Abstract Algebra

Hechen Hu

November 26, 2017

Contents

1

Groups

1.1 Semigroups, Monoids and Groups

Definition. A *semigroup* is a nonempty set G together with a binary operation on G which is associative.

Definition. A *monoid* is a semigroup G which contains a (two-sided) identity element $e \in G$ such that $ae = ea = a$ for all $a \in G$.

Definition. A *group* is a monoid G such that there exists a (two-sided) inverse element and the operation between the inverse element and the original element yields the identity element regardless of order of operation.

Definition. A semigroup G is said to be *abelian* or *commutative* if its binary operation is commutative.

Definition. The *order* of a group G is the cardinal number $|G|$. G is said to be finite(resp. infinite) if $|G|$ is finite(resp. infinite).

Theorem 1.1.1. *If G is a monoid, then the identity element e is unique. If G is a group, then*

- $c \in G$ *and* $(cc = c) \Rightarrow (c = e)$*;*
- *for all* $a, b, c \in G$ *we have* $(ab = ac) \Rightarrow (b = c)$ *and* $(ba = ca) \Rightarrow (b = c)$ *(left and right cancellation);*
- *for each element in* G *its inverse element is unique;*
- *for each element in* G *the inverse of its inverse is itself;*
- *for* $a, b \in G$ *we have* $(ab)^{-1} = b^{-1}a^{-1}$*;*
- *for* $a, b \in G$ *the equation* $ax = b$ *and* $ya = b$ *have unique solutions in* $G : x = a^{-1}b$ *and* $y = ba^{-1}$.

Proposition. Let G be a semigroup. G is a group iff the following conditions hold:

- there exists an element $e \in G$ such that $ea = a$ for all $a \in G$ (left identity element);
- for each $a \in G$, there exists an element $a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

and an analogous result holds for "right inverses" and a "right identity".

Proposition. Let G be a semigroup. G is a group iff for all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G.

Proof. Left for Exercise □

***Example* 1.1.** *Let S be a nonempty set and $A(S)$ the set of all bijections $S \to S$. Under the operation of composition of functions, $\circ$, $A(S)$ is a group. The elements of $A(S)$ are called permutations and $A(S)$ is called the group of permutations on the set S. If $S = \{1, 2, 3, \cdots, n\}$, then $A(S)$ is called the symmetric group on n letters and denoted S_n. $|S_n| = n!$.*

Definition. The *direct product* of two groups G and H with identities e_G and e_H is the group whose underlying set is $G \times H$ and whose binary operation is given by:

$$(a, b)(a', b') = (aa', bb'), \qquad \text{where } a, a' \in G; b, b' \in H$$

$G \times H$ is abelian if both G and H are; (e_G, e_H) is the identity and (a^{-1}, b^{-1}) is the inverse of (a, b). Clearly $|G \times H| = |G||H|$.

Theorem 1.1.2. *Let $R(\sim)$ be an equivalence relation on a monoid G such that $a_1\ a_2$ and $b_1\ b_2$ imply $a_1b_1\ a_2b_2$ for all $a_i, b_i \in G$. Then the set G/R of all equivalence classes of G under R is a monoid under the binary operation defined by $(\bar{a})(\bar{b}) = \overline{ab}$, where $\bar{x}$ denoted the equivalence class of $x \in G$. If G is an [abelian] group, then so is G/R.*

*An equivalence relation on a monoid G that satisfies these hypothesis is called a **congruence relation** on G.*

***Example* 1.2.** *The following relation on the additive froup $\mathbb{Q}$ is a congruence relation:*

$$a \sim b \Leftrightarrow a - b \in \mathbb{Z}$$

The set of equivalence classes (denoted $\mathbb{Q}/\mathbb{Z}$) is an infinite abelian group, with addition given by $\bar{a} + \bar{b} = \overline{a + b}$, and called the group of rationals modulo one.

Definition. The *meaningful product* on any sequence of elements of a semigroup G, $\{a_1, a_2, \cdots\}$, $a_1, \cdots, a_n$(in this order), is defined inductively as below: If $n = 1$, the only meaningful product is a_1. If $n > 1$, then a meaningful product is defined to be any product of the form $(a_1 \cdots a_m)(a_{m+1} \cdots a_n)$ where $m < n$ and $(a_1 \cdots a_m)$ and $(a_{m+1} \cdots a_n)$ are meaningful products of m and $n - m$ elements respectively.

Definition. The *standard* n *product* $\prod_{i=1}^{n} a_i$ is defined as follows:

$$\prod_{i=1}^{1} a_i = a_i; \quad \text{for } n > 1, \prod_{i=1}^{n} a_i = (\prod_{i=1}^{n-1} a_i)a_n$$

Theorem 1.1.3 (Generalized Associative Law). *If G is a semigroup and $a_1, \cdots, a_n \in G$, then any two meaningful products of $a_1, \cdots, a_n$ in this order are equal.*

Theorem 1.1.4 (Generalized Commutative Law). *If G is a commutative semigroup and $a_1, \cdots, a_n \in G$, then for any permutation $i_1, \cdots, i_n$ of $1, 2, \cdots, n$, $a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}$.*

Definition. Let G be a semigroup, $a \in G$ and $n \in \mathbb{N}$. The element $a^n \in G$ is defined to be the standard n product $\prod_{i=1}^{n} a_i$ with $a_i = a$ for $1 \leqslant i \leqslant n$. If G is a monoid, a^0 is defined to be the identity element e. If G is a group, then for each $n \in \mathbb{N}$, a^{-n} is defined to be $(a^{-1})^n \in G$.

Theorem 1.1.5. *If G is a group(resp. semigroup, monoid) and $a \in G$, then for all $m, n \in \mathbb{Z}$ (resp. $\mathbb{N}$ and $\mathbb{N} \cup \{0\}$) :*

- $a^m a^n = a^{m+n}$
- $(a^m)^n = a^{mn}$

1.2 Homomorphisms and Subgroups

1.3 Cyclic Groups

1.4 Cosets and Counting

1.5 Normality, Quotient Groups, and Homomorphisms

1.6 Symmetric, Alternating, and Dihedral Groups

1.7 Categories: Products, Coproducts, and Free Objects

1.8 Direct Products and Direct Sums

1.9 Free Groups, Free Products, Generators and Relations

2

The Structure of Groups

2.1 Free Abelian Groups

2.2 Finitely Generated Abelian Groups

2.3 The Krull-Schmidt Theorem

2.4 The Action of a Group on a Set

2.5 The Sylow Theorem

2.6 Classification of Finite Groups

2.7 Nilpotent and Solvable Groups

2.8 Normal and Subnormal Series

3

Rings

3.1 Rings and Homomorphisms

3.2 Ideals

3.3 Factorization in Commutative Rings

3.4 Rings of Quotients and Localization

3.5 Rings of Polynomials and Formal Power Series

3.6 Factorization in Polynomial Rings

4

Modules

4.1 Modules, Homomorphisms and Exact Sequences

4.2 Free Modules and Vector Spaces

4.3 Projective and Injective Modules

4.4 Hom and Duality

4.5 Tensor Products

4.6 Modules over a Principal Ideal Domain

4.7 Algebras

5

Fields and Galois Theory

5.1 Field Extensions

5.2 The Fundamental Theorem

5.3 Splitting Fields, Algebraic Closure and Normality

5.4 The Galois Group of a Polynomial

5.5 Finite Fields

5.6 Separability

5.7 Cyclic Extensions

5.8 Cyclotomic Extensions

5.9 Radical Extensions

6

The Structure of Fields

6.1 Transcendence Bases

6.2 Linear Disjointness and Separability

7

Commutative Rings and Modules

7.1 Chain Conditions

7.2 Prime and Primary Ideals

7.3 Primary Decomposition

7.4 Noetherian Rings and Modules

7.5 Ring Extensions

7.6 Dedekind Domains

7.7 The Hilbert Nullstellensatz

8

The Structure of Rings

8.1 Simple and Primitive Rings

8.2 The Jacobson Radical

8.3 Semisimple Rings

8.4 The Prime Radical; Prime and Semiprime Rings

8.5 Algebras

8.6 Division Algebras

9

Categories

9.1 Functors and Natural Transformations

9.2 Adjoint Functors

9.3 Morphisms