Algebra I

Ikhan Choi

April 26, 2025

Contents

Part I

Groups

Chapter 1

Natural numbers

1.1 Peano arithmetic

1.2

1.1 (Von Neumann construction).

algebraic and order structures

1.3 Integers and rational numbers

1.4 Divisibility

Chapter 2

Groups

2.1 Groups

2.1 (Groups). A *group* is a set G equipped with a binary operation $\cdot : G \times G \to G$ and a constant $e \in G$ satisfying

(i) for all $g, h, k \in G$ we have $(gh)k = g(hk)$, (associativity)

(ii) for all $g \in G$ we have $ge = eg = g$, (identity)

(iii) for all $g \in G$ there is $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$. (inverses)

A group G is called *commutative* or *abelian* if it satisfies

(iv) for all $g, h \in G$ we have $gh = hg$. (commutativity)

The equipped binary operation on a group is sometimes called the *group structure*, and the constant e is called the *identity*. We say a group is *additive* if we use the symbol $+$, 0, $-g$ for the group structure, the identity, and the inverse of an element g of a group, and *multiplicative* if we omit the symbol for the group structure and use the notation e or 1 for the identity. For an abelian group, we basically regard it additive.

(a) For $g_1, \cdots, g_n \in G$, the value of $g_1 \cdots g_n$ is well-defined independently of how the expression is bracketed.

(b) The identity of G and the inverse of each element $g \in G$ are uniquely determined by the group structure.

(c) $(g^{-1})^{-1}$ and $(gh)^{-1} = h^{-1}g^{-1}$ for all $g, h \in G$.

(d) The left and right ancellation laws.

2.2 (Group homomorphisms).

2.2 Subgroups

2.3 (Subgroups). Lagrange theorem, cosets and index
subgroup lattice

2.4 (Generators). group presentation orders of elements

2.5 (Direct sums).

2.3 Quotient groups

2.6 (Normal subgroups).

2.7 (Isomorphism theorems).

2.8 (Direct products).

2.4 Examples of groups

2.9 (Cyclic groups).

2.10 (Dihedral groups).

2.11 (Dicyclic groups). Quaternion group

2.12 (Symmetric and alternating groups). sign homomorphism generators, transpositions cycle type

2.13 (Linear groups). general, special

Chapter 3

Group actions

3.1 Actions and representations

Let G be a group and X be a set. A *left action* of G on X is a function $G \times X \to X : (g, x) \to gx$ such that $g(hx) = (gh)x$ and $ex = x$. A *left G-set* is a set X together with a left action of G on X. We may define right actions and right G-sets similarly.

effective, free, transitive actions. The orbit spaces of a left G-set X is a set $G\backslash$ of orbits. When we do not have to emphasize the G-space is left, that is we do not deal with both left and right actions simultaneously, we often write the orbit space just by X/G.

Let H be a subgroup of G. A left coset is an element of the orbit space of the right action $G \times H \to G$ of H on G given by the right multiplication. Here we can define a left multiplication action of G on G/H, which is transitive.

3.1 (Automorphism groups)**.**

3.2 Orbits and stabilizers

Invariants on orbit space.

3.2 (Orbit-stabilizer theorem)**.** The size of orbits. The number of orbits. The class equation.

3.3 (Transitive actions)**.** (a) Stabilizers are all isomorphic.

3.4 (Free actions)**.** no fixed point, trivial stabilizer for any point, every orbit has 1-1 correspondence to group

3.3 Action by left multiplication

3.4 Action by conjugation

3.5 (Centralizers and normalizers)**.**

3.6 (Conjugacy classes of elements)**.**

3.7 (Conjugacy classes of subgroups)**.**

H has index n : G can act on Sym(G/H) : left mul K normalizes H : K -> NG(H) -> NG(H)/H with ker = KnH K normalizes H : K -> NG(H) -> Aut(H) with ker = CG(H)

Exercises

Problems

1. Show that a group of order $2p$ for a prime p has exactly two isomorphic types.
2. Let G be a finite group of order n and p the smallest prime divisor of n. Show that a subgroup of G of index p is normal in G.
3. Show that a finite group G satisfying $\sum_{g \in G} \operatorname{ord}(g) \leq 2n$ is abelian.
4. Find all homomorphic images of A_4 up to isomorphism.
5. For a prime p, find the number of subgroups of $Z_{p^2} \times Z_{p^3}$ of order p^2.
6. Let G be a finite group. If $G/Z(G)$ is cylic, then G is abelian.
7. Let G be a finite group. If the cube map $x \mapsto x^3$ is a surjective endomorhpism, then G is abelian.
8. Show that if $|G| = p^2$ for a prime p, then a group G is abelian.
9. Show that the order of a group with only on automorphism is at most two.

Part II

Rings

Chapter 4

Rings

4.1 Rings

4.1 (Rings). A *ring* is an additive abelian group R equipped with a binary operation $\cdot : R \times R \to R$ satisfying

(i) for all $r, s, t \in R$ we have $(rs)t = r \cdot (s \cdot t)$, (associativity)

and the compatibility condition

(v) for all $r, s, t \in R$ we have $r(s + t) = rs + rt$ and $(r + s)t = rt + st$. (distributivity)

A *unital ring* is a ring R equipped with a constant $1 \in R \setminus \{0\}$ called the *unity* such that

(ii) for all $r \in R$ we have $r1 = 1r = r$, (identity)

and a *division ring* is a unital ring R such that

(iii) for all $r \in R \setminus \{0\}$ there is $r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1$, (inverses)

A ring R is called *commutative* if

(iv) for all $r, s \in R$ we have $rs = sr$, (commutativity)

and a *field* is a commutative division ring.

4.2 Ideals

4.2 (Ideals). Let R be a commutative unital ring.

4.3 (Quotient rings).

4.4 (Isomorphism theorems).

4.3 Maximal and prime ideals

fields and integral domains existence by Zorn's lemma

4.4 Operations on ideals

Exercises

size of units, the number of ideals

Chapter 5

Integral domains

5.1 Unique factorization domains

5.2 Principal ideal domains

5.1. In a principal ideal domain R,

(a) every irreducible element is prime, (Euclid's lemma)

(b) every two elements has greatest common divisor, (existence of gcd)

(c) the gcd is given as a R-linear combination, (Bźout's identity)

(d) factorization into primes is unique up to permutation, (UFD)

(e) every prime ideal is maximal. (Krull dimension 1)

5.3 Noetherian rings

Exercises

5.2 (Primitive roots)**.** We find all n such that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

Problems

1. Show that a finite integral domain is a field.
2. Show that every ring of order p^2 for a prime p is commutative.
3. Show that a semiring with multiplicative identity and cancellative addtion has commutative addition.
4. Show that the complement of a saturated monoid in a commutative ring is a union of prime ideals.

Chapter 6

Polynomial rings

6.1 Irreducible polynomials

relation to maximal ideals Irreducibles over several fields

6.1 (Gauss lemma).

6.2 (Eisenstein criterion).

6.2 Polynomial rings over a field

6.3 (Euclidean algorithm for polynoimals).

6.4 (Polynomial rings over UFD).

6.5 (Hilbert's basis theorem).

maximal ideals and monic irreducibles