# Algebraic Structures

Ikhan Choi

February 18, 2023

# Contents

# Part I

# Groups

# Chapter 1

# Groups

## 1.1 Definition of groups

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

(i) the *associativity* if for every $a, b, c \in A$ we have

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

(ii) the *existence of identity* if there exists $e \in A$ such that for every $a \in A$ we have

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

(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 for every $a, b \in A$ we have

$$a \cdot b = b \cdot a.$$

A *monoid*, *group*, and *abelian group* is an ordered pair $(A, \cdot)$ of a set $A$ and a binary operation $\cdot : A \times A \to A$ satisfying the first 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) $(\mathbb{N}, +)$ is not a monoid, and $(\mathbb{N}, \times)$ is a monoid.

(b) $(\mathbb{Z}, +)$ is a group, and $(\mathbb{Z}, \times)$ is a monoid.

(c) $(\mathbb{Q}, +)$ is a group, and $(\mathbb{Q} \setminus \{0\}, \times)$ is also a group.

(d) The set of all invertible $2 \times 2$ real matrices forms a group with multiplication, which is not abelian.

**1.2** (Properties of a group structure)**.** 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.

**1.3** (Group table)**.**

## 1.2 Homomorphisms

homomorphisms, image, kernel, preimage isomorphism

## 1.3 Subgroups

**1.4** (Subgroups).

**1.5** (Lagrange theorem). cosets, index

**1.6** (Subgroup lattice).

generators

## 1.4 Quotient groups

**1.7** (Normal subgroups).

**1.8** (Isomorphism theorems).

## Exercises

**1.9** (Direct sum and direct product).

**1.10** (Automorphism groups).

# Chapter 2

# Examples of groups

## 2.1 Cyclic groups

**2.1** (Orders).

cyclic groups

## 2.2 Dihedral and Dicyclic groups

**2.2** (Dihedral groups).

**2.3** (Dicyclic groups).

**2.4** (Quoternion group).

## 2.3 Symmetric and alternating groups

sign homomorphism generators, transpositions cycle type

## 2.4 Matrix groups

general, special

# Chapter 3

# Group actions

## 3.1 Representations

## 3.2 Orbits and stabilizers

Invariants on orbit space.

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

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

**3.3** (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

**3.4** (Centralizers and normalizers).

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

**3.6** (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 $\sum_{g\in G} \operatorname{ord}(g) \le 2n$ 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 additive abelian group $R$ together with a *multiplication* $\times : R \times R \to R$ which defines an *abelian monoid* structure, such that the following compatibility condition holds: the *distributive law*: for every $r, s, t \in R$, we have

$$r \times (s + t) = (r \times s) + (r \times t).$$

The additive and multiplicative identities are usually denoted by 0 and 1 and called the *zero* and the *unity* respectively.

We are only concerned with *commutative* rings with *unity* when mentioning rings, so we specified the multiplication to be an abelian monoid. In particular, rings for which the multiplication is not necessarily commutative or the multiplicative identity does not necessarily exist will be called as *non-commutative rings* or *non-unital rings*, respectively. The theory of such non-commutative or non-unital rings, however, is usually covered in the theory of *algebras*.

**4.2** (Definition of ideals)**.** Let $R$ be a 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 $R$ be a non-commutative ring. An (left) *R-module* is an additive abelian group $M$ together with a *scalar multiplication* $\cdot : R \times M \to M$ which defines an *left action* on $M$, i.e. for every $r, s \in R$ and $m \in M$, we have

$$r \cdot (s \cdot m) = (rs) \cdot m \quad \text{and} \quad 1 \cdot m = m,$$

such that the following compatibility condition holds: the *distributive laws* hold: for every $r, s \in R$ and $m, n \in M$, we have

$$r \cdot (m + n) = r \cdot m + r \cdot n \quad \text{and} \quad (r + s) \cdot m = r \cdot m + s \cdot m.$$

(a) If $R$ is commutative, then

submodules quotient modules isomorphism theorems

## 7.2 Algebras

**7.2** (Definition of algebras)**.** Let $R$ be a ring. An (associative) *R-algebra* is an $R$-module $A$ together with a *multiplication* $\times : A \times A \to A$ which is associative, such that the following compatibility conditions hold:

(i) the *distributive laws* hold: for every $a, b, c \in A$, we have

$$a \times (b + c) = a \times b + a \times c \quad \text{and} \quad (a + b) \times c = a \times c + b \times c,$$

(ii) the *compatibility with scalars*: for every $r, s \in R$ and $a, b \in A$, we have

$$(rs) \cdot (a \times b) = (r \cdot a) \times (s \cdot b).$$

If the multiplication is commutative or admits an identity, then we say the $R$-algebra is *commutative* or *unital* respectively. Although there are examples of *non-associative* algebras in which the multiplication is not associative, we will always mean *associative* $R$-algebras by $R$-algebras if any modifier is not attached.

(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.

(c) There is a one-to-one correspondence between rings and commutative unital $\mathbb{Z}$-algebras.

**7.3** (Algebras as non-commutative rings). The term algebra is commonly used when we have to consider either non-commutative or non-unital of rings. Let $R$ be a ring. An *R-algebra* also can be defined as a non-commutative and non-unital ring $(A, +, \times)$ together with a ring homomorphism $\eta : R \to Z(A)$, where

$$Z(A) := \{\, a \in A : ab = ba \text{ for all } b \in A \},$$

which is called the *center*. The homomorphism $\eta$ defines a scalar multiplication via

$$\cdot : R \times A \to A : (r, a) \mapsto \eta(r)a.$$

(a) A non-commutative and non-unital ring $R$ is a $Z(R)$-algebra.

(b) The "module-with-multiplication definition" is equivalent to the "ring-with-scalar-multiplication definition".

## 7.3 Free modules

generators, cyclic direct sum free modules

## 7.4 Tensor products

# Chapter 8

# Exact sequences

## 8.1

injective modules projective modules flat modules endomorphism algebra Tor and Ext

# Chapter 9

# Modules over principal ideal domains

## 9.1 Structure theorem of finitely generated modules

invariant factors and elementary divisors

**9.1** (Structure theorem of finitely generated modules)**.** Let $R$ be a principal ideal domain and let $M$ be a finitely generated module.

If we know the ideal structure of a PID $R$, then we can classify all finitely generated modules over $R$.

**9.2** (Fundamental theorem of abelian groups)**.**

**9.3** (Cyclic decomposition)**.**

# Part IV

# Vector spaces

# Chapter 10

# Duality

## 10.1 Linear functionals

**10.1** (Double dual space).

## 10.2 Bilinear and sesquilinear forms

**10.2** (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

**10.3** (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

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

## 10.3 Adjoint

**10.5** (Adjoint linear transforms).

# Chapter 11

# Normal forms

## 11.1 Rational canonical form

**11.1** (Finitely generated $F[x]$-modules)**.** Let $F$ be a field. Then, the map

$$V \mapsto (V, x)$$

defines a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{finitely generated} \\ F[x]\text{-modules} \end{array} \right\} \to \left\{ (V,T)\ ;\ \begin{array}{c} V \text{ is a finite-dimensional vector spaces over } F, \\ T : V \to V \text{ is a linear transform} \end{array} \right\}.$$

**11.2** (Cyclic subspaces)**.**

## 11.2 Jordan normal form

## 11.3 Conjugation action

**11.3** (Similar matrices)**.**

**11.4** (Commuting matrices)**.**

## 11.4 Spectral theorems

## Exercises

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

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

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

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

(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 $\frac{p(p-1)}{2}$.

# Chapter 12

# Tensor algebras

## 12.1 Graded and filtered algebras

## 12.2 Exterior algebras

**12.1** (Determinants).

## 12.3 Symmetric algebras