Abstract Algebra

Hechen Hu

November 28, 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

Definition. Let G and H be semigroups. A function $f : G \to H$ is a *homomorphism* provided

$$f(ab) = f(a)f(b) \text{ for all } a, b \in G$$

If f is injective as a map of sets, f is said to be a *monomorphism.* If f is surjective, f is called an *epimorphism.* If f is bijective, f is called an *isomorphism.* In this case G and H are said to be *isomorphic* (written $G \cong H$). A homomorphism $f : G \to G$ is called an *endomorphism* of G and an isomorphism $f : G \to G$ is called an *automorphism* of G.

Definition. Let $f : G \to H$ be a homomorphism of groups. The *kernel* of f(denoted Ker f) is $\{a \in G | f(a) = e \in H\}$. If A is a subset of G, then $f(A) = \{b \in H | b = f(a)$ for some $a \in A\}$ is the *image of* A. $f(G)$ is called the *image of* f and denoted Im f. If B is a subset of H, $f^{-1}(B) = \{a \in G | f(a) \in B\}$ is the *inverse image* of B.

Theorem 1.2.1. *Let $f : G \to H$ be a homomorphism of groups. Then*

- *f is a monomorphism iff Ker $f = \{e\}$.*
- *f is an isomorphism iff there is a homomorphism $f^{-1} : H \to G$ such that $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$.*

Definition. Let G be a semigroup and H a nonempty subset of it. If for every $a, b \in H$ we have $ab \in H$, we say that H is *closed* under the product in G. This is the same as saying that the binary operation on G, when restricted to H, is a binary operation on H.

Definition. Let G be a group and H a nonempty subset that is closed under the product in G. If H is itself a group under the product in G, then H is said to be a *subgroup* of G, denoted $H < G$.

Definition. If a subgroup H is not G itself or the *trivial subgroup*, which consists only of the identity element, is called a *proper subgroup.*

Theorem 1.2.2. *Let H be a nonempty subset of a group G. Then H is a subgroup of G iff $ab^{-1} \in H$ for all $a, b \in H$.*

Corollary. *If G is a group and $\{H_i | i \in I\}$ is a nonempty family of subgroups, then $\bigcap\limits_{i \in I} H_i$ is a subgroup of G.*

Proof. Left for Exercise □

Definition. Let G be a group and X a subset of G. Let $\{H_i | i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap\limits_{i \in I} H_i$ is called the *subgroup of G generated by the set X* and denoted $\langle X \rangle$. The elements of X are the *generators* of $\langle X \rangle$. If $G = \langle a_1, \cdots, a_n \rangle, (a_i \in G)$, G is said to be finitely generated. If $a \in G$, the subgroup $\langle a \rangle$ is called the *cyclic (sub)group* generated by a.

Theorem 1.2.3. *If G is a group and X a nonempty subset of G, then the subgroup $\langle X \rangle$ generated by X consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} (a_i \in X; n_i \in \mathbb{Z})$. In particular for every $a \in G$, $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.*

Proof. Left for Exercise □

Definition. The subgroup $\langle \bigcap\limits_{i \in I} H_i \rangle$ generated by the set $\bigcap\limits_{i \in I} H_i$ is called the *subgroup generated by the groups* $\{H_i | i \in I\}$. If H and K are subgroups, the subgroup $\langle H \cup K \rangle$ generated by H and K is called the *join* of H and K and is denoted $H \vee K$.

1.3 Cyclic Groups

Definition. A *cyclic group* or *monogenous group* is a group that is generated by a single element. That is, it consists of a set of elements with a single invertible associative operation, and it contains an element such that every other element of the group may be obtained by repeatedly applying the group operation or its inverse to it.

Theorem 1.3.1. *Every subgroup H of the additive group $\mathbb{Z}$ is cyclic. Either $H = \langle 0 \rangle$ or $H = \langle m \rangle$, where m is the least positive interger in H. If $H \neq \langle 0 \rangle$, then H is infinite.*

Theorem 1.3.2. *Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite group of order m is isomorphic to the additive group $\mathbb{Z}_m$.*

Proof. Left for Exercise □

Definition. Let G be a group and $a \in G$. The *order* of a is the order of the cyclic subgroup $\langle a \rangle$ and is denoted $|a|$.

Theorem 1.3.3. *Let G be a group and $a \in G$. If a has infinite order, then*

- $a^k = e$ *iff* $k = 0$;
- *the elements* $a^k (k \in \mathbb{Z})$ *are all distinct.*

If a has inite order $m > 0$, then

- m *is the least positive integer such that* $a^m = e$;
- $a^k = e$ *iff* $m|k$;
- $a^r = a^s$ *iff* $r \equiv s (mod m)$;
- $\langle a \rangle$ *consists of the distinct elements* $a, a^2, \cdots, a^{m-1}, a^m = e$;
- *for each k such that* $k|m$, $|a^k| = m/k$.

Theorem 1.3.4. *Every homomorphic image and every subgroup of a cyclic group G is cyclic. In particular, if H is a nontrivial subgroup of $G = \langle a \rangle$ and m is the least positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.*

Theorem 1.3.5. *Let $G = \langle a \rangle$ be a cyclic group. If G is infinite, then a and a^{-1} are the only generators of G. If G is finite of order m, then a^k is a generator of G iff $(k, m) = 1$.*

1.4 Cosets and Counting

Definition. Let H be a subgroup of a group G and $a, b \in G$. a is *right congruent to b modulo H*, denoted $a \equiv_r b(\text{mod } H)$ if $ab^{-1} \in H$. a is *left congruent to b modulo H* , denoted $a \equiv_l b(\text{mod } H)$ if $a^{-1}b \in H$.

Theorem 1.4.1. *Let H be a subgroup of a group G.*

- *Right(resp. left) congruence modulo H is an equivalence relation on G.*
- *The equivalence class of $a \in G$ under right(resp. left) congruence modolo H is the set $Ha = \{ha|h \in H\}$(resp. $aH = \{ah|h \in H\}$).*
- *$|Ha| = |H| = |aH|$ for all $a \in G$.*

Definition. The set Ha above is called a *right coset* of H in G and aH is called an *left coset* of H in G.

Corollary. *Let H be a subgroup of a group G.*

- *G is the union of the right(resp. left) cosets of H in G.*
- *Two right(resp. left) cosets of H in G are either disjoint or equal.*
- *For all $a, b \in G$, $(Ha = Hb) \Leftrightarrow (ab^{-1} \in H)$ and $(aH = bH) \Leftrightarrow (a^{-1}b \in H)$.*
- *If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.*

Definition. Let H be a subgroup of a group G. The *index of H in G*, denoted $[G : H]$, is the cardinal number of the set of distince right(resp. left) cosets of H in G.

Definition. A *complete set of right coset representatives* of a subgroup H in a group G is a set $\{a_i\}$ consisting of precisely one element from each right coset of H in G and having cardinality $[G : H]$.

Theorem 1.4.2. *If K, H, G are groups with $K < H < G$, then $[G : K] = [G : H][H : K]$. If any two of these indices are finite, then so is the third.*

Proof. Left for Exercise □

Corollary (Lagrange)**.** *If H is a subgroup of a group G, then $|G| = [G : H]|H|$. In particular if G is finite, the order $|a|$ of $a \in G$ devides $|G|$.*

Theorem 1.4.3. *If the set $\{ab|a \in H, b \in K\}$ is denoted HK, then for two finite subgroups H and K of a group G $|HK| = |H||K|/|H \cap K|$.*

Proposition. If H and K are subgroups of a group G, then $[H : H \cap K] \leqslant [G : K]$. If $[G : K]$ is finite, then $[H : H \cap K] = [G : K]$ iff $G = KH$.

Proposition. Let H and K be subgroups of finite index of a group G. Then $[G : H \cap K]$ is finite and $[G : H \cap K] \leqslant [G : H][G : K]$. Furthermore, $[G : H \cap K] = [G : H][G : K]$ iff $G = HK$.

Proof. Left for Exercise □

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

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