

# Notes on Groups, Rings, and Fields

Tan Yee Fan

2009 January 15

## 1 Binary Operations and Mathematical Systems

Let  $S$  be a nonempty set. Then a *binary operation*  $*$  on  $S$  is a function from  $S \times S$  to  $S$ . In other words, we say that  $*$  is *closed* on  $S$ . We will write  $a * b$  as the binary operation on  $a$  and  $b$  in  $S$ .

A *mathematical system* is an ordered tuple  $(S, *_1, \dots, *_n)$ , where  $S$  is a nonempty set and each  $*_i$  is a binary operation on  $S$ . When there is no ambiguity, the above mathematical system is often denoted as just  $S$ .

### 1.1 Properties

Let  $(S, *)$  be a mathematical system. The following properties can be defined:

- We say that  $*$  is *commutative* if for all  $a, b \in S$ , we have  $a * b = b * a$ .
- We say that  $*$  is *associative* if for all  $a, b, c \in S$ , we have  $a * (b * c) = (a * b) * c$ .
- We say that  $e \in S$  is an *identity* if for all  $a \in S$ , we have  $a * e = a = e * a$ .
- We say that  $b \in S$  is an *inverse* of  $a \in S$  if  $a * b = e = b * a$ , where  $e$  is an identity of  $S$ .

An identity element, if it exists, is unique. If  $*$  is associative, then we write  $a * b * c$  for  $(a * b) * c$ ,  $a * b * c * d$  for  $(a * b * c) * d$ , and so on.

Let  $(S, *_1, *_2)$  be a mathematical system. We say that  $*_2$  is *distributive* over  $*_1$  if for all  $a, b, c \in S$ , we have  $a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c)$  and  $(b *_1 c) *_2 a = (b *_2 a) *_1 (c *_2 a)$ . In such mathematical systems,  $*_1$  is often some addition operation while  $*_2$  is often some multiplication operation.

Let  $(S, *)$  be a mathematical system. Then an element  $a \in S$  is said to be an *idempotent element* if  $a * a = a$ . The binary operation  $*$  is said to be *idempotent* if all elements in  $S$  are idempotent elements. In particular, the identity element, if it exists, is an idempotent element. An example of an idempotent binary operation is the maximum value function on real numbers, with  $\max(a, a) = a$  for all  $a \in \mathbb{R}$ .

## 1.2 Notations

When describing mathematical systems involving a binary operator  $*$ , it is common to use shorthand notations. There are two common notations in use, namely the multiplicative notation and the additive notation.

- In the multiplicative notation, we write  $ab$  for  $a*b$ . If the identity element exists, it is denoted by 1. If an element  $a$  has a unique inverse, then it is denoted by  $a^{-1}$ . If  $*$  is associative, then we write  $a^n$  for  $a$  multiplied to itself  $n$  times, i.e.,  $a^1 = a$ ,  $a^2 = aa$ ,  $a^3 = aaa$ , and so on. The identity element, if it exists, can be written as  $a^0$ . If unique  $(a^n)^{-1}$  and  $(a^{-1})^n$  exist such that  $(a^n)^{-1} = (a^{-1})^n$ , it can be written as  $a^{-n}$ .
- In the additive notation, we use the  $+$  symbol in place of  $*$ . If the identity element exists, it is denoted by 0. If an element  $a$  has an inverse, then it is denoted by  $-a$ . If  $+$  is associative, then we write  $na$  for  $a$  added to itself  $n$  times, i.e.,  $1a = a$ ,  $2a = a + a$ ,  $3a = a + a + a$ , and so on. The identity element, if it exists, can be written as  $0a$ . If unique  $-(na)$  and  $(-n)a$  exist such that  $-(na) = (-n)a$ , then it can be written as  $-na$ .

By default, we use the multiplicative notation, unless the binary operation  $*$  is some form of addition.

In a mathematical system involving a multiplication operator  $\times$  and an addition operator  $+$ , by convention,  $\times$  takes precedence over  $+$  in the absence of parentheses. That is,  $ab + c$  means  $(ab) + c$  and  $a + bc$  means  $a + (bc)$ .

It is common to discuss two mathematical systems  $(S, *_1, \dots, *_n)$  and  $(S', *'_1, \dots, *'_n)$ , where  $S \neq S'$ , but sharing common binary operations  $*_1, \dots, *_n$ . By convention, each  $*_i$  is a function from  $S \times S$  to  $S$  when we are referring to the mathematical system  $S$ , and each  $*'_i$  is a function from  $S' \times S'$  to  $S'$  when we are referring to the mathematical system  $S'$ . In particular, if  $S' \subseteq S$ , then each  $*'_i$  as applied on  $S'$  is a restriction of  $*_i$  as applied on  $S$ .

## 2 Groups

A *group* is a mathematical system  $(G, *)$  satisfying the following properties:

- $*$  is associative on  $G$ .
- There exists an identity in  $G$  with respect to  $*$ .
- Each element in  $G$  has an inverse with respect to  $*$ .

If  $*$  is commutative, then we say that  $G$  is a *commutative group* or *Abelian group*. If  $G$  satisfies only the first property, then we say that  $G$  is a *semigroup*.

Let  $(G, *)$  be a mathematical system where  $G$  contains exactly one element. Then it is easy to verify that  $G$  is a commutative group whose sole element is its identity. This group is known as the *trivial group*.

Let  $G$  be a group. For any element  $a \in G$ , its inverse is unique and can be denoted by  $a^{-1}$ . The *cancellation laws* can be applied to a group  $G$ : for

all  $a, b, c \in G$ ,  $ab = ac$  or  $ba = ca$  implies  $b = c$ , since for the first case we have  $b = 1b = a^{-1}ab = a^{-1}ac = 1c = c$  and for the second case we have  $b = b1 = baa^{-1} = caa^{-1} = c1 = c$ . Also, we have the properties  $(a^{-1})^{-1} = a$  and  $(ab)^{-1} = b^{-1}a^{-1}$ .

Examples:

- $(\mathbb{Z}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{Q}, +)$ , and  $(\mathbb{C}, +)$  are commutative groups, where  $+$  is the usual addition operation. In each group, the identity element is 0, and the inverse of  $a$  is  $-a$ .
- $(\mathbb{R} \setminus \{0\}, \times)$ ,  $(\mathbb{Q} \setminus \{0\}, \times)$ , and  $(\mathbb{C} \setminus \{0\}, \times)$  are commutative groups, where  $\times$  is the usual multiplication operation. In each group, the identity element is 1, and the inverse of  $a$  is  $\frac{1}{a}$ .
- Let  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  and  $+_n$  to mean addition modulo  $n$ . Then  $(\mathbb{Z}_n, +_n)$  is a commutative group whose identity is 0, and the inverse of  $a$  is  $(-a)(\text{mod } n)$ .
- Let  $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$  and  $\times_n$  to mean multiplication modulo  $n$ . Then  $(\mathbb{Z}_n^*, \times_n)$  is a commutative group whose identity is 1, and the inverse of  $a$  is  $a^{-1}(\text{mod } n)$ . This implies that  $(\mathbb{Z}_n \setminus \{0\}, \times_n)$  is a group if and only if  $n$  is a prime number.
- Let  $GL_n(\mathbb{R})$  be the set of nonsingular real matrices of size  $n$ , and  $\times$  denote matrix multiplication. Then  $(GL_n(\mathbb{R}), \times)$  is a noncommutative group whose identity is  $\mathbf{I}_n$ , and the inverse of  $\mathbf{A} \in GL_n(\mathbb{R})$  is  $\mathbf{A}^{-1}$ , the matrix inverse of  $\mathbf{A}$ .
- Let  $(G_1, *_1)$  and  $(G_2, *_2)$  be groups. Let  $G = G_1 \times G_2$  and define the binary operation  $*$  on  $G_1 \times G_2$  to be  $(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$ . Then  $(G, *)$  is a group and is called the *direct product* of  $G_1$  and  $G_2$ . The identity of  $G$  is  $(1_{G_1}, 1_{G_2})$ , where  $1_{G_1}$  is the identity of  $G_1$  and  $1_{G_2}$  is the identity of  $G_2$ . For  $(a, b) \in G$ , its inverse is  $(a^{-1}, b^{-1})$ , where  $a^{-1}$  is the inverse of  $a$  in  $G_1$  and  $b^{-1}$  is the inverse of  $b$  in  $G_2$ . If  $G_1$  and  $G_2$  are both commutative, then  $G$  is also commutative.

## 2.1 Subgroups

Let  $(G, *)$  be a group and  $G' \subseteq G$ . Then  $(G', *)$  is a *subgroup* of  $(G, *)$  if  $(G', *)$  is a group. If there is no ambiguity, we simply say that  $G'$  is a subgroup of  $G$ . Note that the identity element of  $G$  and  $G'$  are the same, any element in  $G'$  has the same inverse in  $G$  and  $G'$ . For a group  $G$ , its *trivial subgroups* are  $\{1\}$  and  $G$ , and all other subgroups are nontrivial.

The following theorem is useful for determining subgroups. Let  $G$  be a group and  $G'$  be a nonempty subset of  $G$ . Then  $G'$  is a subgroup of  $G$  if and only if for all  $a, b \in G'$ , we have  $ab^{-1} \in G'$ .

Examples:

- Consider the groups  $(G_i, +)$ , where  $G_1 = \{0\}$ ,  $G_2 = \mathbb{Z}$ ,  $G_3 = \mathbb{Q}$ ,  $G_4 = \mathbb{R}$ ,  $G_5 = \mathbb{C}$ , and  $+$  is the usual addition operation. Then if  $i \leq j$ ,  $G_i$  is a subgroup of  $G_j$ .
- Consider the groups  $(G_i, \times)$ , where  $G_1 = \{1\}$ ,  $G_2 = \mathbb{Q} \setminus \{0\}$ ,  $G_3 = \mathbb{R} \setminus \{0\}$ ,  $G_4 = \mathbb{C} \setminus \{0\}$ , and  $\times$  is the usual multiplication operation. Then if  $i \leq j$ ,  $G_i$  is a subgroup of  $G_j$ .
- Any subgroup of  $(\mathbb{Z}, +)$  has the form  $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ , where  $n = 0, 1, 2, \dots$ . Therefore,  $0\mathbb{Z} = \{0\}$ ,  $1\mathbb{Z} = \mathbb{Z}$ ,  $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$  and is denoted by  $\mathbb{E}$ ,  $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$ , and so on.
- Let  $G'$  and  $G''$  be two subgroups of  $G$ . Then  $G' \cap G''$  is a subgroup of  $G$ . Also,  $G' \cup G''$  is a subgroup of  $G$  if and only if  $G' \subseteq G''$  or  $G'' \subseteq G'$ .
- Let  $G_1$  and  $G_2$  be two groups, and let  $G'_1$  and  $G'_2$  be subgroups of  $G_1$  and  $G_2$  respectively. Then the direct product  $G'_1 \times G'_2$  is a subgroup of the direct product  $G_1 \times G_2$ .
- Let  $G$  be a group. Then the *center* of  $G$ , defined by  $Z(G) = \{b \in G \mid \forall a \in G, ba = ab\}$ , is a subgroup of  $G$ .
- Let  $G$  be a group and let  $a \in G$ . Then the *centralizer* or *normalizer* of  $a$  in  $G$ , defined by  $C(a) = \{b \in G \mid ba = ab\}$  is a subgroup of  $G$ . Note that  $C(a) = G$  if and only if  $a \in Z(G)$ .

## 2.2 Cyclic Groups

Let  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ . A group  $G$  is a *cyclic group* if there exists  $a \in G$  such that  $G = \langle a \rangle$ , and we call  $a$  the *generator* of  $G$ . Note that all cyclic groups are commutative. If a cyclic group  $G$  is generated by  $a$  and has a finite number of elements, then  $G = \{1, a, a^2, \dots, a^{n-1}\}$ , where  $n$  is the number of elements in  $G$ . For a group  $G$ , if  $a \in G$ , then  $\langle a \rangle$  is a subgroup of  $G$ .

For example,  $(\mathbb{Z}, +)$  is a cyclic group because  $\mathbb{Z} = \langle 1 \rangle$ . Also,  $(\mathbb{Z}_n, +_n)$  is a cyclic group because  $\mathbb{Z}_n = \langle 1 \rangle$ . Any group with  $p$  elements, where  $p$  is a prime integer, is cyclic and is generated by any nonidentity element of the group. One such group is  $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ , where  $p$  is prime.

## 2.3 Cosets

Let  $G$  be a group,  $a$  be an element of  $G$ , and  $H$  be a subgroup of  $G$ . The set  $aH = \{ah \mid h \in H\}$  is called a *left coset* of  $H$  in  $G$ , and the set  $Ha = \{ha \mid h \in H\}$  is called a *right coset* of  $H$  in  $G$ . A *coset* is either a left coset or a right coset. Note that for all  $a, b \in G$ , either  $aH = bH$  or  $aH \cap bH = \emptyset$ , and hence the set of unique left cosets of  $H$  in  $G$  form a partition of  $G$ . Similar comments can be made for the right cosets. Further, for all  $a \in G$ ,  $|aH| = |H| = |Ha|$ , and hence the number of left cosets of  $H$  in  $G$  equals the number of right cosets of  $H$  in  $G$ . This number is known as the *index* of  $H$  in  $G$  and is written  $[G : H]$ .

## 2.4 Orders

Let  $G$  be a group. Then the *order* of  $G$  is defined as the cardinality of  $G$ , denoted as  $o(G)$  or  $|G|$ . Let  $a$  be an element of a group  $G$ . Then the *order* of  $a$  is the least positive integer  $n$  such that  $a^n = 1$ , or infinite if no such  $n$  exists. Based on these definitions, for any group  $G$ ,  $o(1) = 1$ , and for any  $a \in G \setminus \{1\}$ , we have  $o(a) \geq 1$ . In a finite group  $G$ , i.e.,  $o(G)$  is finite, all elements in  $G$  has finite order. For any element  $a$  in a finite group  $G$ , if  $o(a) = n$ , then  $o(a^k) = \frac{n}{\gcd(k,n)}$  for all positive integers  $k$ . For any finite group  $G$ ,  $G$  is a cyclic group generated by  $a \in G$  if and only if  $o(G) = o(a)$ . If all nonidentity elements of a group  $G$  has order 2, then  $G$  is commutative, because for all  $a, b \in G$ , we have  $ab = 1ab1 = (bb)ab(aa) = b(ba)(ba)a = b1a = ba$ .

*Lagrange's theorem* states that if  $G$  is a group and  $G'$  is any subgroup of  $G$ , then  $|G| = [G : G']|G'|$ , that is,  $o(G')$  divides  $o(G)$ . As a consequence, for a group  $G$ , for any  $a \in G$ , we have  $o(a)$  divides  $o(G)$ , since  $\langle a \rangle$  is a subgroup of  $G$ . On the other hand, *Cauchy's theorem* gives a partial converse of Lagrange's theorem, and states that if  $G$  is a finite group of order  $n$  and  $n$  is divisible by a prime  $p$ , then  $G$  has an element of order  $p$  and hence a subgroup of order  $p$ . As a consequence, if  $G$  is a finite commutative group with order  $n$ , then for any positive integer  $m$  such that  $n$  is divisible by  $m$ ,  $G$  has a subgroup of order  $m$ . *Sylow's first theorem* states that if  $G$  is a group of order  $p^r m$ , where  $p$  is a prime,  $r$  and  $m$  are positive integers such that  $\gcd(p, m) = 1$ , then  $G$  has a subgroup of order  $p^k$  for all  $0 \leq k \leq r$ .

## 2.5 Normal Subgroups and Quotient Groups

Let  $G$  be a group and  $H$  be a subgroup of  $G$ . Then  $H$  is a *normal subgroup* of  $G$  if  $aH = Ha$  for all  $a \in G$ . Let  $H$  be a normal subgroup of  $G$ . Let  $G/H = \{aH | a \in G\}$  and define  $*$  on  $G/H$  by  $(aH) * (bH) = abH$ . Then  $(G/H, *)$  is a group, and we call  $G/H$  the *quotient group* of  $G$  by  $H$ .

## 2.6 Homomorphisms and Isomorphisms

Let  $(G_1, *_1)$  and  $(G_2, *_2)$  be groups. A function  $f : G_1 \rightarrow G_2$  is a *homomorphism* of  $G_1$  to  $G_2$  if for all  $a, b \in G_1$ , we have  $f(a *_1 b) = f(a) *_2 f(b)$ . A homomorphism  $f$  of  $G_1$  to  $G_2$  is an *isomorphism* if  $f$  is a bijective function, in which case we say that  $G_1$  to  $G_2$  are *isomorphic*, and write  $G_1 \simeq G_2$ . An isomorphism between a group with itself is an *automorphism*.

Note that every finite cyclic group of order  $n$  is isomorphic to  $(\mathbb{Z}_n, +_n)$  and every infinite cyclic group is isomorphic to  $(\mathbb{Z}, +)$ , by an isomorphism that maps  $a^n$  to  $n$  for a generator  $a$  of the cyclic group. As such, all cyclic groups of the same order are isomorphic to each other. For any prime number  $p$ , since any group with order  $p$  is cyclic, there is only one group of order  $p$  up to isomorphism. Up to isomorphism, there are only two groups of order 4, and there are only two groups of order 6.

### 3 Rings and Fields

A *ring* is a mathematical system  $(R, +, \times)$  such that  $(R, +)$  is a commutative group,  $(R, \times)$  is a semigroup, and  $\times$  distributes over  $+$ . The identity of  $+$  on  $R$  is called the *zero element* and is denoted by 0. The identity of  $\times$  on  $R$ , if it exists, is called the *identity* of  $R$  and is denoted by 1. An element in  $R$  is called a *unit* or *invertible element* if it has an inverse with respect to  $\times$ . A nonzero element  $a$  in  $R$  is called a *zero divisor* if there exists a nonzero element  $b$  in  $R$  such that either  $ab = 0$  or  $ba = 0$ . Note that any element in  $R$  cannot be a unit and a zero divisor at the same time. An element  $a \in R$  is called *idempotent* if  $a^2 = a$ . An element  $a \in R$  is called *nilpotent* if  $a^n = 0$  for some positive integer  $n$ . Note that a nonzero idempotent cannot be a nilpotent, and if  $R$  has no zero divisors, then the only idempotents in  $R$  are 0 and 1. If  $\times$  is commutative, then we say that  $R$  is a *commutative ring* or *Abelian ring*.

The ring  $R = \{0\}$  is known as the *trivial ring*, and its identity is 0. It can be proven that if  $R$  is a ring with identity, then  $R$  is nontrivial if and only if 0 and 1 are distinct elements. Hence, from here onwards, we assume that all rings are nontrivial by default and therefore  $0 \neq 1$ . With this assumption, 0 cannot be a unit in  $R$ .

Let  $R$  be a ring. Then  $R$  has no zero divisors if and only if the cancellation laws hold, i.e., for all  $a, b, c \in R$ ,  $ab = ac$  or  $ba = ca$  implies that  $b = c$ .

Examples:

- $(\mathbb{Z}, +, \times)$  is known as the *ring of integers*, where  $+$  and  $\times$  are the usual addition and multiplication operations. It is a commutative ring, whose zero element is 0 and identity element is 1.  $\mathbb{Z}$  has no nonidentity units, and has no zero divisors.
- $(\mathbb{Z}_n, +_n, \times_n)$  is a commutative ring whose zero element is 0 and identity element is 1. If  $n$  is prime, then every nonzero element of  $\mathbb{Z}_n$  is a unit, and  $\mathbb{Z}_n$  contains no zero divisors. If  $n$  is composite, then  $n = m_1 m_2$  for some  $1 < m_1, m_2 < n$ , which means  $\mathbb{Z}_n$  contains zero divisors such as  $m_1$  and  $m_2$ , and hence not all elements of  $\mathbb{Z}_n$  are units.
- Let  $M_n(\mathbb{Z})$  be the set of  $n$  by  $n$  matrices over the ring of integers. Then  $(M_n(\mathbb{Z}), +, \times)$  is a noncommutative ring, where  $+$  and  $\times$  are the matrix addition and multiplication operations. Its zero element is the zero matrix  $\mathbf{0}_n$  and its identity is the identity matrix  $\mathbf{I}_n$ .  $M_n(\mathbb{Z})$  contain both nonzero invertible elements and nonzero noninvertible elements, and that  $M_n(\mathbb{Z})$  contains zero divisors.
- Let  $(R_1, +_1, \times_1)$  and  $(R_2, +_2, \times_2)$  be rings. Consider  $R_1 \times R_2$ , where  $+$  and  $\times$  are defined on  $R_1 \times R_2$  by  $(a_1, a_2) + (b_1, b_2) = (a_1 +_1 b_1, a_2 +_2 b_2)$  and  $(a_1, a_2) \times (b_1, b_2) = (a_1 \times_1 b_1, a_2 \times_2 b_2)$ . Then  $(R_1 \times R_2, +, \times)$  is also a ring. If  $R_1$  and  $R_2$  are commutative, then  $R_1 \times R_2$  is also commutative. The zero element of  $R_1 \times R_2$  is  $(0_{R_1}, 0_{R_2})$ , where  $0_{R_1}$  and  $0_{R_2}$  are the respective zero elements of  $R_1$  and  $R_2$ . If  $R_1$  and  $R_2$  have identities  $1_{R_1}$  and  $1_{R_2}$

respectively, then the identity of  $R_1 \times R_2$  is  $(1_{R_1}, 1_{R_2})$ . However, even if  $R_1$  and  $R_2$  are division rings,  $R_1 \times R_2$  is not since  $(0_{R_1}, 1_{R_2}) \times (1_{R_1}, 0_{R_2}) = (0_{R_1}, 0_{R_2})$ , which means that  $R_1 \times R_2$  has zero divisors.

- The *zero ring* is a ring  $R$  where  $ab = 0$  for all  $a, b \in R$ . A nontrivial zero ring  $R$  has no identity and every nonzero element of  $R$  is a zero divisor. Note that a trivial ring is also a zero ring.
- A *Boolean ring* is a ring with identity such that the multiplication operation is idempotent. For example,  $\mathbb{Z}_2$  is a Boolean ring. All Boolean rings are commutative, and the only unit in a Boolean ring is 1.
- An element  $a$  of a ring  $R$  is called *regular* if there is an element  $b \in R$  such that  $a = aba$ . A ring  $R$  is called a *regular ring* if all elements of  $R$  are regular. All division rings and Boolean rings are regular rings.

A *division ring* or *skew field* is a ring with identity such that every nonzero element in the ring is a unit. A *field* is a commutative division ring. Therefore, for a field  $(F, +, \times)$ , both  $(F, +)$  and  $(F \setminus \{0\}, \times)$  are groups. Any finite commutative ring with more than one element and with no zero divisors is a field. A *integral domain* is a commutative ring with identity and with no zero divisors. Thus, every field is an integral domain, and any finite integral domain is a field.

Examples:

- $(\mathbb{R}, +, \times)$ ,  $(\mathbb{Q}, +, \times)$ , and  $(\mathbb{C}, +, \times)$  are fields, where  $+$  and  $\times$  are the usual addition and multiplication operations.  $\mathbb{R}$  is called the *field of real numbers*,  $\mathbb{Q}$  is called the *field of rational numbers*, and  $\mathbb{C}$  is called the *field of complex numbers*.
- $(\mathbb{Z}_n, +_n, \times_n)$  is a field if and only if  $n$  is prime. When  $n$  is prime, it is a commutative field.
- For a ring  $R$ , let  $R[n] = \{a + bn \mid a, b \in R\}$ . Then  $\mathbb{Z}[\sqrt{n}]$ ,  $\mathbb{Z}[i\sqrt{n}]$ ,  $\mathbb{Z}[i]$ ,  $\mathbb{Q}[\sqrt{n}]$ ,  $\mathbb{Q}[i\sqrt{n}]$ , and  $\mathbb{Q}[i]$  are all integral domains under the usual addition and multiplication, where  $n$  is a positive integer and  $i = \sqrt{-1}$ .  $\mathbb{Q}[\sqrt{n}]$ ,  $\mathbb{Q}[i\sqrt{n}]$ , and  $\mathbb{Q}[i]$  are also fields.

### 3.1 Subrings and Subfields

Let  $(R, +, \times)$  be a ring and  $R' \subseteq R$ . Then  $(R', +, \times)$  is a *subring* of  $(R, +, \times)$  if  $(R', +, \times)$  is a ring. In other words,  $(R', +)$  is a subgroup of  $(R, +)$ , and  $\times$  is closed on  $R'$ . If there is no ambiguity, we simply say that  $R'$  is a subring of  $R$ . For a ring  $R$ , its *trivial subrings* are  $\{0\}$  and  $R$ , and all other subrings are nontrivial. If  $F$  and  $F'$  are fields such that  $F'$  is a subring of  $F$ , then we say that  $F'$  is a *subfield* of  $F$ .

The following theorems are useful for determining subrings and subfields. Let  $R$  be a ring and  $R'$  be a nonempty subset of  $R$ . Then  $R'$  is a subring of  $R$  if and only if for all  $a, b \in R'$ , we have  $a - b, ab \in R'$ . Let  $F$  be a field and  $F'$

be a subset of  $F$  containing more than one element. Then  $F'$  is a subfield of  $F$  if and only if for all  $a, b \in F'$ , we have  $a - b, ab \in F'$ , and for all  $a \in F' \setminus \{0\}$ , we have  $a^{-1} \in F'$ .

Examples:

- Any subring of the ring of integers  $\mathbb{Z}$  has the form  $n\mathbb{Z}$ , where  $n$  is a nonnegative integer. If  $n \neq 1$ , then  $n\mathbb{Z}$  is without identity.
- $\mathbb{R}$  is a subfield of  $\mathbb{Q}$ , which is in turn a subfield of  $\mathbb{C}$ .
- Let  $R$  be a ring, and let  $R'$  and  $R''$  be subrings of  $R$ . Then  $R' \cap R''$  is also a subring of  $R$ . Let  $F$  be a field, and let  $F'$  and  $F''$  be subfields of  $F$ . Then  $F' \cap F''$  is also a subfield of  $F$ .

### 3.2 Characteristics

Let  $(R, +, \times)$  be a ring. If every element in the group  $(R, +)$  has finite order, then the *characteristic* of the ring  $R$  is defined as  $o(a)$ , where  $a \in R$  is the element with greatest additive order in  $(R, +)$ . Otherwise, the ring  $R$  is said to be of *characteristic zero*.

If  $R$  is a ring with identity, then  $R$  has positive characteristic  $n$  if and only if  $n$  is the least positive integer such that  $n1 = 0$ . If  $R$  is a finite ring, then the characteristic of  $R$  divides  $|R|$ . The characteristic of an integral domain is either zero or a prime integer.

The rings  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  have characteristic zero. The ring  $\mathbb{Z}_n$  has characteristic  $n$ .

### 3.3 Homomorphisms and Isomorphisms

Let  $(R_1, +_1, \times_1)$  and  $(R_2, +_2, \times_2)$  be rings. A function  $f : R_1 \rightarrow R_2$  is a *homomorphism* of  $R_1$  to  $R_2$  if for all  $a, b \in R_1$ , we have  $f(a +_1 b) = f(a) +_2 f(b)$  and  $f(a \times_1 b) = f(a) \times_2 f(b)$ . A homomorphism  $f$  of  $R_1$  to  $R_2$  is an *isomorphism* if  $f$  is a bijective function, in which case we say that  $R_1$  to  $R_2$  are *isomorphic*, and write  $R_1 \simeq R_2$ .

### 3.4 Polynomial Rings

Let  $R$  be a ring. Let  $R[x]$  denote the set of all infinite sequences  $(a_0, a_1, a_2, \dots)$ , where each  $a_i \in R$  and there exists a nonnegative integer  $n$  such that for all integers  $m \geq n$ ,  $a_m = 0$ . The elements of  $R[x]$  are called *polynomials* over  $R$ .

Let  $(a_0, a_1, a_2, \dots)$  and  $(b_0, b_1, b_2, \dots)$  be polynomials in  $R[x]$ . Define addition and multiplication to be  $(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$  and  $(a_0, a_1, a_2, \dots) \times (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$  where  $c_i = \sum_{j=0}^i a_j b_{i-j}$ . Then  $(R[x], +, \times)$  is a ring known as a *polynomial ring* or *ring of polynomials* over  $R$ .

Let  $a = ax^0$  denote  $(a, 0, 0, \dots)$ ,  $ax = ax^1$  denote  $(0, a, 0, \dots)$ ,  $ax^2$  denote  $(0, 0, a, \dots)$ , and so on. Then  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$ .

The symbol  $x$  is called the *indeterminate* over  $R$ , and  $a_i$  is called the *coefficient* of  $x^i$  in the polynomial  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ . The zero element of  $R[x]$  is  $0 = (0, 0, 0, \dots)$ . If  $R$  has an identity, then  $1 = (1, 0, 0, \dots)$  is the identity of  $R[x]$ . The polynomial  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  with  $a_n \neq 0$  is said to have *degree*  $n$ , and the polynomial  $0$  has no degree. The polynomials of degree zero have a bijective correspondence to  $R \setminus \{0\}$  and are called *scalars*. Two polynomials in  $R[x]$  are equal if and only if their coefficients of  $x^i$  are equal for all nonnegative integers  $i$ .

Note that if  $R$  is a commutative ring with identity, then  $R[x]$  is also a commutative ring with identity. Also, if  $R$  is an integral domain, then  $R[x]$  is also an integral domain.

## References

- [Malik et al., 1996] Malik, D. S., Mordeson, J. M., and Sen, M. K. (1996). *Fundamentals of Abstract Algebra*. McGraw-Hill Companies.