Groups, Rings, and Fields [2, 3, 1]

Yunghsiang S. Han

Dept. Computer Science and Information Engineering,
National Chi Nan University
Taiwan

E-mail: yshan@csie.ncnu.edu.tw

Groups

- If G is a nonempty set and $\circ$ is a binary operation on G, then $(G, \circ)$ is called a group if, and only if (*iff*) the following conditions are satisfied:
  1. for all $a, b \in G$, $a \circ b \in G$;
  2. for all $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$;
  3. there exists $e \in G$ with $a \circ e = e \circ a = a$ for all $a \in G$ (e is called an identity);
  4. for each $a \in G$ there is an element $b \in G$ such that $a \circ b = b \circ a = e$ (b is an inverse of a, vice versa).
- We denote the inverse of a as $-a$ (a^{-1}) and sometimes $a \circ b$ as ab.
- If $a \circ b = b \circ a$ for all $a, b \in G$, then G is called a commutative (abelian) group.

Example 1 $\mathbb{Z}_2 = \{0, 1\}$ *is a commutative group with*

$\circ$	0	1
0	0	1
1	1	0

Example 2 $\mathbb{Z}_7^* = \{1, 2, \ldots, 6\}$ *is a commutative group with*

$\circ$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- For any group G the number of elements in G is called the order of G (denoted by $|G|$).
- $|\mathbb{Z}_2| = 2$ and $|\mathbb{Z}_7^*| = 6$.
- For any group G,
  1. e is unique;
  2. the inverse of each element of G is unique;
  3. if $a, b, c \in G$ and $a \circ b = a \circ c$, then $b = c$;
  4. if $a, b, c \in G$ and $b \circ a = c \circ a$, then $b = c$.

The Integers Modulo n

- Let $n \in \mathbb{Z}^+$, $n > 1$. For $a, b \in \mathbb{Z}$, we say that a is congruent to b modulo n, and we write $a \equiv b \pmod{n}$, if $n | a - b$, or, $a = b + kn$ for some $k \in \mathbb{Z}$.
- Congruence modulo n is an equivalent relation on $\mathbb{Z}$.
- $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, where $[x]$ is the equivalent class $\{y | x \equiv y \pmod{n}\}$.
- For $[a], [b] \in \mathbb{Z}_n$, define $+$ and $\cdot$ by

$$[a] + [b] = [a+b] \text{ and } [a] \cdot [b] = [a][b] = [ab].$$

- For $n \in \mathbb{Z}^+$, $n > 1$, under the closed binary operation $+$ defined above, $\mathbb{Z}_n$ is a commutative group with identity $[0]$.
- For $n \in \mathbb{Z}^+$ and n is a prime, the closed binary operation $\cdot$ defined above, $\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}$ is a commutative group with identity $[1]$.

Proof: We only need to prove that for any $[a] \in \mathbb{Z}_n^*$, there is a $[b] \in \mathbb{Z}_n^*$ such that $[a][b] = [1]$. Since a is relative prime to n, we have $gcd(a, n) = 1$ and $ba + kn = 1$ for some $b, k \in \mathbb{Z}$. Then $ba \equiv 1 \pmod{n}$ and $[ba] = [b][a] = [1]$, where $[b] \in \mathbb{Z}_n^*$.

Subgroups

- **Example 3** *Let* $G = (\mathbb{Z}_6, +)$*. If* $H = \{0, 2, 4\} \subseteq G$*, then* $(H, +)$ *is a group with*

$+$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

- Let G be a group and $\emptyset \neq H \subseteq G$. If H is a group under the binary operation of G, then we call H a subgroup of G.
- If H is a nonempty subset of a group G, then H is a subgroup of G *iff* (a) for all $a, b \in H$, $ab \in H$ and (b) for all $a \in H$, $a^{-1} \in H$.

  Proof: (a) ($\Longrightarrow$) Trivial. (b) ($\Longleftarrow$) Prove that H has an identity. Since a and a^{-1} in H, $aa^{-1} = e \in H$.

- If G is a group and $\emptyset \neq H \subseteq G$, with H is finite, then H is a subgroup of G *iff* H is closed under the binary operation of G.

  Proof: (a) ($\Longrightarrow$) Trivial. (b) ($\Longleftarrow$) Let $a \in H$. Then $aH = \{ah | h \in H\} \subseteq H$. Since $(ah_1 = ah_2) \Longrightarrow (h_1 = h_2)$, $|aH| = |H|$. That is, $aH = H$ and there exists a b such that $ab = a$. Consequently, $b = e \in H$. Furthermore, there exists a c such that $ac = e$ and then $c = a^{-1} \in H$.

- Let $(G, \circ)$ and $(H, *)$ be groups. Define the binary operation $\cdot$ on $G \times H$ by $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$. Then $(G \times H, \cdot)$ is a group and is called the direct product of G and H.

  Example 4 *Let* $(\mathbb{Z}_2, +)$ *and* $(\mathbb{Z}_3, +)$ *be groups.* $G = \mathbb{Z}_2 \times \mathbb{Z}_3$ *defines* $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$.

Group Homomorphism and Group Isomorphism

- If $(G, \circ)$ and $(H, *)$ are groups and $f : G \longmapsto H$, then f is called a group homomorphism *iff* for all $a, b \in G$, $f(a \circ b) = f(a) * f(b)$.

  Example 5 *Let* $G = (\mathbb{Z}, +)$ *and* $H = (\mathbb{Z}_4, +)$. *Define* $f : G \longmapsto H$ *by* $f(x) = [x] = \{x + 4k | k \in \mathbb{Z}\}$. *Then*

  $$f(x + y) = [x + y] = [[x] + [y]] = f(x) + f(y)$$

  is a homomorphism.

- Let $(G, \circ)$ and $(H, *)$ be groups with respective identities e_G, and e_H. If f is a group homomorphism from G to H, then

  1. $f(e_G) = e_H$;
  2. $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$;

3. $f(a^n) = [f(a)]^n$ for all $a \in G$ and $n \in \mathbb{Z}$, where

$$a^n = \begin{cases} \underbrace{a \circ a \circ \cdots \circ a}_{ns\ a} & \text{when } 0 \leq n \\ (\underbrace{a \circ a \circ \cdots \circ a}_{-ns\ a})^{-1} & \text{when } 0 > n; \end{cases}$$

4. $f(S)$ is a subgroup of H for each subgroup S of G.

Example 6 *Let G, H be the groups and f the homomorphic function defined in Example 5. Let S be the subgroup in G such that $S = \{2n \mid n \in \mathbb{Z}\}$. Then $f(S) = \{[0], [2]\}$ is a subgroup of H.*

- If $f : (\boldsymbol{G}, \circ) \longmapsto (H, *)$ is a homomorphism, we call f an isomorphism *iff* it is one-to-one and onto. In this case, G and H are said to be isomorphic.
- An isomorphism from G to G is called an automorphism.

Example 7 *Let $f : (\mathbb{R}^+, \cdot) \longmapsto (\mathbb{R}, +)$, where $f(x) = \log_{10}(x)$.*

Then $f(a \cdot b) = \log_{10}(ab) = \log_{10} a + \log_{10} b = f(a) + f(b)$ *is a homomorphism. Since* f *is one-to-one and onto,* f *is an isomorphism.*

Example 8 *Let* G *be the group of complex numbers* $\{1, -1, i, -i\}$ *under multiplication with*

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Let $H = (\mathbb{Z}_4, +)$ *and* $f : G \longmapsto H$ *defined by*

$$f(1) = [0],\ f(-1) = [2],\ f(i) = [1],\ f(-i) = [3].$$

Then f is an isomorphism.

Example 9 *For fixed $a \in G$, define $f_a : G \longmapsto G$ by $f_a(b) = aba^{-1}$ for $b \in G$. Then f_a is an automorphism of G. The element b and aba^{-1} are said to be conjugate, and for a nonempty subset S of G the set $aSa^{-1} = \{asa^{-1} | s \in S\}$ is called a conjugate of S.*

Proof: we prove that f_a is an automorphism of G for any $a \in G$. Let b, c be any elements in G. First we have

$$f_a(bc) = abca^{-1} = ab(a^{-1}a)ca^{-1} = (aba^{-1})(aca^{-1}) = f_a(b)f_a(c).$$

Next we prove that f_a is one-to-one and onto. Assume that $f_a(b) = f_a(c)$. Then $aba^{-1} = aca^{-1}$. Consequently, $b = c$ and f_a is one-to-one. For any $b \in G$, there is an element in G such that $c = a^{-1}ba$. Hence, $f_a(c) = a(a^{-1}ba)a^{-1} = b$ and f_a is onto.

- (*) The kernel of the homomorphism $f : G \longmapsto H$ of the group G

into the group H is the set

$$\ker f = \{a \in G | f(a) = e_H\},$$

where e_H is the identity on H.

Example 10 *Let the groups G and H be defined as those in Example 5. Then* $\ker f = [0]$. *That is,* $\ker f = \{4n \mid n \in \mathbb{Z}\}$.

- (*) $\ker f$ is a subgroup of G
- (*) If $a \in G$ and $b \in \ker f$, then $aba^{-1} \in \ker f$.

  Proof: Since

$$\begin{aligned} f(aba^{-1}) &= f(a) * f(ba^{-1}) \\ &= f(a) * f(b) * f(a^{-1}) \\ &= f(a) * e_H * f(a^{-1}) \\ &= f(a) * f(a^{-1}) = f(aa^{-1}) = e_H, \end{aligned}$$

$aba^{-1} \in \ker f$.

- (*) The subgroup H of the group G is called a normal subgroup of G *iff* $aha^{-1} \in H$ for all $a \in G$ and all $h \in H$.
- (*) Clearly, every subgroup of an commutative group is normal since we have $aha^{-1} = aa^{-1}h = h \in H$.
- (*) The subgroup H of G is normal *iff* H is equal to its conjugates.
- (*) The subgroup H is normal *iff* aH is equal to Ha for every $a \in G$.

Cyclic Groups

- In the group G defined in Example 8, i generates all elements since $i^1 = i, i^2 = -1, i^3 = -i$, and $i^4 = 1$.
- A group G is called cyclic *iff* there is an element $x \in G$ such that for each $a \in G,\ a = x^n$ for some $n \in \mathbb{Z}$.

  Example 11 $(\mathbb{Z}_4, +)$ *is cyclic and* $[1]$ *generates all elements.*

- If G is a group and $a \in G$, the order of a, denoted $o(a)$, is $| < a > |$, where

  $$< a >= \{a^k | k \in \mathbb{Z}\}.$$

  We can define n is the smallest positive integer such that $a^n = e$. Then $o(a) = n$.

  Example 12 *Let G be the group defined in Example 8. Then* $o(i) = 4,\ o(1) = 1,\ o(-1) = 2,$ *and* $o(-i) = 4$.

- Let G be a group. For all $a \in G$. $< a >$ is a subgroup of G.
- Let $a \in G$ with $o(a) = n$. If $k \in \mathbb{Z}$ and $a^k = e$, then $n|k$.

  Proof: $k = qn + r,\ 0 \leq r < n$. Then

  $$a^k = a^{qn+r} = a^{qn}a^r = ea^r = a^r = e.$$

  Since $r < n$ and $o(a) = n$, then $r = 0$.
- Let G be a cyclic group.
  1. If $|G|$ is infinite, then G is isomorphic to $(\mathbb{Z}, +)$.
  2. If $|G| = n$, where $n > 1$, then G is isomorphic to $(\mathbb{Z}_n, +)$.
- (*) Every subgroup of a cyclic group is cyclic.

  Proof: Let $H \neq \{e\}$ be a subgroup of a cyclic group $< a >$. If $a^j \in H$, then $a^{-j} \in H$. Therefore, H contains at least one power of a with positive exponent. Assume that d is the least positive exponent such that $a^d \in H$. Let $a^s \in H$. Dividing s by d gives

$s = qd + r,\ 0 \le r < d$, and $q, r \in \mathbb{Z}$. Since $a^s(a^{-d})^q = a^r \in H$, r must be zero otherwise d is not the least positive exponent of a in H. Therefore, the exponents of all powers of a that belong to H are divisible by d, and so $H =< a^d >$.

- (*) In a finite cyclic group $< a >$, the element a^k generates a subgroup of order $o(a)/gcd(k, o(a))$.

  Proof: Let d be the least positive number such that $(a^k)^d = e$. Hence, $o(a)|kd$. It is clear $d = o(a)/gcd(o(a), k)$.

- (*) Let f be a positive divisor of $o(a)$ of a finite cyclic group $< a >$. Then $< a >$ contains exactly $\phi(f)$ elements of order f, where $\phi(f)$ is Euler's function and indicates the number of integers n with $1 \le n \le f$ that are relatively prime to f.

  Proof: Assume that $df = o(a)$. Then by previously result $d = gcd(o(a), k)$ for some $1 \le k \le o(a)$. Clearly, $gcd(k/d, f) = 1$.

Since $1 \le k \le df$, $1 \le k/d \le f$. The possible number of k is clearly the possible number of k/d and then is $\phi(f)$.

Example 13 *$(\mathbb{Z}_8, +)$ is a cyclic group with order 8. The subgroup $< 6 >$ is with order $8/gcd(8, 6) = 4$. In deed $< 6 >= \{6, 4, 2, 0\}$. Since $\phi(4) = 2$, there are two elements in $(\mathbb{Z}_8, +)$ with order 4. The other one is $< 2 >= \{2, 4, 6, 0\}$.*

- (*) A finite cyclic group $< a >$ contains $\phi(o(a))$ generators, that is, elements a^r such that $< a^r >=< a >$. The generators are the powers of a^r with $gcd(r, o(a)) = 1$.

Cosets

- If H is a subgroup of G, then for any $a \in G$ the set $aH = \{ah|h \in H\}$ is called a left coset of H in G. The set $Ha = \{ha|h \in H\}$ is a right coset of H in G.

  Example 14 *For* $G = (\mathbb{Z}_{12}, +)$ *and* $H = \{[0], [4], [8]\}$,

$$\begin{aligned} [0] + H &= H \\ [1] + H &= \{[1], [5], [9]\} \\ [2] + H &= \{[2], [6], [10]\} \\ [3] + H &= \{[3], [7], [11]\} \end{aligned}$$

- If H is a subgroup of the finite group G, then for all $a, b \in G$ (a) $|aH| = |H|$ (b) $aH = bH$ or $aH \cap bH = \emptyset$.

  Proof: (a) Since $aH = \{ah|h \in H\}$, $|aH| \le |H|$. If $|aH| < |H|$, then there exists h_i and h_j, $h_i \ne h_j$ such that $ah_i = ah_j$. This results in $h_i = h_j$, contradiction.

(b) Assume that $aH \cap bH \neq \emptyset$. Let $c \in aH \cap bH$. Then $c = ah_i = bh_j$, $h_i, h_j \in H$. Thus, $a = bh_j h_i^{-1} = bh'$. For any $x \in aH$, $x = ah = bh'h \in bH$. Consequently, $aH \subseteq bH$. Similarly, $bH \subseteq aH$. Hence, $aH = bH$.

- Let G be a finite group and H be a subgroup of G. By the above result, all left (right) cosets of H partition G.

Lagrange's Theorem

- If G is a finite group of order n with H a subgroup of order m, then m divides n, i.e., $m|n$.
- If G is a finite group and $a \in G$, then $o(a)|\ |G|$.
- Any group of prime order is cyclic.

Rings

- Let R be a nonempty set on which we have two closed binary operations, denoted by $+$ and $\cdot$. Then $(R, +, \cdot)$ is a ring *iff* for $a, b, c \in R$, the following conditions are satisfied:
  1. $(R, +)$ is a commutative group;
  2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
  3. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

  Example 15 $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, *and* $(\mathbb{C}, +, \cdot)$ *are rings.*
- Let $(R, +, \cdot)$ be a ring with the additive identity (or zero) z.
  1. If $ab = ba$ for all $a, b \in R$, then R is called a commutative ring.
  2. The ring R is said to have no proper divisors of zero if for any $a, b \in R$, $(ab = z) \Longrightarrow (a = z \text{ or } b = z)$.
  3. If an element $u \in R$ such that $u \neq z$ and $au = ua = a$ for all $a \in R$, we call u a unity, or multiplicative identity of R.

Sometimes u is denoted by 1.

Example 16 *Let $M_2(\mathbb{Z})$ denote the set of all 2×2 matrices with integer entries. $M_2(\mathbb{Z})$ is a noncommutative ring. The unity is*

$$u = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and additive identity

$$z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

$M_2(\mathbb{Z})$ has proper divisors of zero since, for example,

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} = z$$

Example 17 *Prove that* $(\mathbb{Z}, \oplus, \odot)$ *is a ring, where*

$$x \oplus y = x + y - 1,\ x \odot y = x + y - xy.$$

Proof: (in part)

1. $x \oplus y = x + y - 1 = y + x - 1 = y \oplus x$.
2. $a + z - 1 = a$ *and then* $z = 1$.
3. $b = 2 - a$ *is the additive inverse of* a *since* $a \oplus b = 1$.
4.

$$\begin{aligned} a \odot (b \oplus c) &= a + (b \oplus c) - a(b \oplus c) \\ &= a + b + c - 1 - a(b + c - 1) \\ &= (a + b - ab) + (a + c - ac) - 1 \\ &= (a \odot b) \oplus (a \odot c) \end{aligned}$$

5. *DIY, prove that* 0 *is the unity.*

Example 18 *Let $U = \{1, 2\}$ and $R = P(U)$, the power set of U. Define*

$$\begin{aligned} A + B &= \{x | x \in A \text{ or } x \in B, \text{but not both}\} = (A \cup B) \setminus (A \cap B) \\ A \cdot B &= A \cap B \end{aligned}$$

Then $(R, +, \cdot)$ is a ring.

- Let R be a ring with unity u. If $a, b \in R$, and $ab = ba = u$, then b is called a multiplicative inverse of a and a is called a unit of R.
- In any ring $(R, +, \cdot)$,
  1. the zero element z is unique;
  2. the additive inverse of each ring element is unique.
- (Cancellation Law) Let $(R, +, \cdot)$ be a ring. For all $a, b, c \in R$,
  1. $(a + b = a + c) \Longrightarrow (b = c)$;
  2. $(b + a = c + a) \Longrightarrow (b = c)$.

- For any ring $(R, +, \cdot)$ and $a \in R$, we have $az = za = z$.

  Proof: $az = a(z + z) = az + az$ and $z + az = az = az + az$. By the cancellation law, we have $z = az$.

- For any ring $(R, +, \cdot)$ and for any $a, b \in R$,

  1. -(-a)=a;
  2. a(-b)=(-a)b=-(ab);
  3. (-a)(-b)=ab.

- A function $\varphi : R \longmapsto S$ from a ring $(R, +, \cdot)$ into a ring $(S, \oplus, \odot)$ is called a homomorphism *iff* for any $a, b \in R$, we have

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b) \text{ and } \varphi(a \cdot b) = \varphi(a) \odot \varphi(b).$$

- (*) The set

$$\ker \varphi = \{a \in R | \varphi(a) = 0 \in S\}$$

  is called the kernel of φ. Other concepts, such as that of an isomorphism, are analogous to those for groups.

Subrings and Ideals

- A subset S of a ring R is called a subring of R if S is also a ring under the operations of R.
- A subset J of a ring R is called an ideal if J is a subring of R and for all $a \in J$ and $r \in R$ we have $ar \in J$ and $ra \in J$.

  Example 19 $(\mathbb{Z}, +, \cdot)$ *is a subring of* $(\mathbb{Q}, +, \cdot)$ *but not an ideal since, for example,* $1 \in \mathbb{Z}, 1/2 \in Q$, *but* $1 \cdot 1/2 = 1/2 \notin \mathbb{Z}$.

  Example 20 *It is clear that* $(n\mathbb{Z}, +, \cdot)$ *is a subring of* $(\mathbb{Z}, +, \cdot)$, *where*
  $$n\mathbb{Z} = \{nz | z \in \mathbb{Z}\}$$
  and $n \neq 0$. *Then* $(n\mathbb{Z}, +, \cdot)$ *is an ideal.*
- Let R be a commutative ring. Then the smallest ideal containing a given element $a \in R$ is the ideal $(a) = \{ra + na | r \in R, n \in \mathbb{Z}\}$,

where

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{ns\ \ a} & \text{if } n \geq 0 \\ -(\underbrace{a + a + \cdots + a}_{ns\ \ a}) & \text{otherwise.} \end{cases}$$

If R contains an unity, then $(a) = \{ra | r \in R\}$.

Proof:

1. We prove that (a) is a ring. DIY.
2. We prove that (a) is an ideal. For any $b \in (a)$ and any $r \in R$ we need to prove that $rb \in (a)$. Since $b = r'a + na$ for some $r' \in R$ and $n \in \mathbb{Z}$, we have

$$rb = r(r'a + na) = (rr')a + n(ra).$$

Since $ra \in (a)$, we have $ra = r''a + n'a$ for some $r'' \in R$ and

$n' \in \mathbb{Z}$. Hence,

$$rb = (rr')a + n(r''a + n'a) = (rr' + nr'')a + (nn')a \in (a).$$

Therefore, (a) is an ideal.

3. We prove that (a) is the smallest ideal containing a. Let J_a be any ideal containing a. Let $x \in (a)$. Then $x = ra + na$ for some $r \in R$ and $n \in \mathbb{Z}$. Since $a \in J_a$ and J_a is an ideal, $ra \in J_a$ and $na \in J_a$. Consequently, $ra + na \in J_a$ which implies that $x \in J_a$. Hence, we have $(a) \subseteq J_a$ and then (a) is the smallest ideal containing a.
4. If $u \in R$, then

$$\begin{aligned} na &= \underbrace{au + au + \cdots + au}_{ns\ au} \\ &= a(nu) = ar', \end{aligned}$$

where $r' = nu \in R$ and $n \geq 0$. Thus, for any $x \in (a)$,

$$x = ra + na = ra + r'a = (r + r')a = r''a.$$

If $n < 0$, $na = -ar'$ and hence $x = (r - r')a = r'''a$. Therefore, $(a) \subseteq \{ra|r \in R\}$. It is clear that $\{ra|r \in R\} \subseteq (a)$. Hence, $(a) = \{ra|r \in R\}$.

- If R is a ring with unity, and J is an ideal of R containing a unit, then $J = R$.

  Proof: Assume that $u \in J$ is a unit in R. Then the condition $aJ \subseteq J$ for all $a \in R$ implies that $1 = u^{-1}u$ is in J. Since $a1 \in J$ for all $a \in R$, $J = R$.

- Let R be a commutative ring. An ideal J of R is said to be principal *iff* there is an $a \in R$ such that $J = (a)$. In this case J is also called the principal ideal generated by a.

Integral Domains and Fields

- Let R be a commutative ring with unity. Then
  1. R is called an integral domain *iff* R has no proper divisors of zero;
  2. R is called a field *iff* every nonzero element of R is a unit.

  Example 21

	integral domain	field
$(\mathbb{Z}, +, \cdot)$	$\surd$	
$(\mathbb{Q}, +, \cdot)$	$\surd$	$\surd$
$(\mathbb{R}, +, \cdot)$	$\surd$	$\surd$

- Let $(R, +, \cdot)$ be a commutative ring with unity. Then R is an integral domain *iff*, for any $a, b \in R$, whenever $a \neq z$, $(ab = ac) \Longrightarrow (b = c)$.

Proof:

1. ($\Longrightarrow$) Assume that $(R, +, \cdot)$ is an integral domain. Then for any $a, b \in R$, $(ab = z) \Longrightarrow (a = z \text{ or } b = z)$. Assume that $ab = ac$ where $a \neq z$. then $ab + (-ac) = z$ and then $a(b - c) = z$. Since $a \neq z$, then $b - c = z$. That is $-c$ is the inverse of b. So $b = c$.
2. ($\Longleftarrow$) Assume that for any $a, b, c \in R$, where $a \neq z$, $(ab = ac) \Longrightarrow (b = c)$. Assume that $ab = z$. If $a = z$ we have done. Now let $a \neq z$. Since $az = z$ we have $ab = az$. Thus, $b = z$.

- Every finite integral domain R is a field.

  Proof: We must prove that if $a \in R$ and $a \neq 0$, there exists $b \in R$ such that $a \cdot b = u$, where u is the unity of R. Consider that $aR = \{a \cdot r | r \in R\} \subseteq R$. Then $|aR| \leq |R|$. If $|aR| < |R|$, we have $r_1 \neq r_2$, $r_1, r_2 \in R$ such that $a \cdot r_1 = a \cdot r_2$. Since R is an integral domain, we have $r_1 = r_2$. Contradiction. Hence $aR = R$ and there exists some b such that $a \cdot b = u$.

- If $(F, +, \cdot)$ is a field, then it is an integral domain.
- For $n \in \mathbb{Z}^+$, $n > 1$, under the closed binary operations defined for the integers modulo n, $\mathbb{Z}_n$ is a commutative ring with unity [1].

Example 22 $\mathbb{Z}_5$ *is also a field, where*

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- $\mathbb{Z}_n$ is a field *iff* n is a prime.

  Proof:

  1. ($\Longleftarrow$) Let n be a prime. then for all $0 < a < n$, $gcd(a, n) = 1$. Consequently, $sa + tn = 1$ and $sa \equiv 1 \pmod{n}$, or $[a][s] = [1]$.
  2. ($\Longrightarrow$) Assume that n is not a prime. then $n = n_1 n_2$, $0 < n_1, n_2 < n$. It is clear that $[n_1] \neq [0] \neq [n_2]$. Since $[n_1][n_2] = [0]$, $\mathbb{Z}_n$ is not an integral domain. Therefore, $\mathbb{Z}_n$ is not a field.

- In $\mathbb{Z}_n$, $[a]$ is a unit *iff* $gcd(a, n) = 1$.

  Example 23 *Find* $[25]^{-1}$ *in* $\mathbb{Z}_{72}$.

  Since $gcd(25, 72) = 1$, *by Euclidean algorithm,*

$$\begin{aligned} 72 &= 2(25) + 22 \\ 25 &= 1(22) + 3 \end{aligned}$$

$$22 = 7(3) + 1.$$

Thus,

$$\begin{aligned} 1 &= 22 - 7(3) = 22 - 7(25 - 22) \\ &= (-7)(25) + 8(22) \\ &= (-7)(25) + 8[72 - 2(25)] \\ &= 8(72) - 23(25). \end{aligned}$$

$$[25]^{-1} = [-23] = [49].$$

Polynomials

- Let R be an arbitrary ring. A polynomial over R is an expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where n is a nonnegative integer, the coefficients a_i, $0 \le i \le n$, are elements in R, and x is a symbol not belonging to R, called an indeterminate over R.

- The polynomials

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ and } g(x) = \sum_{i=0}^{n} b_i x^i$$

over R are equal *iff* $a_i = b_i$, for $0 \le i \le n$.

- Define the sum of $f(x)$ and $g(x)$ by

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)x^i.$$

- Let

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ and } g(x) = \sum_{j=0}^{m} b_j x^j.$$

Define the product of two polynomials over R by

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k,$$

where

$$c_k = \sum_{\substack{i+j=k \\ 0 \le i \le n, 0 \le j \le m}} a_i b_j.$$

- The ring formed by the polynomials over R with the above operations is called the polynomial ring over R and denoted by $R[x]$.

- The zero in $R[x]$ is the polynomial with all coefficients to be zero.
- Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial over R with $a_n \neq 0$. Then a_n is called the leading coefficient of $f(x)$ and $n = deg(f(x)) = deg(f)$ is the degree of $f(x)$. By convention, we set $deg(0) = -\infty$, where 0 is the zero in $R[x]$. Polynomials of degree ≤ 0 are called constant polynomials. If R has the unity u (1) and if the leading coefficient of $f(x)$ is 1, then $f(x)$ is called a monic polynomial.

Some Basic Properties of $R[x]$

- Let $f(x), g(x) \in R[x]$. Then

$$deg(f(x)+g(x)) \leq \max\{deg(f), deg(g)\},$$

$$deg(fg) \leq deg(f)+deg(g).$$

If R is an integral domain, we have $deg(fg) = deg(f)+deg(g)$.

- Let R be a ring. Then
  1. $R[x]$ is communicative *iff* R is communicative;
  2. $R[x]$ is a ring with unity *iff* R has an unity;
  3. $R[x]$ is an integral domain *iff* R is an integral domain.
- If F is a field, then $F[x]$ is an integral domain but not a field. This can be verified by noting that x is not a unit in $F[x]$ since there is no polynomial $f(x) \in F[x]$ such that $xf(x) = 1$.

The Evaluation Homomorphisms

- Let F be a subfield of a field E, let α be any element of E, and let x be an indeterminate. The function $\phi_\alpha : F[x] \longmapsto E$ defined by

$$\phi_\alpha(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

for $(a_0 + a_1 x + \cdots + a_n x^n) \in F[x]$ is a homomorphism of $F[x]$ into E. Also, $\phi_\alpha(x) = \alpha$, and ϕ_α maps F isomorphically by the identity function; that is, $\phi_\alpha(a) = a$ for $a \in F$. The homomorphism ϕ_α is evaluation at α.

Example 24 *Let F be $\mathbb{Q}$ and E be $\mathbb{R}$. Consider the evaluation homomorphism $\phi_\alpha : \mathbb{Q}[x] \longmapsto \mathbb{R}$, where*

$$\phi_2(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 2 + \cdots + a_n 2^n.$$

Note that

$$\phi_2(x^2 + x - 6) = 2^2 + 2 - 6 = 0.$$

Thus, $x^2 + x - 6$ *is in the ker* ϕ_2*. Of course,*

$$x^2 + x - 6 = (x - 2)(x + 3),$$

and the reason that $\phi_2(x^2 + x - 6) = 0$ *is that* $\phi_2(x - 2) = 2 - 2 = 0$*.*

Example 25 *Let* F *be* $\mathbb{Q}$ *and* E *be* $\mathbb{C}$*. Consider the evaluation homomorphism* $\phi_i : \mathbb{Q}[x] \longmapsto \mathbb{C}$*, where*

$$\phi_i(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 i + \cdots + a_n i^n,$$

and $\phi_i(x) = i$*. Note that*

$$\phi_i(x^2 + 1) = i^2 + 1 = 0,$$

so $x^2 + 1$ *is in the ker* ϕ_i*.*

Example 26 *Let* F *be* $\mathbb{Q}$ *and let* E *be* $\mathbb{R}$*. Consider the* *evaluation homomorphism* $\phi_\pi : \mathbb{Q}[x] \longmapsto \mathbb{R}$, *where*

$$\phi_\pi(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\pi + \cdots + a_n\pi^n.$$

It can be proved that $a_0 + a_1\pi + \cdots + a_n\pi^n = 0$ *iff* $a_i = 0$ *for* $i = 0, 1, \ldots, n$. *Thus, ker* ϕ_π *is* $\{0\}$, *and* ϕ_π *is a one-to-one function. This shows that all formal polynomials in* π *with rational coefficients form a ring isomorphic to* $\mathbb{Q}[x]$ *in a natural way with* $\phi_\pi(x) = \pi$.

- Let F be a subfield of a field E, and let α be an element of E. Let $f(x) = \sum_{i=0}^{n} a_ix^i \in F[x]$, and let $\phi_\alpha : F[x] \longmapsto E$ be the evaluation homomorphism. Let $f(\alpha)$ denote

$$\phi_\alpha(f(x)) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

If $f(\alpha) = 0$, then α is a zero of $f(x)$.

Example 27 *To find all real solutions of the polynomial* *equation* $r^2 + r - 6 = 0$ *one may let* $F = \mathbb{Q}$ *and* $E = \mathbb{R}$ *and find all* $\alpha \in \mathbb{R}$ *such that*

$$\phi_\alpha(x^2 + x - 6) = 0,$$

that is, find all zeros of $x^2 + x - 6$ *in* $\mathbb{R}$. *both have the same answer since*

$$\{\alpha \in \mathbb{R} \mid \phi_\alpha(x^2+x-6) = 0\} = \{r \in \mathbb{R} \mid r^2+r-6 = 0\} = \{2, -3\}.$$

The Division Algorithm in $F[x]$

- If there exists a polynomial $h(x) \in F[x]$ such that $f(x) = g(x)h(x)$, where $f(x), g(x) \in F[x]$, then the polynomial $g(x)$ divides the polynomial $f(x)$.
- (Division Algorithm) Let $g(x) \neq 0$ be a polynomial in $F[x]$. Then for any $f(x) \in F[x]$ there exists unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x),$$

where $deg(r) < deg(g)$.

Proof: Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$, where $deg(f) = n$ and $deg(g) = m$. Consider the set $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$. Let $r(x)$ be an element of minimal degree in S. Then

$$f(x) = q(x)g(x) + r(x)$$

for some $q(x) \in F[x]$. We must show that $deg(r) < deg(g) = m$. Suppose that

$$r(x) = \sum_{i=0}^{t} c_i x^i,$$

with $c_i \in F$ and $c_t \neq 0$ if $t \neq 0$. If $t \geq m$, then

$$f(x) - q(x)g(x) - \left(\frac{c_t}{b_m}\right) x^{t-m} g(x) = r(x) - \left(\frac{c_t}{b_m}\right) x^{t-m} g(x),$$

and the latter is of the form

$$r(x) - (c_t x^t + \text{ terms of lower degree}),$$

which is a polynomial of degree lower than t, the degree of $r(x)$.

However, the polynomial above can be written in the form

$$f(x) - g(x)\left[q(x) + \left(\frac{c_t}{b_m}\right)x^{t-m}\right],$$

so it is in S, contradicting the fact that $r(x)$ was selected to have minimal degree in S. Thus $deg(r) < m$. For uniqueness, DIY.

Example 28 *Consider* $f(x) = 2x^5 + x^4 + 4x + 3 \in \mathbb{Z}_5[x]$,$g(x) = 3x^2 + 1 \in \mathbb{Z}_5[x]$. *We compute the polynomials* $q(x), r(x) \in \mathbb{Z}_5[x]$ *with* $f(x) = q(x)g(x) + r(x)$ *and* $q(x) = 4x^3 + 2x^2 + 2x + 1$, *and* $r(x) = 2x + 2$,. *Obviously,* $deg(r) < deg(g)$.

- An element $a \in F$ is a zero of $f(x) \in F[x]$ *iff* $x - a$ is a factor of $f(x)$ in $F[x]$.

  Proof: (a) ($\Longrightarrow$) Assume that for $a \in F$ we have $f(a) = 0$. By

Division Algorithm, there exist $q(x),\ r(x) \in F[x]$ such that

$$f(x) = q(x)(x-a) + r(x),$$

where $deg(r) < 1$. Then we have $r(x) = c$ for $c \in F$, so

$$f(x) = q(x)(x-a) + c.$$

Applying the evaluation homomorphism, $\phi_a : F[x] \longmapsto F$, we find

$$0 = f(a) = q(a)0 + c,$$

so it must be that $c = 0$. Then $f(x) = q(a)(x-a)$.

(b) ($\Longleftarrow$) If $x-a$ is a factor of $f(x)$ in $F[x]$, where $a \in F$, then applying the evaluation homomorphism ϕ_a to $f(x) = q(x)(x-a)$, we have $f(a) = q(a)0 = 0$.

- A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

Irreducible Polynomials

- A nonconstant polynomial $f(x) \in F[x]$ is irreducible over F or is an irreducible polynomial in $F[x]$ *iff* $f(x)$ can not be expressed as a product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than the degree of $f(x)$.
- A polynomial $f(x)$ may be irreducible over F, but may not be irreducible if viewed over a larger field E containing F.

  Example 29 *Let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$. However, $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ is not irreducible in $\mathbb{R}[x]$.*
- The units in $F[x]$ are precisely the nonzero elements of F. We may define an irreducible polynomial $f(x)$ as a nonconstant polynomial such that in any factorization $f(x) = g(x)h(x)$ in $F[x]$, either $g(x)$ or $h(x)$ is a unit.

Example 30 *Let us show that* $f(x) = x^3 + 3x + 2$ *viewed in* $\mathbb{Z}_5[x]$ *is irreducible over* $\mathbb{Z}_5$*. If* $x^3 + 3x + 2$ *can be factorized in* $\mathbb{Z}_5[x]$*, then there exist at least one linear factor of* $f(x)$ *of the form* $x - a$ *for some* $a \in \mathbb{Z}_5$*. Thus,* $f(a) = 0$*. But*

$$f(0) = 2,\ f(1) = 1,\ f(2) = 1,\ f(3) = 3,\ \textit{and}\ f(4) = 3,$$

$f(x)$ *has no zeros in* $\mathbb{Z}_5$*.*

- Let $f(x) \in F[x]$, and let $1 \leq deg(f) \leq 3$. then $f(x)$ is reducible over F *iff* it has a zero in F.

Ideal Structure in $F[x]$

- If F is a field, every ideal in $F[x]$ is principal.

  Proof: Let J be an ideal of $F[x]$. If $J = \{0\}$, then $J = (0)$. Assume that $J \neq \{0\}$, and let $g(x)$ be a nonzero element of J of minimal degree. If the degree of $g(x)$ is zero, then $g(x) \in F$ and is a unit, so $J = F[x] = (1)$ and is principal. If the degree of $g(x)$ is greater than and equal to 1, let $f(x)$ be any element of J. Then by Division Algorithm

  $$f(x) = q(x)g(x) + r(x),$$

  where $deg(r) < deg(g)$. Since $f(x) \in J$ and $g(x) \in J$, $f(x) - q(x)g(x) = r(x) \in J$ by the definition of ideal. Hence, $r(x) = 0$ otherwise $g(x)$ is not a minimal degree polynomial in J. Thus $f(x) = q(x)g(x)$ and $J = (g(x))$.

- $F[x]$ is a principal ideal domain. In fact, for every ideal $J \neq (0)$

of $F[x]$ there exists a uniquely determined monic polynomial $g(x) \in F[x]$ with $J = (g(x))$.

Uniqueness of Factorization in $F[x]$

- Let $f_1(x), f_2(x), \ldots, f_n(x)$ be polynomials in $F[x]$ not all of which are 0. Then there exists a uniquely determined monic polynomial $d(x) \in F[x]$ with the following properties:
  1. $d(x)$ divides each $f_i(x)$, $1 \leq i \leq n$;
  2. any polynomial $g(x) \in F[x]$ dividing each $f_i(x)$, $1 \leq i \leq n$, divides $d(x)$;
  3. $d(x)$ can be expressed in the form
  $$d(x) = b_1(x)f_1(x) + \cdots + b_n(x)f_n(x),$$
  where $b_i(x) \in F[x]$ for $1 \leq i \leq n$.

  Proof: The set J containing of all polynomials of the form
  $$c_1(x)f_1(x) + \cdots + c_n(x)f_n(x),$$
  where $c_1(x), c_2(x), \ldots, c_n(x) \in F[x]$ is easily seen to be an ideal

of $F[x]$. Since not all $f_i(x)$ are 0, we have $J \neq \{0\}$, and $J = (d(x))$ for some monic polynomial $d(x) \in F[x]$. Since $d(x) \in J$, all results follow immediately except the uniqueness. For uniqueness, DIY.

- Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.
- Let F be a field. Then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit (that is, nonzero constant) factors in F.

  Proof: Let $f(x) \in F[x]$ be a nonconstant polynomial. If $f(x)$ is not irreducible, then $f(x) = g(x)h(x)$, with the degree of $g(x)$ and the degree of $h(x)$ both less than degree of $f(x)$. If $g(x)$ and $h(x)$ are both irreducible, we stop here. If not, at least one of them factors into polynomials of lower degree. Continuing this process, we arrive at a factorization

$$f(x) = p_1(x)p_2(x)\cdots p_r(x),$$

where $p_i(x)$ is irreducible for $i = 1, 2, \ldots, r$.
Suppose that

$$f(x) = p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x)$$

are two factorizations of $f(x)$ into irreducible polynomials and $s \geq r$. Then $p_1(x)$ divides some $q_j(x)$, let assume $q_1(x)$. Since $q_1(x)$ is irreducible,

$$q_1(x) = u_1p_1(x),$$

where $u_1 \neq 0$ and is a unit in F. Then substituting $u_1p_1(x)$ for $q_1(x)$ and cancelling, we get

$$p_2(x)p_3(x)\cdots p_r(x) = u_1q_2(x)\cdots q_s(x).$$

By a similar argument, we eventually arrive at

$$1 = u_1 u_2 \cdots u_r q_{r+1}(x) \cdots q_s(x).$$

Clearly, this is only possible if $s = r$, so that this equation is actually $1 = u_1 u_2 \cdots u_r$. Thus, the irreducible factors $p_i(x)$ and $q_j(x)$ were the same except possibly for order and unit factors.

References

[1] J. B. Fraleigh, *A First Course in Abstract Algebra*. Reading, Mass: Addison-Wesley Publishing Company, fourth edition, 1989.

[2] R. P. Grimaldi, *Discrete and Combinatorial Mathematics– An Applied Introduction*. Reading, Mass: Addison-Wesley, fourth edition, 1999.

[3] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge, UK: Cambridge University Press, revised edition, 1994.