \curvearrowright X$ is one orbit, the action is called transitive.*

Eg 2. $G \curvearrowright G/H$ by left transilation $g \cdot (aH) = (ga)H$

Eg 3.1. $H \subseteq G$. H acts on G by right multiplication $g \cdot h = gh$ with orbits are left cosets.

Eg 3.2. H can also act on the left, with orbits to be the right cosets.

Eg 4. G acts on itself by conjugation. $g/cdota = gag^{-1}$ with orbits to be conjugacy classes.

Definition 4.0.5 (Stablizer) *Let G acts on X. The stablizer $Stab_G(X) = \{g \in G | gx = x\}$.*

Proposition 4.0.1 $Stab_G(X) \subseteq G$

Theorem 4.0.1 *Let G acts on X, $x \in X$. There is a natural bijection $\phi : G/Stab_G(x) \to G \cdot X$*

Theorem 4.0.2 (Orbit-Stablizer Theorem)

$$|\mathcal{O}(x)| = \frac{|G|}{|Stab(x)|}$$

Definition 4.0.6 (Normalizer) *Consider the action of a group G on its subgroups by conjugation. The stabilizer of a subgroup H is called the normalizer of H in G and denoted $N_G(H)$.*

Definition 4.0.7 (Centralizer) *Consider the action of a group G on its subgroups by conjugation. The stabilizer of an element $g \in G$ is called the centralizer of g in G and denoted $Cent_G(H)$.*

4.1 Group Actions and counting

Definition 4.1.1 *For $g \in G$, let $Fix(g) = \{x \in X : gx = xg\}$*

Proposition 4.1.1 *Let a finite group G act on a finite set X. Then the number of orbits of the action is*

$$\# \text{ of orbits} = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$$

4.2 Group Automorphisms

Definition 4.2.1 *If G is a group, then automorphism* $\mathrm{Aut}(G) = \{\varphi : G \to G | \varphi \text{ is isomorphism}\}$.

Definition 4.2.2 $\mathrm{Int}(G) = \{c_g | g \in G\}$ *for each $g \in G, c_g : G \to G$ and $c_g(x) = gxg^{-1}$.*

Proposition 4.2.1 Int(G) $\subseteq$ Aut(G)

Proposition 4.2.2 *If G is abelian, then* $\mathrm{Int}(G) = \{1\}$

Proposition 4.2.3 $\mathrm{Int}(G) \cong G/Z(G)$

Proposition 4.2.4 $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$

Proposition 4.2.5 $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$. *If p is a prime,* $\mathrm{Aut}(\mathbb{Z}_p) = \mathbb{Z}_{p-1}$

4.3 Sylow Theorem

Proposition 4.3.1 *Suppose p is a prime, $|G| = p^n$. Then $Z(G)$ contains nonidentity elements.*

Corollary 4.3.1 *Suppose p is prime and $|G| = p^2$, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

Definition 4.3.1 *$|G| = p^n$, then there is a normal subgroup $N \trianglelefteq G, \{e\} \subsetneq N \subsetneq G$, such that all subgroups of N are normal.*

Corollary 4.3.2 *$|G| = p^n$, p is prime, then there exists subgroups $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ such that $|G_k| = p^k$ and each $G_k \trianglelefteq G$.*

Theorem 4.3.1 (Cauchy's Theorem) *Suppose p is prime and $p||G|$, then G has an element of order p.*

Definition 4.3.2 *G is a finite group, p is prime. If p^n is the largest power of p dividing $|G|$ then a subgroup of size p^n is a* ***p-Sylow subgroup*** *of G.*

Theorem 4.3.2 (1st Sylow Theorem) *If $p^n||G|$ then G has a subgroup of size p^n.*

Theorem 4.3.3 (2nd Sylow Theorem) *Let P, Q be 2 p-Sylow subgroups. Then P and Q are conjugate subgroups. ($g \in G, gPg^{-1} = Q$)*

Corollary 4.3.3 *There is exactly 1 p-Sylow subgroup if and only if the subgroup is normal.*

Theorem 4.3.4 (3rd Sylow Theorem) *If p^n is the order of a p-Sylow subgroup of G, the number of p-Sylow subgroups of G satisfies*

- $\# \equiv 1 \mod p$
- $\#$ *divides* $\frac{|G|}{p^n}$

5 Ring

5.1 Basics

Definition 5.1.1 (Ring) *A* ***ring*** *with two operations $+, \cdot$, if*

1. *$R, +$ is an abelian group with identity:0 and inverses $-a$,*
2. *$R, \cdot$ is closed and associative*
3. *$R, +, \cdot$ is distributive.*

5.2 Homomorphism and Ideal

Definition 5.2.1 (Ring homomorphism) *A* ***ring homomorphism*** *$\varphi : R \to S$ is a map which preserves addition and multiplication.*

Let $a, b \in R$, we have:

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\varphi(b)$

*φ is an **isomorphism** if it is also bijection.*

Definition 5.2.2 *An element of a ring with multiplicative inverse is called a **unit**.*

Definition 5.2.3 *A left(right) **ideal** of a ring R, is a subset $I \subseteq R$ that*

1. $I \subseteq R$
2. *If $r \in R$, $a \in I$, then $ra \in I (ar \in I)$*

[14]

Proposition 5.2.1 *If $\varphi : R \to S$ is a ring homomorphism, then $\operatorname{Ker}(\varphi)$ is a (left and right) ideal of R.*

Proposition 5.2.2 *If an ideal contains a unit, then it contains the whole ring.*

Proposition 5.2.3 *If a ring is a field, then its ideal is either $\{0\}$ or the whole ring.*

Proposition 5.2.4

- *If $\{I_\alpha\}$ is ideals of R, then $\bigcap I_\alpha$ is an ideal.*
- *If $I_1 \subseteq I_2 \subseteq \cdots$ are ideals of R, then $\bigcup I_i$ is an ideal.*

5.2.1 Ideals generated by sets

Definition 5.2.4 *Let $S \subseteq R$ and $S \neq \emptyset$, then the **ideal generated by S** (S), the smallest ideal of R containing S.*

*If $S = \{a\}$, $(S) = (a)$ is called a **Principal ideal**.*

[14]Check if $I \subseteq R$ is an ideal:

1. $I \neq \emptyset$
2. If $a, b \in I$, $ar - b \in I$

5.3 Quotient Ring

Proposition 5.3.1 *Let I is an ideal of R, $R/I = \{r + I | r \in R\}$ is a ring.*

Definition 5.3.1 *Say a is a zero-divisor, if $\exists b$ that $ab = 0$.*

5.3.1 Four Isomorphism Theorem for Ring

Theorem 5.3.1 (First) *If $\varphi : R \to S$ surjective ring hom with kernel I, then $R/I \cong S$.*

Ex. $ev_0 : \mathbb{Z}[x] \to \mathbb{Z} \Rightarrow \mathbb{Z}[x]/(x) = \mathbb{Z}$.

Theorem 5.3.2 (Second) *If I is an ideal of R and A is a subring, then $(A + I)/I \cong A/A \cap I$.*

Theorem 5.3.3 (Third) *If $J \subseteq I$ are ideals of R, then $(R/J)/(I/J) \cong R/I$.*

Theorem 5.3.4 (Fourth) *Let $I \subseteq R$ be an ideal, then there is one-to-one correspondence $\{ideals\ of\ R/I\} \leftrightarrow \{ideals\ of\ R\ containing\ I\}$*

Definition 5.3.2 *An ideal M of R is* ***maximal*** *if whenever an ideal $M \subseteq I \subseteq R$ then $I = M$ or $I = R$.*

Ex. $2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

Proposition 5.3.2 *Let R be commutative with multiplicative identity 1. Then M is a max ideal $\Leftrightarrow R/M$ is a field.*