Groups, Rings and Fields

Cunsheng Ding

HKUST, Hong Kong

November 17, 2015

Contents

Definition of Groups

Definition 1

A group is a set G together with a binary operation $*$ on G such that the following three properties hold:

1. $a * b \in G$ for all $a \in G$ and $b \in G$ (i.e., G is closed under "$*$").
2. $*$ is associative; that is, for any $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
3. There is an *identity* (or *unity*) element e in G such that for all $a \in G$, $a * e = e * a = a$.
4. For each $a \in G$, there exists an inverse element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Remarks

- If $a * b = b * a$ for all $a, b \in G$, then G is called abelian (or commutative).
- For simplicity, we frequently use the notation of ordinary multiplication to designate the operation in the group, writing simply ab instead of $a * b$. But by doing so we do not assume that the operation actually is the ordinary multiplication.

Order of Elements and Groups

Definition 2

Let $(G, *)$ be a group with identity e. Due to the associativity of $*$, we define

$$a^n = \underbrace{a * a * \cdots * a}_{n \text{ copies of } a}$$

for any $n \in \mathbb{N}$. The least positive integer n such that $a^n = e$, if it exits, is called the order of $a \in G$, and denoted by $\mathrm{ord}(a)$.
If every element a of G can be expressed as g^k for some integer $k \geq 0$, then $g \in G$ is called a generator of G. In this case, $(G, *)$ is called a cyclic group.

Definition 3

A group is called a finite group if it has finitely many elements. The number of elements in a finite group G is called its order, denoted by $|G|$.

Subgroups of a Group

Definition 4

A subset H of a group G is called a subgroup of G if H is itself a group with respect to the operation of G.
Subgroups of G other than the trivial subgroups $\{e\}$ and G itself are called nontrivial subgroups of G.

Example 5

Let $(G, *)$ be any group. Define $\langle a \rangle = \{a^i \mid i = 0, 1, 2, \cdots,\}$. Then it is easy to verify that $\langle a \rangle$ is a subgroup of G and $|\langle a \rangle| = \mathrm{ord}(a)$.

Examples of Groups and Subgroups

Example 6

Let $n > 1$ be an integer. Then $(\mathbb{Z}_n, \oplus_n)$ is an abelian group with n elements.

- The identity element of this group is 0.
- The inverse of any $a \in \mathbb{Z}_n$ is $n - a$.
- $\mathrm{ord}(1) = n$.
- $(\mathbb{Z}_n, \oplus_n)$ is cyclic and 1 is a generator.
- If $n = n_1 n_2$, then $\langle n_1 \rangle = \{0, n_1, 2n_1, \cdots, (n_2 - 1)n_1\}$ is a subgroup of $(\mathbb{Z}_n, \oplus_n)$.

Examples of Groups

Example 7

Let p be a prime. Then $(\mathbb{Z}_p^*, \otimes_p)$ is an abelian group with $p-1$ elements, where $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$.

- The identity element of this group is 1.
- The inverse of any $a \in \mathbb{Z}_p^*$ is the multiplicative inverse of a modulo p.
- The group is cyclic, and has $\phi(p-1)$ generators. Each generator is called a primitive root of p or modulo p, where $\phi(n)$ is the Euler totient function.

Recall of definition

For any $n \in \mathbb{N}$, the **Euler totient function** $\phi(n)$ is the total number of integers i such that $1 \leq i \leq n-1$ and $\gcd(i, n) = 1$.

Lagrange's Theorem

Theorem 8 (Lagrange)

The order of every subgroup H of a finite group G divides the order of G.

Proof.

Define a binary relation R_H on G by $(a,b) \in R_H$ if and only if $a = bh$ for some $h \in H$. Since H is a subgroup, it is easily verified that R_H is an equivalence relation. Hence, the equivalence classes, $\{aH \mid a \in G\}$, called left cosets of H, form a partition of G.

Now we define a map $f : aH \to bH$ by $f(x) = ba^{-1}x$. Then f is bijective as its inverse is given by $f^{-1}(y) = ab^{-1}y$. Hence, all the left cosets have the same number of elements, i.e., $|H|$.

If we use $[G : H]$ to denote the number of distinct left cosets, we have then $|G| = [G : H]|H|$.

The desired conclusion then follows.

$\square$

Order of Elements and Groups

Corollary 9

Let G be a finite group. Then $\mathrm{ord}(a)$ divides $|G|$ for every $a \in G$.

Proof.

By Example 5, $\mathrm{ord}(a) = |\langle a \rangle|$, which is the order of the subgroup $\langle a \rangle$. The desired conclusion then follows from Theorem 8. $\square$

Rings

Definition 10

A ring $(R, +, \cdot)$ is a set R, together with two binary operations, denoted by $+$ and $\cdot$, such that:

1. $(R, +)$ is an abelian group.
2. $\cdot$ is associative, i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
3. The distributive laws hold; that is, for all $a, b, c \in R$ we have

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (b + c) \cdot a = b \cdot a + c \cdot a.$$

Remarks on the Definition of Rings

- We use 0 (called the <u>zero element</u>) to denote the identity of the group $(R, +)$.
- $-a$ denotes the inverse of a with respect to $+$.
- By $a - b$ we mean $a + (-b)$.
- Instead of $a \cdot b$, we write ab.
- $a0 = 0a = 0$.
  - Note $a(0+0) = a0 + a0$ by the distribution law. But $0 + 0 = 0$. Hence $a0 = a0 + a0$ and $a0 = 0$.
- We shall use R as a designation for the ring $(R, +, \cdot)$, and stress that the operations $+$ and $\cdot$ are not necessarily the ordinary operations with numbers.

Integral Domains, Division Rings and Fields

Definition 11

1. A ring is called a ring with identity if the ring has a multiplicative identity, i.e., if there is an element e such that $ae = ea = a$ for all $a \in R$.
2. A ring is commutative if $\cdot$ is commutative.
3. A ring is called an integral domain if it is a commutative ring with identity $e \neq 0$ in which $ab = 0$ implies $a = 0$ or $b = 0$.
4. A ring is called a division ring (or skew field) if the nonzero elements of R form a group under "$\cdot$".
5. A commutative division ring is called a field.

Examples of Rings, Integral Domains and Fields

Example 12

$(\mathbb{Z}, +, \times)$ is commutative ring with identify 1 and an integral domain, but not a division ring, not a field.

Example 13

Let $n > 1$ be an integer. Then $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ is a commutative ring with identity 1. In particular, $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ is a field if and only if n is a prime.

Notation

Let p be any prime. We use $\mathrm{GF}(p)$ or $\mathbb{F}_p$ to denote the field $(\mathbb{Z}_p, \oplus_p, \otimes_p)$, which is called a prime field.
$\mathrm{GF}(p)$ is called a finite field, as it has finitely many elements.

Examples of Rings, Integral Domains and Fields

Example 14

Let $\mathbb{Q}$ denote the set of all rational numbers. Then $(\mathbb{Q}, +, \times)$ is a field.

Example 15

Let $\mathbb{R}$ denote the set of all real numbers. Then $(\mathbb{R}, +, \times)$ is a field.

Example 16

Let $\mathbb{C}$ denote the set of all complex numbers. Then $(\mathbb{C}, +, \times)$ is a field.

Euclidean Domains

Definition 17

A Euclidean domain is an integral domain $(R, +, \cdot)$ associated with a function g from R to the set of nonnegative integers such that

C1: $g(a) \leq g(ab)$ if $b \neq 0$; and

C2: for all $a, b \neq 0$, there exist q and r ("quotient" and "remainder") such that $a = qb + r$, with $r = 0$ or $g(r) < g(b)$.

Examples of Euclidean Domains

Proposition 18

$(\mathbb{Z}, +, \cdot, g)$ *is a Euclidean domain, where* $g(a) = |a|$ *and* $\mathbb{Z}$ *is the set of all integers.*

Proof.

It is easily verified that $(\mathbb{Z}, +, \cdot, g)$ is an integral domain. For any integers a and $b \neq 0$, we have

$$|a| \leq |ab| = |a||b|.$$

This means that Condition C1 is met.
For any a and $b > 0$, let $q = \lfloor a/b \rfloor$ and $r = a - qb$. Then $0 \leq r < b$. Hence, $r = 0$ or $g(r) < g(b)$.
For any a and $b < 0$, let $q = \lfloor -a/b \rfloor$ and $r = -a - qb$. Then $0 \leq r < -b$. Hence, $r = 0$ or $g(r) < g(b) = g(-b)$.
Summarizing the conclusions in the two cases above proves that C2 is also satisfied. The desired conclusion then follows. $\square$

Examples of Euclidean Domains

Example 19

Let $R = \left\{ a + b\sqrt{-1} \mid a, b \text{ integers } \right\}$. Define $g(a + b\sqrt{-1}) = a^2 + b^2$. Then $(R, +, \cdot, g)$ is an Euclidean domain.

Proof.

Left as an exercise. A proof is also available on the course web page. □