

## 1 Beginning

**Definition 1.1.** A **group** is a pairing of a set and a binary operation such that the operation is associative, and each element of the set has both an inverse and an identity.

*Remark 1.1.1.* Considering an identity element is defined both as a left and a right identity, it can be proven that it is unique for the group.

*Remark 1.1.2.* Considering the binary operation is well defined, it can be proven that the inverse is distinct for every element of the set.

**Definition 1.1.1.** A **commutative group** is a group where the binary operation is commutative.

**Definition 1.2.** A **ring** is a commutative group with another operation defined such that the two operations are similar to “addition” and “multiplication” of the integers. The multiplication operation must be associative and distributive.

**Definition 1.2.1.** A **commutative ring** is a ring where multiplication is commutative.

**Definition 1.2.2.** We say that a ring has **unity** if there is a multiplicative identity.

*Remark 1.2.1.* For any ring  $R$  with additive identity  $0$ , it can be proven that  $0a = 0$  for all  $a \in R$ .

*Remark 1.2.2.* Using Remark 1.2.1, it can be proven that  $-ab = (-a)b = a(-b)$  for all  $a, b \in R$ .

**Definition 1.2.3.** For some non-zero  $a, b \in R$ , we say  $a$  and  $b$  are **zero divisors** if  $ab = 0$ .

*Remark 1.2.3.* For some non-zero  $a \in R$ , it can be proven that  $a$  is a left zero divisor if and only if there exists non-zero  $b, c \in R$  such that  $b \neq c$  and  $ab = ac$ .

*Remark 1.2.4.* It follows from Remark 1.2.3, that if a ring  $R$  does *not* have any zero divisors, then  $ab = ac \implies b = c$  for all  $a, b, c \in R$  and  $a \neq 0$ .

**Definition 1.2.4.** A **unit** in a ring with unity is an element which has a multiplicative inverse.

*Remark 1.2.5.* A unit cannot be a zero-divisor.

**Definition 1.3.** An **integral domain** is a commutative ring with unity and no zero divisors.

**Definition 1.4.** A **field** is a commutative ring where every non-zero element is a unit, and the additive and multiplicative identities are not equal.

## 2 Developing

**Definition 2.1.** The **characteristic** of a ring is the lowest integer  $c$  such that  $\underbrace{1 + 1 + \cdots + 1}_{c \text{ times}} = 0$ .

**Theorem 2.1.1.** *If the characteristic of a ring is composite, it must have zero divisors.*

*Proof.* Let  $c$  be the characteristic of some ring where there exists positive integers  $m, n$  such that  $c = mn$  and  $m, n < c$ . Consider, using the distributivity of multiplication, that  $\underbrace{(1 + 1 + \cdots + 1)}_{m \text{ times}} \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ times}} = 0$ .  $\square$

**Theorem 2.1.2** (Euler's Theorem). *Let  $R^*$  be the finite set of the units in a ring. For all  $a \in R^*$ ,  $a^{|R^*|} = 1$ .*

*Proof.* We have  $R^* = \{r_1, \dots, r_n\} = \{ar_1, \dots, ar_n\}$  since multiplication is one-to-one. Then,  $r_1 \cdots r_n = (ar_1) \cdots (ar_n) = a^n(r_1 \cdots r_n) \implies a^n = 1$ .  $\square$

**Theorem 2.1.3.** *For a finite ring with unity, any element is either 0, a zero divisor, or a unit.*

*Proof.* For an element  $r$  that is not zero or a zero divisor, we have the following set of non-zero elements  $\{r, r^2, \dots\}$ . Since the ring is finite, we have  $r^{e_1} = r^{e_2}$  for some  $e_1 < e_2$ . Then,  $r^{e_1} = r^{e_2} = r^{e_1} r^{e_2 - e_1} \implies r^{e_2 - e_1} = 1$ . Therefore,  $r \cdot r^{e_2 - e_1 - 1} = 1$ .  $\square$

*Remark 2.1.1.* Theorem 2.1.3 shows every finite integral domain is a field.

**Definition 2.2.** A **quadratic ring extension**  $R[\gamma]$  of some ring  $R$  is created by adding an element  $\gamma$  to  $R$  such that  $\gamma^2 = c$  for some  $c \in R$  and  $\gamma \notin R$ .

*Remark 2.2.1.* Elements in  $R[\gamma]$  are denoted  $a + \gamma b$  for  $a, b \in R$ . This means elements in  $R[\gamma]$  can be seen as elements in  $R \times R$ .

**Theorem 2.2.4.** The norm map<sup>1</sup>  $N : R[\gamma] \rightarrow R$  is defined as  $N(a + \gamma b) = a^2 - cb^2$  and has the property that  $N(a + \gamma b)$  is a unit in  $R$  if and only if  $a + \gamma b$  is a unit in  $R[\gamma]$ .

*Proof.* We see that  $N(a + \gamma b)^{-1}$  exists if and only if  $N(a + \gamma b)$  is a unit. Then,  $(a + \gamma b)(a - \gamma b) = N(a + \gamma b)$  so  $(a + \gamma b) [(a - \gamma b)N(a + \gamma b)^{-1}] = 1$ .  $\square$

*Remark 2.2.2.* Theorem 2.2.4 shows the quadratic ring extension of any field or integral domain maintains that status.

**Definition 2.3.** An element in an integral domain is called **irreducible** if it cannot be written as a product of two non-units.

**Definition 2.4.** Elements  $a, b$  in an integral domain  $R$  are called **associates** if there exists  $u \in R$  such that  $a = ub$ .

**Definition 2.5.** An integral domain has **unique factorization** if every element can be written as a product of irreducibles which are unique up to order and associates.

**Theorem 2.5.5.** A ring  $R$  has unique factorization if all irreducible elements are prime.

---

<sup>1</sup>We have not yet formally defined a *norm map*.

*Proof.* Let  $x = a_1 \cdots a_n = b_1 \cdots b_m$ . Since  $a_1$  is prime, we know that it divides one of  $b_i$ . Without loss of generality, let  $b_1 = ca_1$ . However, since  $b_1$  is irreducible and  $a_1 \neq 1$ , we have  $c = 1$ . Then, we can repeat this process on  $a_2 \cdots a_n = b_2 \cdots b_m$ .  $\square$

**Definition 2.6.** A **polynomial ring**  $R[x]$  of some ring  $R$  is created by using polynomials of the variable  $x$  using coefficients from  $R$ .

*Remark 2.6.1.* For some field  $F$ , Euclidean division works on  $F[x]$  because all non-zero coefficients are units. It then follows that irreducible elements are prime, so unique factorization exists in  $F[x]$ .

**Theorem 2.6.6** (Fundamental Theorem of Algebra). *The only irreducible polynomials in  $\mathbb{C}[x]$  are linear.*

*Remark 2.6.2.* It follows from Theorem 2.6.6 that the only irreducible polynomials in  $\mathbb{R}[x]$  are linear or quadratic. This can be proven using  $\mathbb{R}[x] \subset \mathbb{C}[x]$  and that multiplying some linear  $f(x) \in \mathbb{C}[x]$  with its conjugate results in some  $F(x) \in \mathbb{R}[x]$  with  $\deg(F(x)) = 2$ .

**Definition 2.7.** A subset  $I$  of ring  $R$  is called an **ideal** if for all  $a, b \in I$  and  $r \in R$ ,  $a + b, -a, ra, ar \in I$ .

**Definition 2.8.** For a commutative ring  $R$  and  $a \in R$ , a **principal ideal** generated by  $a$  is defined as  $aR = \{ar : r \in R\}$ . For some  $a, b \in R$ , we can also generate  $(a, b)R = \{xa + yb : x, y \in R\}$ .

*Remark 2.8.1.* For  $a \in R$  with integral domain  $R$ ,  $aR = 1R = R$  if and only if  $a$  is a unit.

*Remark 2.8.2.* For  $a, b \in R$ ,  $b \mid a \implies bR \subseteq aR$ . Furthermore,  $aR = bR$  if and only if  $a$  and  $b$  are associates.

*Remark 2.8.3.* For  $a, b \in R$ , if  $a$  is irreducible and  $b \mid a$ , then  $aR \subseteq bR \subseteq R$  so either  $aR = bR$  or  $bR = R$ . Therefore,  $aR$  is not properly contained in any other principal ideal. Also, if  $a$  is not irreducible, then  $aR \subset bR \subset R$ .

**Theorem 2.8.7.** *If an element  $a \in R$  cannot be written as a finite product of irreducibles, then  $R$  has an infinite ascending chain of principal ideals.*

*Proof.* Assume that  $a$  cannot be written as a finite product of irreducibles. Then,  $a = r_1 a_1 = r_1 r_2 a_2 = \dots$  for non-units  $r_i, a_i$  and reducible  $a_i$ . This implies  $aR \subset a_1 R \subset a_2 R \subset \dots$ .  $\square$

*Remark 2.8.4.* This tells us that every element in  $\mathbb{N}$  has a factorization into irreducibles since every proper divisor is “smaller” so there cannot be an infinite chain.

**Definition 2.9.** An integral domain  $R$  is a **principal ideal domain** if every ideal in  $R$  is a principal ideal.

**Proposition 2.9.1.** *The ring  $\mathbb{Z}$  is a principal ideal domain.*

*Proof.* If  $I = \{0\}$ , then  $I = 0\mathbb{Z}$ . Therefore, we prove with  $I \neq \{0\}$ . Then, there exists a positive element in  $I$ . Let  $a$  be the least positive element in  $I$  and we claim that  $I = a\mathbb{Z}$ .

Let  $b \in I$  be some other element in  $I$ . Then we have  $b = qa + r$  for  $0 \leq r < a$ . This also means  $b - qa = r$  so  $r \in I$ . However, by the minimality of  $a$ , this implies  $r = 0$  so  $b$  is a multiple of  $a$  and  $b \in a\mathbb{Z}$ .  $\square$

**Corollary 2.9.1.** *For field  $F$ ,  $F[x]$  is a principal ideal domain.*

**Theorem 2.9.8.** *For a principal ideal domain, every ascending chain of ideals stabilizes.*

*Proof.* Let  $I_1 \subseteq I_2 \subseteq \dots$  be an ascending chain of ideals in a principal ideal domain  $R$ . Then,  $\bigcup_{i=1}^{\infty} I_i$  is a principal ideal  $aR$ . For some  $j$ ,  $a \in I_j$  so  $aR = I_j = I_{j+1} = \dots$ .  $\square$

**Definition 2.10.** Let  $I, J$  be ideals of  $R$ . Then,  $I + J$  is the smallest ideal which contains both  $I$  and  $J$ . Therefore,  $I + J = \{a + b : a \in I \text{ and } b \in J\}$ .

*Remark 2.10.1.* Since  $\mathbb{Z}$  is a principal ideal domain,  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ . Then,  $d\mathbb{Z} = \{xa + yb : x, y \in \mathbb{Z}\}$ . Therefore,  $d = \gcd(a, b)$  since it is the least positive element (by proof of Theorem 2.9.1).

**Definition 2.11.** An ideal  $I$  of ring  $R$  is a **prime ideal** if  $ab \in I$  implies  $a \in I$  or  $b \in I$  for all  $a, b \in R$ .

*Remark 2.11.1.* An element  $p \in R$  is prime if and only if  $pR$  is prime.

*Remark 2.11.2.* Not all prime ideals are principal (eg.  $(x, y) \subset \mathbb{Q}[x, y]$ ).

**Definition 2.12.** An ideal  $I$  in ring  $R$  is called **maximal** if for any ideal  $J \subseteq R$  where  $I \subseteq J \subseteq R$ , it follows that  $I = J$  or  $J = R$ .

*Remark 2.12.1.* In a principal ideal domain, the principal ideal generated by an irreducible element is maximal.

**Theorem 2.12.9.** *In an integral domain, maximal ideals are prime.*

*Proof.* Let  $I$  be a maximal ideal of ring  $R$  with  $bc \in I$  and  $b \notin I$ . Then, we have  $I \subsetneq I + bR \subseteq R$  so, by the maximality of  $I$ ,  $I + bR = R$ . This also means that  $1 \in I + bR$  so  $1 = a + br$  for  $a \in I$  and  $r \in R$ . Multiplying through by  $c$ , this gives us  $c = ac + bcr \in I$  since  $a, bc \in I$ .  $\square$

*Remark 2.12.2.* For a principal ideal domain  $R$ , this gives us that  $a \in R$  is irreducible implies  $aR$  is maximal implies  $aR$  is prime implies  $a$  is prime. Therefore, by Theorem 2.5.5, every principal ideal domain has unique factorization.

**Definition 2.13.** A ring is a unique factorization domain if every non-zero non-unit can be written uniquely as a product of irreducible elements, up to order and associates. Duplicate of Definition 2.5; don't ask why.

*Remark 2.13.1.* Unique factorization domains exist which are not principal ideal domains. For example,  $\mathbb{Z}[x]$  with  $2\mathbb{Z}[x] + x\mathbb{Z}[x]$ .