Algebraic Structures

Ikhan Choi

October 22, 2022

Contents

Part I

Groups

Chapter 1

Subgroups

1.1 Definition of groups

1.1 (Definition of groups)**.** Let A be a set. A binary operation $\cdot : A \times A \to A$ 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 a set G together with a binary operation $\cdot : G \times G \to G$ 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). 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.

subgroups homomorphisms, image, kernel, inverse images normality, quotient, coset counting direct sum, direct product generators, subgroup lattice

Exercises

Problems

1. Let G be a finite group. If the cube map $x \mapsto x^3$ is a surjective endomorhpism, then G is abelian.
2. Show that if $|G| = p^2$ for a prime p, then a group G is abelian.
3. Show that the order of a group with only on automorphism is at most two.

Chapter 2

Group actions

2.1 Orbits and stabilizers

Invariants on orbit space. The size and number of orbits.

2.1 (Transitive actions)**.** stabilizer of an action is well defined

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

2.2 Action by conjugation

2.3 Action by left multiplication

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)

Problems

1. Let G be a finite group. If $G/Z(G)$ is cylic, then G is abelian.

Chapter 3

Symmetry groups

Information about: element counting by order, element counting by conjugacy class, subgroups by order (existence) subgroups by conjugacy class.

3.1 Cyclic groups

3.2 Dihedral groups

3.3 Symmetric groups

alternating groups

3.4 Automorphism groups

Maybe too hard

cyclic groups. abelian groups? symmetric groups?

Exercises

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

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.

Part II

Rings

Chapter 4

Ideals

4.1 Definitions of rings and ideals

4.1 (Definition of rings)**.** A *ring* is a set R together with

(i) an *addition* $+ : R \times R \to R$ which defines an abelian group structure,

(ii) a *multiplication* $\times : R \times R \to R$ which defines an *abelian monoid* structure,

such that the following compatibility condition holds:

(iii) 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.

Exercises

size of units, the number of ideals

Chapter 5

Integral domains

5.1 Principal ideal domains

5.2 Unique factorization domains

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.

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).

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 a set M together with

(i) an *addition* $+ : M \times M \to M$ which defines an abelian group structure on M,

(ii) a *scalar multiplication* $\cdot : R \times M \to M$ which defines an *left action* on M: 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:

(iii) 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 a set A together with

(i) an *addition* $+ : A \times A \to A$ which defines an abelian group structure,

(ii) a *scalar multiplication* $\cdot : R \times A \to A$ which defines a left action,

(iii) a *multiplication* $\times : A \times A \to A$ which is associative,

such that the following compatibility conditions hold:

(iv) $(A, +, \cdot)$ is an R-module,

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

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

(vi) 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 η 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

10.1 Dual spaces

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 Conjugacy classes in matrix groups

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

11.4 Spectral theorems

Exercises

Chapter 12

Tensor algebras

Exterior algebras Symmetric algebras