Algebra

Ikhan Choi

May 23, 2024

Contents

Part I

Groups

Chapter 1

Natural numbers

1.1 Algebraic structures

1.1 (Binary operations)**.** Let A be a set. Recall that a *binary operation* on A is just a function $\cdot : A \times A \to A$. A binary operation $\cdot$ on A is called to satisfy

(i) the *associativity* if

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \qquad a, b, c \in A,$$

(ii) the *existence of identity* if there exists $e \in A$ such that

$$a \cdot e = e \cdot a = a, \qquad a \in A,$$

(iii) the *existence of inverses* if satisfies (ii) and for every $a \in A$ there is $x \in A$ such that

$$a \cdot x = x \cdot a = e,$$

(iv) the *commutativity* if

$$a \cdot b = b \cdot a, \qquad a, b \in A.$$

A *semi-group*, *monoid*, *group*, and *abelian group* is a set A equipped with a binary operation $\cdot : A \times A \to A$ satisfying the first one, two, three, and four of the above conditions, respectively. An accompanying binary operation is called a *group structure* if it defines a group, that is, it satisfies (i), (ii), and (iii).

(a)

1.2 (Properties of groups)**.** We say a group is *additive* if we use the symbol $+$ for the group structure, and *multiplicative* if we use the symbol $\cdot$ or omit the symbol for the group structure.

(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 inverses of each element $g \in G$ are unique.

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

(d) The left and right ancellation laws.

Cayley table

1.3 (Homomorphisms)**.** image and kernel and preimage how to construct

1.2 Peano axioms

1.3 Integers and rational numbers

1.4 Divisibility

Chapter 2

Groups

2.1 Subgroups

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

2.2 (Generators). group presentation orders of elements

2.2 Quotient groups

2.3 (Normal subgroups).

2.4 (Isomorphism theorems).

2.5 (Direct sum and direct product).

2.3 Examples of groups

2.6 (Cyclic groups).

2.7 (Dihedral groups).

2.8 (Dicyclic groups). Quaternion group

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

2.10 (Linear groups). general, special

Chapter 3

Group actions

3.1 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

Ideals

4.1 Definitions of rings and ideals

4.1 (Definition of rings)**.** A *ring* is an abelian group $R = (R, +)$ together with a *multiplication* $\times : R \times R \to R$ which satisfies the associativity law, such that the following compatibility condition holds: the *distributive laws*:

$$r \times (s+t) = (r \times s) + (r \times t), \qquad (s+t) \times r = (s \times r) + (t \times r), \qquad r, s, t \in R.$$

We usually omit the cross symbol to write $r \times s$ as rs.

We are usually concerned with commutative unital rings, that is, rings whose multiplication is commutative and admits a multiplicative identity. The additive and multiplicative identities are usually denoted by 0 and 1 and called the *zero* and the *unity* respectively.

4.2 (Definition of ideals)**.** Let R be a commutative unital ring.

4.3 (Quotient rings)**.**

4.4 (Isomorphism theorems)**.**

4.2 Maximal and prime ideals

fields and integral domains existence by Zorn's lemma

4.3 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 PID 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

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.

Exercises

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

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

Part III

Modules

Chapter 7

Modules

7.1 Modules

7.1 (Definition of modules)**.** Let A be a ring, which is possibly neither commutative nor unital. A *left A-module* is an abelian group $(M,+)$ together with a ring homomorphism $\alpha : A \to \mathrm{End}_{\mathbb{Z}}(M)$, where $\mathrm{End}_{\mathbb{Z}}(M)$ denotes the group endomorphisms on M. We assume conventionally that α is unital if A is unital. The homomorphism α is called the *left action* and the operation $\cdot : A \times M \to M$ defined by $a \cdot m := \alpha(a)(m)$ is called the *scalar multiplication*. We usually omit the dot to denote it by am.

(a)

submodules quotient modules isomorphism theorems

7.2 Free modules

generators, cyclic direct sum free modules

7.3 Tensor products

7.2 (Tensor product of algebras)**.** Let A and

Chapter 8

Exact sequences

8.1

injective modules projective modules flat modules endomorphism algebra Tor and Ext

A left R-module P is projective if and only if the left exact functor $\mathrm{Hom}_R(P,-)$ is exact.

A left R-module I is injective if and only if the left exact contravariant functor $\mathrm{Hom}_R(-,I)$ is exact.

projective

- direct sum of projectives is projective
  (lem) if free, then projective
- PID: projective iff free (note sub of free is free in PID)
- projective iff direct summand of a free
- every module is a quotient of a free module

injective

- direct product of injectives is injective
  (lem) M injective iff $\mathrm{Hom}_R(R,M) \to \mathrm{Hom}_R(I,M)$ surj
- PID: injective iff divisible $(\cdots a : M \to M$ surj)
  (lem) $\mathrm{Hom}_Z(R,M)$ is injective if M is injective $\mathbb{Z}$-module
- every module is embedded in injective

flat

- PID: flat iff $(\cdot a : M \to M$ inj)
- M flat iff $\mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ is injective
- M flat iff $I \otimes M \to R \otimes M$ inj
- if projective, then flat

continuity of functors

8.1 (Tor functor)**.** Let R be a ring and M be a left R-module. We define the *Tor functor* as the left derived functor of the right exact functor $- \otimes_R M : \mathrm{Mod}\text{-}R \to \mathrm{Ab}$

$$\mathrm{Tor}_n^R(N,M) := H_n(P_\bullet \otimes_R M),$$

where $P_\bullet$ is a projective resolution of a right R-module N.

(a) In fact, the Tor functor may be defined by the left derived functor of the right exact functor $M \otimes_R - : R\text{-}\mathrm{Mod} \to \mathrm{Ab}$ for a right R-module M.

(b) In fact, only for Tor functors, we may only assume $P_\bullet$ is a flat resolution. (Flat resolution lemma)

8.2 (Ext functor)**.** Let R be a ring and M be a left R-module. We define the *Ext functor* as the right derived functor of left exact functor $\mathrm{Hom}_R(M,-)$

$$\mathrm{Ext}^n_R(M,N) := H^n(M,I^\bullet),$$

where $I^\bullet$ is an injective resolution of N.

(a) In fact, the Ext functor may be defined by the right derived functor of the left exact contravariant functor $\mathrm{Hom}(-,M)$.

long exact seuqence

8.3 (Universal coefficient theorem)**.** Let R be a ring. Let $C_\bullet$ be a chain complex of flat right R-modules and M be a left R-module.

Proof. We first prove the Künneth formula. Note that modules in $Z_\bullet$ and $B_\bullet$ are also flat. We start from that we have a short exact sequence of chain complexes

$$0 \to Z_\bullet \to C_\bullet \to B_{\bullet-1} \to 0.$$

We have a short exact sequence of chain complexes

$$\mathrm{Tor}_1^R(B_{\bullet-1},M) \to Z_\bullet \otimes_R M \to C_\bullet \otimes_R M \to B_{\bullet-1} \otimes_R M \to 0.$$

Since modules in $B_{\bullet-1}$ are flat so that $\mathrm{Tor}_1^R(B_{\bullet-1},M) = 0$, we have a short exact sequence of chain complexes

$$0 \to Z_\bullet \otimes_R M \to C_\bullet \otimes_R M \to B_{\bullet-1} \otimes_R M \to 0.$$

Since $H_n(C_{\bullet-1}) = H_{n-1}(C_\bullet)$ for any chain complex C, we have a long exact sequence

$$H_n(B_\bullet \otimes_R M) \to H_n(Z_\bullet \otimes_R M) \to H_n(C_\bullet \otimes_R M) \to H_{n-1}(B_\bullet \otimes_R M) \to H_{n-1}(Z_\bullet \otimes_R M).$$

Since every morphism in $B_\bullet$ and $Z_\bullet$ is zero, we have an exact sequence

$$B_n \otimes_R M \xrightarrow{f_n} Z_n \otimes_R M \to H_n(C_\bullet \otimes_R M) \to B_{n-1} \otimes_R M \xrightarrow{f_{n-1}} Z_{n-1} \otimes_R M.$$

Therefore, we have a short exact sequence

$$0 \to \operatorname{coker} f_n \to H_n(C_\bullet \otimes_R M) \to \ker f_{n-1} \to 0.$$

Since

$$0 \to B_n \to Z_n \to H_n(C_\bullet) \to 0$$

is a flat resolution of $H_n(C_\bullet)$, by the flat resolution lemma, we have a long exact sequence

$$\mathrm{Tor}_1^R(Z_n,M) \to \mathrm{Tor}_1^R(H_n(C_\bullet),M) \to B_n \otimes_R M \xrightarrow{f_n} Z_n \otimes_R M \to H_n(C_\bullet) \otimes_R M \to 0.$$

Since Z_n is flat so that $\mathrm{Tor}_1^R(Z_n,M) = 0$, we have

$$\operatorname{coker} f_n = H_n(C_\bullet) \otimes_R M, \quad \ker f_n = \mathrm{Tor}_1^R(H_n(C_\bullet),M).$$

Therefore, we have an exact sequence

$$0 \to H_n(C_\bullet) \otimes_R M \to H_n(C_\bullet \otimes_R M) \to \mathrm{Tor}_1^R(H_{n-1}(C_\bullet),M) \to 0.$$

Universal coefficient theorem states that if R is a PID, then the Künneth formula splits non-canonically. $\square$

$$\begin{array}{ccccccc}
K & \longrightarrow & A & \longrightarrow & B & \longrightarrow & 0 \\
 & & \twoheaddownarrow & & \downarrow & & \\
K' & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & 0
\end{array}$$

(a) If $A \to A'$ is monic, then $K \to K'$ is monic.

(b) If $B \to B'$ is monic, then $K \to K'$ is epic.

Chapter 9

Linear algebra

9.1 Modules over principal ideal domains

9.1 (Torsion modules)**.** Let R be a commutative unital ring. An R-module M is called a *torsion* module if for every element $m \in M$ there is $r \in R$ such that $rm = 0$.

9.2 (Cyclic modules)**.** Let R be a commutative unital ring. An R-module M is said to be *cyclic* if it is generated by one element.

(a) A cyclic R-module is isomorphic to a quotient of R.

(b) A cyclic R-module is torsion-free if and only if it is isomorphic to R.

9.3. Let R be a principal ideal domain. A submodule of a finite-rank free module is also a finite-rank free module. Two ways to take the basis imply the existence of invariant factors and elementary divisors.

9.4 (Structure theorem of finitely generated modules)**.** Let R be a principal ideal domain and M be a finitely generated R-module. If we know the ideal structure of a PID R, then we can classify all finitely generated modules over R.

(a) M is isomorphic to the direct sum of cyclic R-modules.

(b) existence and uniqueness: invariant factors

(c) existence and uniqueness: elementary divisors

$$(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/12\mathbb{Z}) \oplus (\mathbb{Z}/48\mathbb{Z}) \iff \begin{array}{c|cccc} & 2 & 4 & 12 & 48 \\ \hline 2 & 2 & 4 & 4 & 16 \\ 3 & 0 & 0 & 3 & 3 \end{array}$$

$$(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2^2\mathbb{Z})^2 \oplus (\mathbb{Z}/2^4\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})^2 \iff \begin{array}{c|cccc} p \setminus e & 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 2 & 0 & 1 \\ 3 & 2 & 0 & 0 & 0 \end{array}$$

9.2 Vector spaces

9.5 (Dual spaces)**.** Double dual

9.6 (Polarization identity)**.** (a) Let F be a field of characteristic not 2. If $\langle -, - \rangle$ is a symmetric bilinear form, then

$$\langle x, y \rangle = \frac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2).$$

(b) Let $F = \mathbb{C}$. If $\langle -,- \rangle$ is a sesquilinear form, then

$$\langle x, y \rangle = \frac{1}{4} \sum_{k=0}^{3} i^k \|x + i^k y\|^2.$$

(c) isometry check

9.7 (Cauchy-Schwarz inequality). (a) Let $F = \mathbb{R}$. If $\langle -,- \rangle$ is a positive semi-definite symmetric bilinear form, then

(b) Let $F = \mathbb{C}$. If $\langle -,- \rangle$ is a positive semi-definite Hermitian form, then

9.8 (Dual space identification). Let $\langle -,- \rangle$ be a non-degenerate bilinear form

9.9 (Adjoint linear transforms).

9.3 Normal forms

9.10 (Rational canonical form). Let F be a field. Invariant factor form

(a) There is a one-to-one correspondence between the similarity classes of square matrices over F and the isomorphism classes of finitely generated $F[x]$-modules.

(b) Every finitely generated $F[x]$-module is a direct sum of cylic torsion $F[x]$-modules, i.e. no free submodules.

(c) Every cyclic torsion $F[x]$-module $V \cong R/(a)$ can be represented by the associated companion matrix C_a, constructed by the coefficients of a.

For $A \in M_n(F)$, the minimal polynomial $m_A(x)$ can be defined by the generator of the annihilator of the associated $F[x]$-module (V, A). The minimal polynomial is the largest invariant factor of (V, A). For each invariant factor a_i, we can construct a companion matrix with its coefficients.

9.11 (Jordan normal form).

9.12 (Commuting matrices).

spectral theorems

Exercises

9.13 (Conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_p)$). The conjugacy classes are classified by normal forms. There are four cases: for some a and b in $\mathbb{F}_p$,

(a) $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$: $\binom{p-1}{2}$ classes of size $\frac{|G|}{(p-1)^2} = p(p+1)$.

(b) $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$: $p - 1$ classes of size 1.

(c) $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$: $p - 1$ classes of size $\frac{|G|}{p(p-1)} = p^2 - 1$.

(d) otherwise, the eigenvalues are in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. In this case, the number of conjugacy classes is same as the number of monic irreducible qudratic polynomials over $\mathbb{F}_p$; $\frac{|\mathbb{F}_{p^2}| - |\mathbb{F}_p|}{2} = \frac{p(p-1)}{2}$ classes. Their size is $\frac{p(p-1)}{2}$.

9.14 (Conjugacy classes of $\mathrm{GL}_3(\mathbb{F}_p)$). There are eight types of invariant factors:

$$(x-a)(x-b)(x-c),\ (x-a)^2(x-b),\ (x-a)^3,\ (x^2+ax+b)(x-c),\ (x^3+ax^2+bx+c),$$

$$(x-a)\mid(x-a)(x-b),\ (x-a)\mid(x-a)^2,\ (x-a)\mid(x-a)\mid(x-a)$$

Show that a square matrix A over $\mathbb{F}_p$ satisfying $A^p=A$ is diagonalizable.

Part IV

Algebras

Chapter 10

Tensor algebras

10.1 Algebras

10.1 (Definition of algebras). Let R be a commutative unital ring. An (associative) *algebra* over R or *R-algebra* is a ring A together with a unital ring homomoprhism $\alpha : R \to Z(\widetilde{A}) \subset \mathrm{End}_{\mathbb{Z}}(A)$. Although there are some important examples of *non-associative* algebras in which the associativity of multiplication is dropped, we will assume that an R-algebra is associative if no mention.

(a) The set of matrices $M_n(R)$ over a ring R is a unital R-algebra.

(b) The set of quaternions $\mathbb{H}$ is an $\mathbb{R}$-algebra.

10.2 Graded and filtered algebras

10.3 Exterior algebras

10.2 (Determinants).

10.4 Symmetric algebras