

# Contents

|          |                                       |           |
|----------|---------------------------------------|-----------|
| <b>1</b> | <b>The Integers</b>                   | <b>2</b>  |
| 1.1      | Prime Numbers . . . . .               | 4         |
| 1.2      | Modular Arithmetic . . . . .          | 5         |
| <b>2</b> | <b>Rings</b>                          | <b>11</b> |
| 2.1      | Subrings . . . . .                    | 13        |
| 2.2      | Ideals . . . . .                      | 16        |
| 2.3      | Quotient Rings . . . . .              | 17        |
| 2.4      | Prime and Maximal Ideals . . . . .    | 23        |
| <b>3</b> | <b>Polynomial Rings over Fields</b>   | <b>25</b> |
| 3.1      | Irreducibility . . . . .              | 28        |
| 3.2      | Roots . . . . .                       | 30        |
| 3.3      | Quotienting by Irreducibles . . . . . | 31        |
| <b>4</b> | <b>Integral Domains</b>               | <b>32</b> |
| 4.1      | Euclidean Domains . . . . .           | 36        |
| 4.2      | Principal Ideal Domains . . . . .     | 38        |

# 1 The Integers

## Theorem (Well-Ordering Principle)

Every nonempty set of non-negative integers contain a least element. Mathematically,  
 $\exists a \in S : \forall b \in S, a \leq b$ .

*Proof.* Let  $S$  be a set of non-negative integers. Suppose  $S$  has no smallest element. Then,  $0 \notin S$ , because otherwise, 0 would be the smallest element. By induction, suppose  $0, 1, \dots, k \notin S$ . Then,  $k + 1 \notin S$  since otherwise, it would be the smallest element. Therefore,  $S = \emptyset$ .  $\square$

## Definition: Divides

Let  $a, b \in \mathbb{Z}$ .  $b$  **divides**  $a$  if  $a = bc$  for some  $c \in \mathbb{Z}$ , written as  $b \mid a$ .

**Proposition:** Let  $a, b \in \mathbb{Z}, a \neq 0$  such that  $b \mid a$ . Then  $|b| \leq |a|$ .

*Proof.* Let  $a, b \in \mathbb{Z}$  such that  $b \mid a$  and  $a \neq 0$ . Then there exists some  $c \in \mathbb{Z}$  such that  $a = bc$ . Since  $a \neq 0$ ,  $b, c$  are necessarily nonzero. Applying the absolute value to both sides of the equation, we get  $|a| = |bc| = |b||c|$ . Since  $b, c \neq 0$ , we have  $|b|, |c| > 0$ . Then  $|b| \leq |b||c| = |bc| = |a|$ , so  $|b| \leq |a|$ .  $\square$

## Theorem (Division Algorithm)

Let  $a, b \in \mathbb{Z}$  such that  $b > 0$ . There exists unique  $q, r \in \mathbb{Z}$  such that  $a = bq + r$  where  $0 \leq r < b$ .

*Proof. Existence:* Let  $a, b \in \mathbb{Z}, b > 0$ . Consider the set  $S = \{a - bx : x \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$ . Consider  $b = -|a|$ . Then,  $a - (-|a|)x \in S$ . By the well-ordering principle, choose the smallest  $a - bx \in S$  such that  $q := x, r := a - bx$ . Then, rearranging  $r$  and substituting  $q$  for  $x$ , we get  $a = bq + r \in S$ . By construction of  $S$ ,  $0 \leq r$ . Suppose  $r \geq b$ . Then,  $0 \leq r - b = (a - bx) - b = a - b(x + 1)$ . This implies that  $r - b < r$ , a contradiction, since  $r \in S$  was the least element by choice. Therefore,  $0 \leq r < b$ .

**Uniqueness:** Suppose we have  $q_1, r_1, q_2, r_2 \in \mathbb{Z}$  such that  $a = bq_1 + r_1 = bq_2 + r_2$ , where  $0 \leq r_1, r_2 < b$ . Then, we have

$$\begin{aligned} bq_1 + r_1 &= bq_2 + r_2 \\ bq_1 + r_1 - (bq_2 + r_2) &= 0 \\ b(q_1 - q_2) + (r_1 - r_2) &= 0 \\ b(q_1 - q_2) &= -(r_1 - r_2) \\ b(q_1 - q_2) &= r_2 - r_1 \end{aligned}$$

Since  $0 \leq r_1 < b$ , we can rewrite the inequality to be  $-b < -r_1 \leq 0$ . Then, adding  $0 \leq r_2 < b$  to the inequality, we get  $-b < r_2 - r_1 < b$ . Because  $b \mid (r_2 - r_1)$ ,  $(r_2 - r_1)$  must be a multiple of  $b$ , but since  $-b < r_2 - r_1 < b$ , we have that  $(r_2 - r_1) = 0b = 0$ . Then,  $b(q_1 - q_2) = r_2 - r_1 = 0$ . This implies that  $q_1 = q_2$  and  $r_1 = r_2$ . Therefore,  $q_1, r_1 \in \mathbb{Z}$  are unique.  $\square$

### Definition: Greatest Common Divisor (gcd)

Let  $a, b \in \mathbb{Z}$  and either  $a \neq 0$  or  $b \neq 0$ , but not both. The **greatest common divisor** of  $a$  and  $b$  is the largest integer dividing  $a$  and  $b$ . We write  $\gcd(a, b)$  or  $(a, b)$ .

$(a, b) \mid a$  and  $(a, b) \mid b$ . Further, if  $c > 0$  divides  $a$  and  $b$ , then  $0 < c \leq (a, b)$ .

### Theorem (Bezout's Identity)

Let  $a, b \in \mathbb{Z}$  with  $a \neq 0$  or  $b \neq 0$ , but not both. Suppose  $d = (a, b)$ . We can find  $x, y \in \mathbb{Z}$  such that  $ax + by = d$ .

*Proof.* Let  $d = (a, b)$ . Consider the set  $S = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$ . Consider  $x = a, y = b$ . Then  $ax + by = a^2 + b^2 \geq 0 \in S$ , so  $S$  is not empty. By the well-ordering principle, choose the least element  $s = ax + by \in S$  and consider  $a = sq + r$  where  $0 \leq r < s$ . Rearranging the second equation, we get

$$\begin{aligned} a &= sq + r \\ r &= a - sq \\ &= a - (ax + by)q \\ r &= a(1 - xq) + b(-yq) \end{aligned}$$

This implies that  $r \in S$  since  $0 \leq r$  by definition. We also have that  $r < s$ , but since  $s$  was chosen to be the smallest element in  $S$ , this forces  $r = 0$ . Then,  $a = sq + r = sq$ , so  $s \mid a$ . Similarly,  $b = st$  for some  $t \in \mathbb{Z}$ , so  $s \mid b$ . Since  $s \mid a$  and  $s \mid b$ ,  $s \leq d$ . But  $d \mid a$  and  $d \mid b$  by definition, so  $d \mid s$  which implies that  $d \leq s$ . Therefore,  $d = s = ax + by$ .  $\square$

### Theorem

Let  $a, b \in \mathbb{Z}$  and suppose  $a \mid bc$  and  $(a, b) = 1$ . Then  $a \mid c$ .

*Proof.* Because  $(a, b) = 1$ , we can write  $1 = ax + by$ . Also, since  $a \mid bc$ , there exists some  $z \in \mathbb{Z}$  such that  $bc = az$ . Then

$$\begin{aligned} c &= cax + cby \\ &= a(cx) + (bc)y \\ &= a(cx) + a(z)y \\ c &= a(cx + zy) \end{aligned}$$

Therefore,  $a \mid c$ .  $\square$

### Corollary

Let  $a, b, c \in \mathbb{Z}$  and  $(a, b) = 1$ . If  $a \mid c$  and  $b \mid c$ , then  $ab \mid c$ .

*Proof.* Since  $(a, b) = 1$ , we have  $ax + by = 1$ . By definition, since  $a \mid c$  and  $b \mid c$ , there exist  $n, m \in \mathbb{Z}$  such that  $c = na$  and  $c = mb$ . Then, we have

$$\begin{aligned} 1 &= ax + by \\ c &= cax + cby \\ &= (bm)ax + (an)by \\ &= (ba)mx + (ab)ny \\ c &= ab(mx + ny) \end{aligned}$$

so  $ab \mid c$ . □

## 1.1 Prime Numbers

### Definition: Prime

A nonzero non-unit integer  $p$  is **prime** if its only divisors are  $\pm 1, \pm p$ .

### Theorem

Let  $p \in \mathbb{Z} \setminus \{0, \pm 1\}$ . The following statements are equivalent.

- (1)  $p$  is prime.
- (2) If  $p \mid bc$ , then  $p \mid b$  or  $p \mid c$  where  $b, c \in \mathbb{Z}$ .

*Proof.* (1)  $\implies$  (2) Suppose  $p$  is prime and  $p \mid bc$ . If  $p \mid b$ , we are done, so suppose  $p \nmid b$ . Then,  $(p, b) = 1$ , so we have

$$\begin{aligned} 1 &= px + by \\ c &= cpx + cby \\ &= p(cx) + (bc)y \\ &= p(cx) + (pn)y & p \mid bc \implies bc = pn, n \in \mathbb{Z} \\ &= p(cx) + p(ny) \\ c &= p(cx + ny) \end{aligned}$$

so  $p \mid c$ .

(1)  $\longleftarrow$  (2) To prove the reverse implication, suppose the contrapositive: “If  $p$  is not prime, then there exist some  $b, c \in \mathbb{Z}$  such that  $p \mid bc$  but  $p \nmid b$  and  $p \nmid c$ ”. Suppose  $p \in \mathbb{Z} \setminus \{0, \pm 1\}$  is not prime; i.e.  $p$  is composite. Then,  $p$  can be written as its unique factorization  $q_1 q_2 \cdots q_n$  where  $n \geq 2$  and each  $q_i$  is prime. Choose  $b = q_1$  and  $c = q_2 \cdots q_n$ . Then  $p \mid bc$  because  $bc = p$  and  $p \mid p$ , but  $p \nmid b$  and  $p \nmid c$  because  $|p| > |b|$  and  $|p| > |c|$  respectively. □

### Theorem

Let  $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ .  $n$  can be written as a product of primes.

*Proof.* Let  $n > 1$ . Let  $S$  be the set of positive integers greater than 1 that cannot be written as a product of primes. Suppose for the sake of contradiction that  $S$  is nonempty. Then by the well-ordering principle, pick a least element  $m \in S$ . By definition,  $m$  is not prime or a product of primes. Because  $m$  is not prime, there exists  $a \in \mathbb{Z}$  such that  $a \neq \pm 1, \pm m$  and  $a \mid m$ . Then,  $m = ab$  for some  $b \in \mathbb{Z}$ . By definition,  $|a| \leq |m|$  and  $|b| \leq |m|$ . Without loss of generality, assume  $a, b > 0$ . Note that  $b \neq 1$  since otherwise,  $a = m$ . So,  $1 < a, b < m$  and  $a, b \notin S$ . Because  $a, b \notin S$ , they are products of primes. But  $m = a \cdot b$ , so  $m$  is a product of primes, a contradiction. Therefore,  $S = \emptyset$ , so  $n$  can be written as a product of primes.  $\square$

### Theorem (Fundamental Theorem of Arithmetic)

Let  $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ . Suppose  $n = p_1 \cdots p_r$  and  $n = q_1 \cdots q_s$  where each  $p_i, q_j$  is prime. Then  $r = s$  and there is a unique permutation  $\sigma$  on  $\{1, \dots, r\}$  such that  $p_i = \pm q_{\sigma(i)}$ .

*Proof.* Let  $n \in \mathbb{Z} \setminus \{0, 1\}$ . Without loss of generality, suppose  $n$  is positive and  $n = p_1 \cdots p_r$  and  $n = q_1 \cdots q_s$  where each  $p_i, q_j$  is prime. Then  $p_1 \mid q_1 \cdots q_s$ . In particular,  $p_1 \mid q_j$  for some  $j \leq s$ . Because  $q_j$  is prime, we necessarily have that  $q_j = |p_1|$ . Without loss of generality reindex  $j = 1$  to get  $q_1 = |p_1|$ . Then,  $p_1 \cdot (p_2 \cdots p_r) = p_1 \cdot (q_2 \cdots q_s) \implies p_2 \cdots p_r = q_2 \cdots q_s$ . By induction, we have that  $p_r = q_r$ . If  $r < s$ , by the above, we have that  $1 = q_{r+1} \cdots q_s$ , which implies  $q_j = 1$  for each  $j$ . A similar argument is said for  $s < r$ . In either case, we have a contradiction. Therefore,  $r = s$  and there is a unique permutation  $\sigma$  on  $\{1, \dots, r\}$  such that  $p_i = q_{\sigma(i)}$ .  $\square$

## 1.2 Modular Arithmetic

### Definition: Well-Defined Functions

A function  $f : X \rightarrow Y$  is **well-defined** if, for all  $a, b \in X$ , we have  $f(a) = f(b)$  whenever  $a = b$ .

### Definition: Equivalence Relation

A relation  $R$  on a set  $S$  is any subset of  $S \times S$ . An **equivalence relation** is a relation with the following properties:

1. Reflexivity: For any  $a \in S$ ,  $(a, a) \in R$  (alternatively written as  $a \sim a$ ).
2. Symmetry: For any  $(a, b) \in S \times S$ ,  $(a, b) \in R$  implies  $(b, a) \in R$  (alternatively written as  $a \sim b \implies b \sim a$ ).
3. Transitivity: For any  $a, b, c \in S$ , if  $(a, b), (b, c) \in R$ , then  $(a, c) \in R$  (alternatively written as  $a \sim b, b \sim c \implies a \sim c$ ).

Pick  $m \in \mathbb{Z}$  to be nonzero. The **Division Algorithm** says that for any  $a, b \in \mathbb{Z}$ , we can write  $a = q_1m + r_1, b = q_2m + r_2$  for unique  $q_1, q_2, r_1, r_2 \in \mathbb{Z}$  where  $0 \leq r_1, r_2 < |m|$ .

**Definition: Modulo**

Define a relation  $R_m$  on  $\mathbb{Z}$  by saying  $(a, b) \in R_m$  if and only if  $r_1 = r_2$  (alternatively written as  $a \sim b$  if and only if  $r_1 = r_2$ ). We write this as  $a \equiv b \pmod{m}$ .

**Proposition:** For any  $m \in \mathbb{Z}$  nonzero,  $R_m$  is an equivalence relation.

*Proof.* Let  $R_m$  be the relation defined above for  $m \in \mathbb{Z}$  nonzero.

- (1) For any  $a \in \mathbb{Z}$ , write  $a = bq + r$ . Then, since  $r = r$ ,  $a \equiv a \pmod{m}$ ,  $R_m$  is reflexive.
- (2) Take  $a, b \in \mathbb{Z}$  and assume  $a \equiv b \pmod{m}$ . By the division algorithm, we can write  $a = q_1m + r_1, b = q_2m + r_2$ . By assumption,  $a \equiv b \pmod{m}$ , so  $r_1 = r_2$ . Since equality is symmetric,  $r_1 = r_2 \iff r_2 = r_1$ , so  $b \equiv a \pmod{m}$ .  $R_m$  is symmetric.
- (3) Pick  $a, b, c \in \mathbb{Z}$  and assume  $a \equiv b \pmod{m}, b \equiv c \pmod{m}$ . By the division algorithm, we can write  $a = q_1m + r_1, b = q_2m + r_2, c = q_3m + r_3$ . By assumption,  $r_1 = r_2$  and  $r_2 = r_3$ . Since equality is transitive,  $r_1 = r_2, r_2 = r_3 \implies r_1 = r_3$ , so  $a \equiv c \pmod{m}$ .  $R_m$  is transitive.

Since  $R_m$  satisfies (1) – (3),  $R_m$  is an equivalence relation. □

**Definition: Equivalence Class**

If  $R$  is an equivalence relation on a set  $S$ , then  $S$  can be written as the union of equivalence classes. The **equivalence class** of  $x$  is the set  $[x] := \{y \in S : (x, y) \in R\}$ .

**Note:** The equivalence classes of  $R_m$  are  $[0], [1], \dots, [m-1]$ .

**Definition: Congruent Modulo  $n$**

Let  $a, b \in \mathbb{Z}$  and  $n \in \mathbb{Z}$  be positive. We say  $a$  and  $b$  are **congruent modulo  $n$**  if  $n \mid (a - b)$ , written as  $a \equiv b \pmod{n}$ .

The **integers modulo  $n$**  is the set of equivalence classes modulo  $n$ , written as  $\mathbb{Z}/n, \mathbb{Z}_n, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/(n)$ .

**Definition: Operations on  $\mathbb{Z}/n$**

Let  $n \in \mathbb{Z}$  and  $[a], [b] \in \mathbb{Z}/n$ . Define

$$\rightarrow [a] + [b] = [a + b]$$

$$\rightarrow [a][b] = [ab]$$

$$\rightarrow \text{For } k \geq 0, [a]^k = [a^k]$$

**Proposition:** The operations above are well-defined.

*Proof.* Let  $n \in \mathbb{Z}$  and  $[a], [a'], [b], [b'] \in \mathbb{Z}/n$  where  $[a] = [a'], [b] = [b']$ . Then  $([a] = [a']$  and  $[b] = [b']$  implies  $n \mid (a - a')$  and  $n \mid (b - b')$ , so  $n \mid (a - a') + (b - b') = (a + b) - (a' + b')$ . Therefore,  $[a + b] = [a' + b']$ . Similarly,

$$\begin{aligned} ab - a'b' &= ab + 0 - a'b' \\ &= ab + (-ab' + ab') - a'b' \\ &= (ab - ab') + (ab' - a'b') \\ ab - a'b' &= a(b - b') + b'(a - a') \end{aligned}$$

Since  $n \mid (a - a')$  and  $n \mid (b - b')$ ,  $n \mid ab - a'b'$ , so  $[ab] = [a'b']$ . □

**Proposition:** Let  $[a], [b], [c] \in \mathbb{Z}/n$ . Then the following properties hold:

- (1)  $[a] + [b] = [b] + [a]$
- (2)  $[a] + ([b] + [c]) = ([a] + [b]) + [c]$
- (3)  $[a] + [0] = [a]$
- (4) There exists  $x \in \mathbb{Z}$  such that  $[a] + x = [0]$
- (5)  $[a][b] = [b][a]$
- (6)  $[a]([b][c]) = ([a][b])[c]$
- (7)  $[a][1] = [a]$
- (8)  $[a]([b] + [c]) = [a][b] + [a][c]$

*Proof.* Let  $[a], [b], [c] \in \mathbb{Z}/n$ . Then

- (1)  $\underline{[a]} + \underline{[b]} = [a + b] = [b + a] = \underline{[b]} + \underline{[a]}$
- (2)  $\underline{[a]} + (\underline{[b]} + \underline{[c]}) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = \underline{([a] + [b])} + \underline{[c]}$
- (3)  $\underline{[a]} + \underline{[0]} = [a + 0] = \underline{[a]}$
- (4) Take  $x \in \mathbb{Z}$  such that  $x = n - a$ . Then,  $\underline{[a]} + x = [a] + [n - a] = [a - n + a] = [n] = \underline{[0]}$ .
- (5)  $\underline{[a][b]} = [ab] = [ba] = \underline{[b][a]}$
- (6)  $\underline{[a]}(\underline{[b][c]}) = [a][bc] = [abc] = [ab][c] = \underline{([a][b])} \underline{[c]}$
- (7)  $\underline{[a][1]} = [a \cdot 1] = [a]$
- (8)  $\underline{[a]}(\underline{[b]} + \underline{[c]}) = [a][b + c] = [a \cdot (b + c)] = [ab + ac] = [ab] + [ac] = \underline{[a][b]} + \underline{[a][c]}$

□

### Definition: Unit and Inverse

Let  $n > 1$  be an integer. Consider  $[a] \in \mathbb{Z}/n$ . If there exists  $[b] \in \mathbb{Z}/n$  such that  $[a][b] = [1]$ , then we say  $[a]$  is a **unit** and  $[b]$  is the **inverse** of  $[a]$ , written as  $[a]^{-1}$ .

### Theorem

Let  $p > 1$  be an integer. The following statements are equivalent:

- (1)  $p$  is prime.
- (2) Each nonzero  $[a] \in \mathbb{Z}/p$  has an inverse.
- (3) If  $[ab] = [0]$ , then either  $[a] = [0]$  or  $[b] = [0]$

*Proof.* Let  $p > 1$  be an integer.

(1)  $\implies$  (2) Take  $[a] \in \mathbb{Z}/p$  to be nonzero. Then  $p \nmid a$  since  $p$  is prime. That is,  $(p, a) = 1$ . Then  $px + ay = 1$ , or  $[1] = [px + ay] = [px] + [ay]$ . But  $[px] = [p][x] = [0][x] = [0] \in \mathbb{Z}/p$ , so  $[1] = [0] + [ay] = [ay] = [a][y]$ . Then,  $[y]$  is the inverse of  $[a]$ . Since  $[a]$  was arbitrary, this holds for all  $[a] \in \mathbb{Z}/p$ .

(2)  $\implies$  (3) Let  $[a], [b] \in \mathbb{Z}/p$  and suppose  $[ab] = [0]$ . If  $[a] = [0]$ , we are done, so suppose  $[a] \neq [0]$ . Then,  $[a]$  has an inverse, so  $[a]^{-1}[ab] = [a]^{-1}[a][b] = [1][b] = [b] = [0]$ . Therefore, either  $[a] = [0]$  or  $[b] = [0]$ .

(3)  $\implies$  (1) Suppose for the sake of contradiction that  $p$  is not prime; i.e.  $p$  is composite. Then we can find a divisor  $a > 0$  such that  $a \neq \pm 1, \pm p$ . That is,  $|1| < a < |p|$ . Let  $p = ab$ . Then  $1 < a, b < p$ , but  $[ab] = [p] = [0]$ , a contradiction.  $\square$

### Theorem

Let  $n > 1$  be an integer and  $[a] \in \mathbb{Z}/n$ . Then  $[a]$  has a multiplicative inverse if and only if  $(a, n) = 1$ .

*Proof.* ( $\implies$ ) Suppose  $[a]$  has a multiplicative inverse. Then there exists  $[x] \in \mathbb{Z}/n$  such that  $[a][x] = [1]$ . Then

$$\begin{aligned} [1] &= [a][x] \\ &= [ax] + [0] \\ &= [ax] + [ny] & [ny] = [0] \in \mathbb{Z}/n, y \in \mathbb{Z} \\ [1] &= [ax + ny] \end{aligned}$$

so  $(a, n) = 1$ .

( $\impliedby$ ) Suppose  $(a, n) = 1$ . Then  $ax + ny = 1$  for some  $x, y \in \mathbb{Z}$ , but  $[ny] = [0] \in \mathbb{Z}/p$ , so  $[ax] = [a][x] = [1]$ , where  $[x]$  is the multiplicative inverse of  $[a]$ .  $\square$



### Theorem Chinese Remainder Theorem

Let  $m, n \in \mathbb{Z}$  be coprime and positive. Let  $a, b \in \mathbb{Z}$ . We can find  $x \in \mathbb{Z}$  such that

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}$$

Moreover, if  $y$  is another solution, then  $y \equiv x \pmod{mn}$ .

*Proof.* Let  $m, n \in \mathbb{Z}$  such that  $(n, m) = 1$ . Then we can write  $na + mb = 1$  for some  $a, b \in \mathbb{Z}$ . Set  $x := c(na) + d(mb)$ . Then

$$\begin{aligned} [x]_m &= [cna]_m + [dmb]_m \\ &= [n(cn)]_m + [m(db)]_m \\ &= [a(cn)]_m + [0] \qquad [m(db)]_m = [0] \in \mathbb{Z}/m \\ [x]_m &= [a]_m \end{aligned}$$

so  $[x]_m = [a]_m$ . Similarly,  $[x]_n = [b]_n$ . So we have

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}$$

Let  $y$  be another solution. Then  $[y]_m = [x]_m$  so  $m \mid y - x$ . Similarly,  $n \mid y - x$ . But since  $(n, m) = 1$ , we have that  $mn \mid y - x$ , or  $[y]_{mn} = [x]_{mn}$ . So  $y \equiv x \pmod{mn}$ .  $\square$

### Theorem Chinese Remainder Theorem (General)

Let  $m_1, \dots, m_n \in \mathbb{Z}$  be positive and pairwise relatively prime (i.e.,  $(m_i, m_j) = 1$  when  $i \neq j$ ). Let  $a_1, \dots, a_n \in \mathbb{Z}$ . We can find  $x$  such that

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Moreover, if  $y$  is another solution, then  $y \equiv x \pmod{m_1 m_2 \cdots m_n}$

*Proof.* We will induct on  $n \in \mathbb{N}$ .

**Base case:** At  $n = 2$ , we have  $m_1, m_2 \in \mathbb{Z}$  where  $(m_1, m_2) = 1$ . Then, we can find  $p, q \in \mathbb{Z}$  such that  $m_1 p + m_2 q = 1$ . Then, because  $m_2 q \equiv 0 \pmod{m_2}$ , we have  $m_1 \equiv 1 \pmod{m_2}$ . Similarly,  $m_2 \equiv 1 \pmod{m_1}$ . Consider  $x = (m_2 q)r + (m_1 p)s$  for  $r, s \in \mathbb{Z}$ . Then, since  $(m_2 q)r \equiv 0 \pmod{m_2}$ , we have  $x \equiv (m_1 p)s \equiv s \pmod{m_2}$ . Similarly,  $x \equiv (m_2 q)r \equiv r \pmod{m_1}$ . So,  $x \equiv r \pmod{m_1}$  and  $x \equiv s \pmod{m_2}$ . Now suppose  $y$  is another solution. Then, we have  $y \equiv x \pmod{m}$ , which implies that  $m_1 | (y - x)$  and similarly,  $m_2 | (y - x)$ . Then because  $(m_1, m_2) = 1$ , we have that  $m_1 m_2 | (y - x)$ , so  $y \equiv x \pmod{m_1 m_2}$ .

**Inductive step:** At  $n = n + 1$ , we have  $m_1, m_2 \in \mathbb{Z}$  where  $(m_1, m_2) = 1$ . Then by the inductive hypothesis, we have a set of  $n$  pairwise coprime integers  $m_1, \dots, m_n$  where  $x' \equiv a_i \pmod{m_i}$  for each  $i = 1, \dots, n$ . Define  $M = \prod_{i=1}^n m_i$  and consider  $x = x' + sM$  for some  $s \in \mathbb{Z}$ . Then since  $m_i | M$  implies  $sM \equiv 0 \pmod{m_i}$  and from the inductive hypothesis,  $x' \equiv a_i \pmod{m_i}$ , we have  $x \equiv x' + sM \equiv x' \equiv a_i \pmod{m_i}$  for  $i = 1, \dots, n$ . At  $m_{n+1}$ , because  $m_{n+1} \nmid M$ , we can choose an  $s \in \mathbb{Z}$  such that  $x \equiv x' + sM \equiv a_{n+1} \pmod{m_{n+1}}$ . Now suppose  $y$  is another solution. Then  $y \equiv x' \pmod{M}$  and  $y \equiv a_{n+1} \pmod{m_{n+1}}$ . Since  $(M, m_{n+1}) = 1$ , by the inductive hypothesis, we have that  $y \equiv x \pmod{M m_{n+1}}$ , so  $y \equiv x \pmod{m_1 m_2 \cdots m_{n+1}}$ .  $\square$

The rest of this page is intentionally left blank

## 2 Rings

### Definition: Ring

A **ring**  $R$  is a nonempty subset with two operations, addition (+) and multiplication ( $\cdot$ ) such that, for all  $a, b, c \in R$ , the following properties hold:

- (1)  $a + b \in R$
- (2)  $a + (b + c) = (a + b) + c$
- (3)  $a + b = b + a$
- (4) There exists  $0 \in R$  such that  $0 + a = a + 0 = a$  for all  $a \in R$ .
- (5) For all  $a \in R$ , there exists  $-a$  such that  $(-a) + a = a + (-a) = 0$ .
- (6)  $a \cdot b \in R$
- (7)  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- (8)  $a \cdot (b + c) = a \cdot b + a \cdot c$
- (9)\* There exists  $1 \in R$  such that  $1 \cdot a = a \cdot 1 = a$  for all  $a \in R$ .

\*A set satisfying (1) - (8) is called a **nonunital ring**. If the set also satisfies (9), it is called a **unital ring**.

- A ring is **commutative** if, for all  $a, b \in R$ ,  $a \cdot b = b \cdot a$ .
- An element  $a \in R$  is a **zero divisor** if there exists a nonzero  $b \in R$  such that  $a \cdot b = 0$  or  $b \cdot a = 0$ .
- An element  $a \in R$  is a **unit** if there exists  $b \in R$  such that  $a \cdot b = b \cdot a = 1$ , and is called the *inverse* of  $a$ , written as  $a^{-1}$ .

**Proposition:** Let  $n > 1$ ,  $a \in \mathbb{Z}$ . If  $(a, n) = 1$ ,  $[a]$  is a unit. Otherwise, it is a zero divisor.

*Proof.* Let  $n > 1$  and  $a \in \mathbb{Z}$ . There are two cases.

**Case (1):**  $(a, n) = 1$ . Then  $ax + ny = 1$  so  $[ax] = [a][x] = [1]$  where  $[x]$  is the inverse of  $[a]$ , so  $[a]$  is a unit.

**Case (2):**  $(a, n) \neq 1$ . Then  $(a, n) = d$  for  $d > 1$ . Then,  $ax + ny = d$  so  $[ax] = [d]$ . Since  $d|n$ ,  $n = dm$  for some  $m \in \mathbb{Z}$ . Then since  $[d] = [dm] = [0]$ , we get  $[ax] = [a][x] = [0]$ , where  $[x]$  is nonzero, so  $[a]$  is a zero divisor.

□

**Proposition:** Let  $R$  be a ring and  $a, b, c \in R$ . The following hold:

- (1) The additive identity is unique.
- (2) An additive inverse is unique.
- (3) If  $a + b = a + c$ , then  $b = c$ .
- (4) The multiplicative identity is unique.
- (5) If  $a$  is a unit, then its inverse is unique.
- (6)  $0 \cdot a = a \cdot 0 = 0$
- (7)  $(a)(-b) = -ab = (-a)(b)$
- (8)  $-(-a) = a$
- (9)  $-(a + b) = -a - b$
- (10)  $-(a - b) = -a + b$
- (11)  $(-a)(-b) = ab$

*Proof.* Let  $R$  be a ring. Then

- (1) Let  $0, 0' \in R$  be two additive identities. Then  $\underline{0} = 0 \cdot 0' = 0' \cdot 0 = \underline{0'}$ .
- (2) Let  $a \in R$  have two additive inverses  $b, c \in R$ . Then  $\underline{b} = 0 + b = (c + a) + b = c + (a + b) = c + 0 = \underline{c}$ .
- (3) Let  $a + b = a + c$ . Then  $(-a + a) + b = (-a + a) + c \rightarrow 0 + b = 0 + c \rightarrow b = c$ .
- (4)  $1, 1' \in R$  be two multiplicative identities. Then  $\underline{1} = 1 \cdot 1' = 1' \cdot 1 = \underline{1'}$ .
- (5) Let  $a \in R$  be a unit with two multiplicative inverses  $b, c \in R$ . Then  $\underline{b} = b \cdot 1 = b \cdot (ac) = (ba) \cdot c = 1 \cdot c = \underline{c}$ .
- (6) Let  $a \in R$ . Then  $0 = (a + a) \cdot 0 = a0 + a0 = a0$ . Similarly,  $0 = 0a$ .
- (7) Let  $a, b \in R$ . Then  $a0 = a(b + (-b)) = ab + (a)(-b) \implies (a)(-b) = -ab$ . Similarly,  $(-a)(b) = -ab$ .
- (8) Let  $a \in R$ . Then  $\underline{-(-a)} = 0 - (-a) = (a + (-a)) + (-(-a)) = a + ((-a) - (-a)) = a + 0 = \underline{a}$ .

(9) Let  $a, b \in R$ . Then

$$\begin{aligned}
 -(a+b) &= 0 - (a+b) \\
 &= 0 + 0 - (a+b) \\
 &= (a-a) + (-b+b) - (a+b) \\
 &= a + (-a-b) + b - (a+b) & a-b = a + (-b) \\
 &= (-a-b) + (a+b) - (a+b) \\
 &= (-a-b) + 0 \\
 -(a+b) &= -a-b
 \end{aligned}$$

(10) Let  $a, b \in R$ . Then  $\underline{-(a-b)} = -(a+(-b)) = -a - (-b) = \underline{-a+b}$ .

(11) Let  $a, b \in R$ . Then  $\underline{(-a)(-b)} = a(-(-b)) = \underline{ab}$ .

□

## 2.1 Subrings

### Definition: Subring

Let  $R$  be a ring. A **subring**  $S \subseteq R$  is a subset such that  $S$  forms a ring with the same operations and same identities as  $R$ . If  $S$  forms a nonunital ring with the same operations or forms a ring but  $1_s \neq 1_R$ ,  $S$  is a **nonunital subring**.

Let  $R$  be a ring.  $S \subseteq R$  is a subring of  $R$  if and only if it satisfies the following:

- (1)  $1_R \in S$
- (2)  $S$  is closed under addition.
- (3)  $S$  is closed under multiplication.
- (4) If  $a \in S$ , then  $-a \in S$ .

### Definition: Integral Domain

A commutative ring  $R$  is an **integral domain** if it has no nonzero zero divisors. That is, if  $a, b \in R$  and  $ab = 0$ , then  $a = 0$  or  $b = 0$ .

**Proposition:** Let  $R$  be an integral domain and  $a, b, c \in R$ . If  $ac = bc$  for  $c \neq 0$ , then  $a = b$ .

*Proof.* Suppose  $ac = bc$ . Then  $ac - bc = 0 \rightarrow (a-b)c = 0$ . because  $R$  is an integral domain,  $(a-b) = 0$  or  $c = 0$ . But since  $c \neq 0$  by assumption,  $(a-b) = 0$  which implies that  $a = b$ . □

### Definition: Field

Let  $R$  be a commutative ring. If all nonzero elements of  $R$  are units,  $R$  is a field.

**Proposition:** Every field is an integral domain.

*Proof.* Let  $R$  be a field. Since all nonzero elements of  $R$  are units, they cannot be zero divisors.  $\square$

### Theorem

Every finite integral domain is a field.

*Proof.* Let  $R$  be a finite integral domain  $R = \{r_1, \dots, r_n\}$ . Take  $r_i \in R$  to be nonzero. Consider  $r_i R = \{r_i r_1, \dots, r_i r_n\} \subseteq R$ . Then,  $|r_i R| \leq |R|$  since  $r_i R \subseteq R$ . Take  $r_i r_j, r_i r_k \in r_i R$  such that  $r_i r_j = r_i r_k$ . Then because  $r_i \neq 0$ , we have  $r_i r_j - r_i r_k = 0$ , or  $(r_j - r_k)r_i = 0$ . Since  $r_i \neq 0$  by assumption,  $(r_j - r_k) = 0 \rightarrow r_j = r_k$ . So  $R \subseteq r_i R$  which implies  $|R| \leq |r_i R|$ . Because  $|r_i R| \leq |R|$  and  $|r_i R| \geq |R|$ ,  $|r_i R| = |R|$ .  $\square$

### Definition: Homomorphism

Let  $R, S$  be rings. A function  $f : R \rightarrow S$  is a **ring homomorphism** if

- (1)  $f(a + b) = f(a) + f(b)$
- (2)  $f(a \cdot b) = f(a) \cdot f(b)$
- (3)\*  $f(1_R) = 1_S$

\*A function satisfying (1), (2), but not (3) is a **nonunital ring homomorphism**.

**Proposition:** Let  $R, S$  be rings and  $f : R \rightarrow S$  a ring homomorphism. Given  $a, b \in R$ , the following hold:

- (1)  $f(0_R) = 0_S$
- (2)  $f(-a) = -f(a)$
- (3)  $f(a - b) = f(a) - f(b)$
- (4) If  $a \in R$  is a unit, then  $f(a)$  is a unit and  $f(a^{-1}) = [f(a)]^{-1}$ .

*Proof.* Let  $R, S$  be rings and  $f : R \rightarrow S$  a ring homomorphism.

- (1) Take any  $a \in R$ . Then  $\underline{f(a) + 0_S} = f(a + 0_R) = \underline{f(a) + f(0_R)}$ , so  $f(0_R) = 0_S$ .
- (2)  $\underline{0_S} = f(0_R) = f(a + (-a)) = \underline{f(a) + f(-a)}$ , so  $f(a) + f(-a) = 0_S \implies f(-a) = -f(a)$ .
- (3)  $\underline{f(a - b)} = f(a + (-b)) = f(a) + f(-b) = f(a) + (-f(b)) = \underline{f(a) - f(b)}$ .
- (4) Let  $a \in R$  be a unit. Then there exists  $a^{-1} \in R$  such that  $aa^{-1} = 1$ . Then  $\underline{1_S} = f(1_R) = f(aa^{-1}) = \underline{f(a)f(a^{-1})}$  and  $\underline{1_S} = f(1_R) = f(a^{-1}a) = \underline{f(a^{-1})f(a)}$ , so  $f(a)$  is a unit and define  $[f(a)]^{-1} := f(a^{-1})$  to get  $f(a^{-1}) = [f(a)]^{-1}$ .

$\square$

### Definition: Isomorphism

Let  $f : R \rightarrow S$  be a ring homomorphism.  $f$  is an isomorphism if  $f$  is a bijection. Then  $R$  and  $S$  are isomorphic, written as  $R \simeq S$ .

### Definition: Kernel and Image

Let  $f : R \rightarrow S$  be a ring homomorphism.

→ The **kernel** of  $f$  is defined as  $\ker(f) := \{a \in R : f(a) = 0_S\}$ .

→ The **image** of  $f$  is defined as  $\text{Im}(f) := \{f(a) : a \in R\}$ .

**Proposition:** Given a ring homomorphism  $f : R \rightarrow S$ , the image of  $f$  is a subring of  $S$  and the kernel of  $f$  is a nonunital subring of  $R$ .

*Proof.* Let  $f : R \rightarrow S$  be a ring homomorphism. Then

**Im( $f$ ) is a subring of  $S$ :** Given  $f(a), f(b) \in \text{Im}(f)$ , we have the following:

$$(1) f(a) + f(b) = f(a + b) \in \text{Im}(f).$$

$$(2) f(a)f(b) = f(ab) \in \text{Im}(f).$$

$$(3) -f(a) = f(-a) \in \text{Im}(f).$$

$$(4) f(1_R) = 1_S \in \text{Im}(f).$$

so  $\text{Im}(f)$  is a subring of  $S$ .

**ker( $f$ ) is a nonunital subring of  $R$ :** Given  $a, b \in \ker(f)$ , we have the following:

$$(1) f(a + b) = f(a) + f(b) = 0_S + 0_S \in \ker(f).$$

$$(2) f(ab) = f(a)f(b) = 0_S \cdot 0_S \in \ker(f).$$

$$(3) f(-a) = -f(a) = -0_S = 0_S \in \ker(f).$$

$$(4) f(0_R) = 0_S \in \ker(f).$$

so  $\ker(f)$  is a nonunital subring of  $R$ . □

**Proposition:** Let  $f : R \rightarrow S$  be a ring homomorphism. Then, for any  $a \in \ker(f)$  and  $b \in R$ , we have  $ab, ba \in \ker(f)$ .

*Proof.*  $\underline{f(ab)} = f(a)f(b) = 0_S \cdot f(b) = \underline{0_S} = f(b) \cdot 0_S = f(b)f(a) = \underline{f(ba)} \in \ker(f)$ . □

### Definition: Initial Object

$\mathbb{Z}$  is the **initial object**. Let  $R$  be any ring. Then, there is a unique homomorphism  $f : \mathbb{Z} \rightarrow R$ . At  $n = 1$ ,  $1 \mapsto 1_R$ . At  $n = n + 1$ ,  $n + 1 \mapsto \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} + 1_R$ . The same is true for  $n < 0$ .  $f$  as defined above is a well-defined ring homomorphism.

## 2.2 Ideals

### Definition: Ideal

Let  $R$  be a ring and  $I \subseteq R$  a nonempty subset.  $I$  is an **ideal** of  $R$  if  $I$  is a nonunital subring such that for all  $a \in I$  and  $x \in R$ ,  $xa, ax \in I$ . This is often called the “*absorbing property*”.

**Remark:** The kernel of any ring homomorphism is an ideal. Further, all ideal can be realized as the kernel of a ring homomorphism.

### Definition: Principal Ideal

Let  $R$  be a commutative ring and  $a \in R$ . The **principal ideal**  $(a)$  is an ideal where  $(a) := \{ar : r \in R\}$ . We say “ $a$  generates  $I$ ”. Note that  $(a) \iff aR$ .

### Theorem

Let  $R$  be a commutative ring and  $a \in R$ . Then the principal ideal  $(a)$  is an ideal.

*Proof.* Suppose  $(a)$  is the principal ideal. Then,  $0 = a \cdot 0 \in (a)$ . Given  $ar_1, ar_2 \in (a)$ ,  $ar_1 + ar_2 = a(r_1 + r_2) \in (a)$ . Take  $ar \in (a)$ . Then  $-ar = a(-r) \in (a)$ . Take  $ar_1 \in (a), r \in R$ . Then  $(ar_1)r = a(r_1r) \in (a)$ . Because  $(a)$  is a nonunital subring with the absorbing property, it is an ideal.  $\square$

### Theorem

Let  $R$  be a ring and  $I_1, \dots, I_k$  be ideals. Then

- (1)  $I_1 + \dots + I_k = \{i_1 + \dots + i_k : i_j \in I_j\}$  is an ideal.
- (2)  $I_1 \cap \dots \cap I_k$  is an ideal.

*Proof.* Let  $R$  be a ring, and  $I_1, \dots, I_k$  be ideals.

**$I_1 + \dots + I_k = \{i_1 + \dots + i_k : i_j \in I_j\}$  is an ideal.**

- (1) Since  $I_j$  is an ideal,  $0 \in I_j$  so we get  $0 + \dots + 0 = 0 \in I_1 + \dots + I_k$ .
- (2) Take two elements  $a, b \in I_1 + \dots + I_k$ . We can rewrite  $a, b$  as,  $a = p_1 + \dots + p_k$  and  $b = q_1 + \dots + q_k$  for  $p_j, q_j \in I_j$ . Then  $a + b = (p_1 + \dots + p_k) + (q_1 + \dots + q_k) = (p_1 + q_1) + \dots + (p_k + q_k)$ , and since  $p_j + q_j \in I_j$  for all  $j \leq k$ , we get  $a + b \in I_1 + \dots + I_k$ .
- (3) Take any  $a \in I_1 + \dots + I_k$ . We can rewrite  $a$  as,  $a = p_1 + \dots + p_k$  for  $p_j \in I_j$ . Consider an element  $r \in R$ . Then,  $ar = (p_1 + \dots + p_k)r = p_1r + \dots + p_kr$ . Similarly,  $ar = r(p_1 + \dots + p_k) = rp_1 + \dots + rp_k$ . Since  $I_j$  is an ideal,  $p_jr, rp_j \in I_j$ . Then  $ar, ra \in I_1 + \dots + I_k$ .
- (4) Let  $a := a_1 + \dots + a_k \in I_1 + \dots + I_k$ . Since  $I_j$  is an ideal, there exists  $-a \in I_j$ , so we get  $-a_1 + \dots + -a_k = -(a_1 + \dots + a_k) = -a \in I_1 + \dots + I_k$ .

Because  $I_1 + \dots + I_k$  satisfies (1) - (4),  $I_1 + \dots + I_k$  is an ideal.



**$I_1 \cap \cdots \cap I_k$  is an ideal.**

- (1) Since  $I_j$  is an ideal,  $0 \in I_j$ , so  $0 \in I_1 \cap \cdots \cap I_k$ .
- (2) Take two elements  $a, b \in I_1 \cap \cdots \cap I_k$ . Then since each  $I_j$  is an ideal,  $a + b \in I_j$ . So,  $a + b \in I_1 \cap \cdots \cap I_k$ .
- (3) Take any  $a \in I_1 \cap \cdots \cap I_k$ . Consider an element  $r \in R$ . Then, since each  $I_j$  is an ideal,  $ar, ra \in I_j$ . Therefore,  $ar, ra \in I_1 \cap \cdots \cap I_k$ .
- (4) Take any  $a \in I_1 \cap \cdots \cap I_k$ . Then, since  $I_j$  is an ideal,  $-a \in I_j$ , so  $-a \in I_1 \cap \cdots \cap I_k$ .

Because  $I_1 \cap \cdots \cap I_k$  satisfies (1) - (4),  $I_1 \cap \cdots \cap I_k$  is an ideal.  $\square$

#### Definition: Multiple Generators

Let  $R$  be a commutative ring and  $a_1, \dots, a_k \in R$ . The ideal generated by  $a_1, \dots, a_k$  is given by  $(a_1) + \cdots + (a_k)$  and is written as  $(a_1, \dots, a_k)$ .

**Proposition:** Let  $F$  be a field. The only ideal of  $F$  are  $\{0\}$  and  $F$ .

*Proof.* Let  $I$  be a nonzero ideal of  $F$  and take  $a \in I$ . Then,  $1 = aa^{-1} \in I$ . Because  $1 \in I$ ,  $F = (1) = I$ .  $\square$

## 2.3 Quotient Rings

**Preface:** To generalize the construction of  $\mathbb{Z}/n$  to general rings, consider the following: given an ideal  $I \subseteq R$ , define equivalence where  $a \sim b$  if  $a - b \in I$ . We can then inherit  $(+, \cdot)$  from  $R$ . Given two equivalence classes  $[a], [b]$ , define  $[a] + [b] = [a + b]$  and  $[a] \cdot [b] = [ab]$ .

#### Definition: Congruent Modulo $I$

Let  $R$  be a ring,  $I \subseteq R$  and ideal, and  $a, b \in R$ .  $a$  and  $b$  are **congruent modulo  $I$**  if  $a - b \in I$ . We write  $a \equiv b \pmod{I}$ , or  $a + I = b + I$ .

**Remark:** The notation  $a + I := \{a + x : x \in I\}$  is precisely the congruence class modulo  $I$  containing  $a$ .

**Proposition:** Let  $R$  be a ring and  $I \subseteq R$  an ideal. Congruence modulo  $I$  is an equivalence relation.

*Proof.* Let  $R$  be a ring and  $I \subseteq R$  an ideal.

- (1) For any  $a \in R$ ,  $a - a = 0 \in I$ , so  $a \equiv a \pmod{I}$ .
- (2) Take  $a, b \in R$  such that  $a \equiv b \pmod{I}$ . Then  $a - b \in I$ . Since  $I$  is an ideal,  $-(a - b) = b - a \in I$ , so  $b \equiv a \pmod{I}$ .
- (3) Let  $a, b, c \in R$  such that  $a \equiv b \pmod{I}$  and  $b \equiv c \pmod{I}$ . Then  $a - b, b - c \in I$ . Then  $(a - b) + (b - c) = a + (-b + b) - c = a - c \in I$ , so  $a \equiv c \pmod{I}$ .

Since congruence modulo  $I$  satisfies (1) - (3), it is an equivalence relation.  $\square$

### Theorem

Let  $R$  be a ring,  $a, b, c, d \in R$ , and  $I \subseteq R$  and ideal. Suppose  $a \equiv c \pmod{I}$ ,  $b \equiv d \pmod{I}$ . Then  $a + b \equiv c + d \pmod{I}$  and  $ab \equiv cd \pmod{I}$ .

*Proof.* Since  $a - c, b - d \in I$ , we have that  $(a - c) + (b - d) = (a + b) - (c + d) \in I$ . Then by definition, we have  $a + b \equiv c + d \pmod{I}$ . Now consider the following:

$$\begin{aligned} ab - cd &= ab + 0 - cd \\ &= ab + (-bc + bc) - cd \\ &= (ab - bc) + (bc - cd) \\ ab - cd &= b(a - c) + c(b - d) \end{aligned}$$

Since  $a - c, b - d \in I$ ,  $ab - cd \in I$ , so  $ab \equiv cd \pmod{I}$ . □

**Notation:**  $(a + I) + (b + I) = (a + b) + I$  and  $(a + I)(b + I) = ab + I$ .

### Definition: Quotient Ring

Let  $R$  be a ring,  $a, b \in R$ , and  $I \subseteq R$  and ideal. The **quotient ring**  $R/I$  is the set of congruence classes modulo  $I$  with  $(+)$ ,  $(\cdot)$  defined as  $(a + I) + (b + I) = (a + b) + I$  and  $(a + I)(b + I) = ab + I$  respectively.

**Proposition:**  $R/I$  is a ring.

*Proof.* I'm not checking all 9 axioms lol. □

### Theorem

Let  $R$  be a ring and  $I \subseteq R$  and ideal. If  $R$  is commutative, then  $R/I$  is commutative.

*Proof.* Take  $a + I, b + I \in R/I$ . Then  $(a + I)(b + I) = ab + I$  and  $(a + I)(b + I) = ab + I$ , so  $ab + I = ba + I \implies (a + I)(b + I) = (b + I)(a + I)$ . □

**Note:** If  $R/I$  is commutative, it does **not** imply that  $R$  is commutative. For example, if  $I = R$ , then  $R/I \simeq \{0\}$ .

### Definition: Canonical Projection

Let  $R$  be a ring,  $I \subseteq R$  and ideal. Consider  $\pi : R \rightarrow R/I$  such that  $\pi(a) = a + I$ . This map is the **canonical projection**.

### Theorem

Let  $R$  be a ring,  $I \subseteq R$  and ideal. The canonical projection  $\pi : R \rightarrow R/I$  is a surjective ring homomorphism with  $\ker(\pi) = I$ .

*Proof.* Let  $R$  be a ring,  $I \subseteq R$  and ideal. Let  $\pi : R \rightarrow R/I$  be the canonical projection from  $R$  to  $R/I$ . Then

$$(1) \quad \pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b).$$

$$(2) \quad \pi(a \cdot b) = (a \cdot b) + I = (a + I) \cdot (b + I) = \pi(a) \cdot \pi(b).$$

$$(3) \quad \pi(1_R) = 1 + I = 1_{R/I}.$$

so  $\pi$  is a ring homomorphism. Take  $a + I \in R/I$ . Then  $\pi(a) = a + I$ . Moreover, if  $b \in [a + I]$ , then  $\pi(b) = a + I$ . So  $\pi$  is surjective. Finally, let  $a \in I$ . Then  $\pi(a) = a + I$  but  $a \equiv 0 \pmod{I}$ , so we have  $\pi(a) = a + I = 0_R + I = I$ . So,  $\ker(\pi) \subseteq I$ . Now suppose  $\pi(a) = 0_R + I$ . Then  $[a + I] = [0_R + I]$ , or  $a \equiv 0_R \pmod{I}$ . We can rewrite this to get  $a - 0_R = a \in I$ , so  $I \subseteq \ker(\pi)$ . Because  $\ker(\pi) \subseteq I$  and  $I \subseteq \ker(\pi)$ ,  $\ker(\pi) = I$ .  $\square$

The rest of this page is intentionally left blank

### Theorem (First Isomorphism Theorem)

Let  $f : R \rightarrow S$  be a ring homomorphism. The following hold:

→ There exists a unique homomorphism  $\bar{f} : R/\ker(f) \rightarrow S$  such that  $f = \bar{f} \circ \pi$ .

→  $R/\ker(f) \simeq \text{Im}(f)$ .

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \pi \downarrow & \nearrow \bar{f} & \\ R/\ker(f) & & \end{array}$$

*Proof.* Let  $f : R \rightarrow S$  be a ring homomorphism. Then

**$\bar{f}$  is well-defined:** Suppose  $a + \ker(f) = a' + \ker(f)$ . Then  $a - a' \in \ker(f)$ , so  $f(a - a') = 0 = f(a) - f(a')$ . This implies  $f(a) = f(a')$ , so  $\bar{f}$  is well-defined.

**$\bar{f}$  is a homomorphism:**

(1)  $\bar{f}(1_R + \ker(f)) = f(1_R) = 1_S.$

(2) Take  $a + \ker(f), b + \ker(f) \in R/\ker(f)$ . Then

$$\bar{f}((a + b) + \ker(f)) = f(a + b) = f(a) + f(b) = \bar{f}(a + \ker(f)) + \bar{f}(b + \ker(f))$$

(3) Take  $a + \ker(f), b + \ker(f) \in R/\ker(f)$ . Then

$$\bar{f}((a \cdot b) + \ker(f)) = f(a \cdot b) = f(a) \cdot f(b) = \bar{f}(a + \ker(f)) \cdot \bar{f}(b + \ker(f))$$

so  $\bar{f}$  is a homomorphism.

**$f = \bar{f} \circ \pi$ :** Take  $a \in R$ . Then,  $\bar{f} \circ \pi(a) = \bar{f}(\pi(a)) = \bar{f}(a + \ker(f)) = f(a).$

**$\bar{f}$  is unique:** Suppose we have another function  $g : R/\ker(f) \rightarrow S$  such that  $\bar{f} \neq g$ . Then there exists  $b \in R/\ker(f)$  such that  $g(b + \ker(f)) \neq \bar{f}(b + \ker(f))$ , so

$$g \circ \pi(a) = g(\pi(a)) = g(a + \ker(f)) \neq \bar{f}(a + \ker(f)) = f(a)$$

Therefore,  $\bar{f}$  is unique.

**$R/\ker(f) \simeq \text{Im}(f)$ :** Take  $a + \ker(f) \in \ker(\bar{f})$ . Then  $\bar{f}(a + \ker(f)) = f(a) = 0$ . Since  $a + \ker(f)$  was arbitrary, this holds for all  $a + \ker(f) \in \ker(\bar{f})$ , so  $\bar{f}$  is **injective**. Now take any  $y \in \text{Im}(f)$ . Then there is some  $z \in R$  such that  $f(z) = y$ . Set  $x := z + \ker(f) \in R/\ker(f)$ . Then  $\bar{f}(x) = \bar{f}(z + \ker(f)) = f(z) = y$ , so  $\bar{f}$  is **surjective**. Since  $\bar{f}$  is injective and surjective, it is **bijective**, and therefore  $R/\ker(f) \simeq \text{Im}(f)$ .  $\square$

The rest of this page is intentionally left blank

### Theorem (Correspondence Theorem)

Let  $R$  be a ring, and  $I \subseteq R$  an ideal. Consider the projection  $\pi : R \rightarrow R/I$  and let  $\bar{R} := R/I$ . Then

- (1) There is a bijective correspondence between ideals in  $R$  containing  $I$  and ideals of  $\bar{R}$  given by  $J \mapsto \pi(J) = \{r + I : r \in J\}$  and  $\bar{J} \mapsto \pi^{-1}(\bar{J})$  where  $J \subseteq R$  and  $\bar{J} \subseteq \bar{R}$  are ideals.
- (2) If an ideal  $J \subseteq R$  corresponds to  $\bar{J} \subseteq \bar{R}$ , then  $R/J \simeq \bar{R}/\bar{J}$ .

*Proof.* (1) To show that  $\pi(J)$  is an ideal of  $\bar{R}$ , take  $a, b \in \pi(J)$  and  $r + I \in \bar{R}$ . Then  $\pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b)$  and  $(a + I)(r + I) = ar + I \in \pi(J)$ . Similarly,  $ra + I \in \pi(J)$ . To show that  $\pi^{-1}(\bar{J})$  is an ideal of  $R$ , take  $a, b \in \pi^{-1}(\bar{J})$ . Then note that  $\pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b) \in \bar{J}$ , so  $a + b \in \pi^{-1}(\bar{J})$ . Also, note that  $\pi(ar) = ar + I = (a + I)(r + I) \in \bar{J}$ , so  $ar \in \pi^{-1}(\bar{J})$ . Similarly,  $rb \in \pi^{-1}(\bar{J})$ . So  $\pi(J)$  is an ideal of  $\bar{R}$  and  $\pi^{-1}(\bar{J})$  is an ideal in  $R$ .

**$\pi^{-1}(\pi(J)) = J$ :** Let  $a \in \pi^{-1}(\pi(J))$ . Then by definition of the pre-image under  $\pi$ , there exists  $x \in J$  such that  $\pi(a) = \pi(x) \in \pi(J)$ , or  $a + I = x + I$ , which implies that  $a - x \in I \subseteq J$ , so  $a \in J$ . Since  $a$  was arbitrary,  $\pi^{-1}(\pi(J)) \subseteq J$ . Now let  $b \in J$ . Then by definition,  $\pi(b) = b + I$ . Then,  $\pi^{-1}(\pi(b)) = \pi^{-1}(b + I)$  but by definition of the pre-image,  $\pi^{-1}(b + I) = b \in \pi^{-1}(\pi(J))$ . Since  $b$  was arbitrary,  $J \subseteq \pi^{-1}(\pi(J))$ . Since we have  $\pi^{-1}(\pi(J)) \subseteq J$  and  $\pi^{-1}(\pi(J)) \supseteq J$ ,  $\pi^{-1}(\pi(J)) = J$ .

**$\pi(\pi^{-1}(\bar{J})) = \bar{J}$ :** Let  $a + I \in \pi(\pi^{-1}(\bar{J}))$ . Then there exists  $x \in R$  such that  $x \in \pi^{-1}(\bar{J})$  and  $\pi(x) = a + I \in \bar{J}$ . Since  $a$  was arbitrary,  $\pi(\pi^{-1}(\bar{J})) \subseteq \bar{J}$ . Now let  $b + I \in \bar{J}$ . Then by definition,  $b + I$  is in the image of  $J$  under  $\pi$ , so  $b \in \pi^{-1}(\bar{J})$ . Then  $\pi(\pi^{-1}(b + I)) = \pi(b) = b + I \in \pi(\pi^{-1}(\bar{J}))$ . Since  $b + I$  was arbitrary,  $\bar{J} \subseteq \pi(\pi^{-1}(\bar{J}))$ . Since  $\pi(\pi^{-1}(\bar{J})) \subseteq \bar{J}$  and  $\pi(\pi^{-1}(\bar{J})) \supseteq \bar{J}$ ,  $\pi(\pi^{-1}(\bar{J})) = \bar{J}$ .

Therefore, there exists a bijective correspondence between the ideals  $J \supseteq I$  in  $R$  and the ideals  $\bar{J} \subseteq \bar{R}$ .

(2) Consider the canonical projection  $\phi : \bar{R} \rightarrow \bar{R}/\bar{J}$ . Since  $\phi$  and  $\pi$  are **surjective**, the composition  $\phi \circ \pi : R \rightarrow \bar{R}/\bar{J}$  is as well. By the **First Isomorphism Theorem**, we have  $\bar{R}/\ker(\phi \circ \pi) \simeq \bar{R}/\bar{J}$ .

**$\ker(\phi \circ \pi) = J$ :** Let  $\bar{J} = \pi(J)$ . Take  $a \in J$ . Then  $\phi \circ \pi(a) = \phi(\pi(a)) = \phi(a + I) = (a + I) + \bar{J}$ , but since  $a + I \in \bar{J}$ , we have that  $(a + I) + \bar{J} = 0 + \bar{J} \in \ker(\phi \circ \pi)$ . Since  $a$  was arbitrary,  $J \subseteq \ker(\phi \circ \pi)$ . Now take any  $b \in R$  such that  $\phi \circ \pi(b) = 0 + \bar{J}$ . Then,  $(b + I) + \bar{J} = 0 + \bar{J}$ . By definition,  $b + I \in \bar{J} = \pi(J)$ . Then  $b + I$  is the image of  $J$  under  $\pi$ , so  $b \in \pi^{-1}(\bar{J}) = \pi^{-1}(\pi(J)) = J$ . Since  $b$  was arbitrary,  $\ker(\phi \circ \pi) \subseteq J$ . Since  $J \subseteq \ker(\phi \circ \pi)$  and  $J \supseteq \ker(\phi \circ \pi)$ ,  $J = \ker(\phi \circ \pi)$ .

Therefore,  $R/J \simeq \bar{R}/\bar{J}$ . □

### Theorem (Chinese Remainder Theorem [Rings])

Let  $R$  be a commutative ring,  $a, b \in R$ , and  $I, J \subseteq R$  be ideals such that  $I + J = R$ . We can find  $x \in R$  such that

$$\begin{aligned}x &\equiv a \pmod{I} \\x &\equiv b \pmod{J}\end{aligned}$$

Moreover, if  $y$  is another solution, then  $y \equiv x \pmod{I \cap J}$ .

*Proof.* Because  $I + J = R$ , we can find  $i \in I$  and  $j \in J$  such that  $i + j = 1_R$ . Then  $i \equiv 1 \pmod{J}$  and  $j \equiv 1 \pmod{I}$ . Consider  $x := bi + aj$ . Then

$$\begin{aligned}x &= bi + aj \\&\equiv aj \pmod{I} \\&\equiv a \cdot 1 \pmod{I} \\x &\equiv a \pmod{I}\end{aligned}$$

and

$$\begin{aligned}x &= bi + aj \\&\equiv bi \pmod{J} \\&\equiv b \cdot 1 \pmod{J} \\x &\equiv b \pmod{J}\end{aligned}$$

Now suppose that  $y$  is another solution. Then  $y \equiv x \pmod{I}$  and  $y \equiv x \pmod{J}$ . By definition, this means that  $y - x \in I$  and  $y - x \in J$ , so  $y \equiv x \pmod{I \cap J}$ .  $\square$

**The rest of this page is intentionally left blank**

### Theorem (Chinese Remainder Theorem [Isomorphism])

Let  $R$  be a ring and  $I, J \subseteq R$  be ideals such that  $I + J = R$ . The quotient rings  $(R/I) \times (R/J)$  and  $R/(I \cap J)$  are isomorphic.

*Proof.* Consider  $f : (R/I) \times (R/J)$  given by  $a \mapsto (a + I, a + J)$ . Then

$$(1) \quad f(1_R) = (1_R + I, 1_R + J)$$

(2) Take  $a, b \in R$ . Then

$$f(a + b) = ((a + b) + I, (a + b) + J) = (a + I, a + J) + (b + I, b + J) = f(a) + f(b)$$

(3) Take  $a, b \in R$ .

$$f(a \cdot b) = ((a \cdot b) + I, (a \cdot b) + J) = (a + I, a + J) \cdot (b + I, b + J) = f(a) \cdot f(b)$$

so  $f$  is a homomorphism.

Take  $(a + I, b + J) \in (R/I) \times (R/J)$ . By the **Chinese Remainder Theorem (Rings)**, we can find  $x \in R$  such that  $x + I = a + I$  and  $x + J = b + J$ . Then,  $f(x) = (a + I, b + J)$ , so  $f$  is **surjective**. Suppose  $f(a) = 0$ . Then  $a \in I$  and  $a \in J$ , so  $a \in I \cap J$ . Now take  $a \in I \cap J$ . Then  $a \in I$  and  $a \in J$ , so  $a + I \in I$  and  $a + J \in J$ . By the **First Isomorphism Theorem**, we have  $R/(I \cap J) = R/\ker(f) \simeq \text{Im}(f) = (R/I) \times (R/J)$ .  $\square$

## 2.4 Prime and Maximal Ideals

**Preface:** All rings in this subsection are commutative rings.

### Definition: Prime Ideal

Let  $R$  be a commutative ring and let  $I \subsetneq R$  be a proper ideal.  $I$  is a **prime ideal** if, whenever  $ab \in I$  for  $a, b \in R$ , we have either  $a \in I$  or  $b \in I$ .

**Example:** Let  $R$  be an integral domain. Then  $(0)$  is prime since whenever  $ab \in (0)$ , we have that either  $a \in (0)$  or  $b \in (0)$ .

**Proposition:**  $(p) \subsetneq \mathbb{Z}$  is a prime ideal if and only if  $p \in \mathbb{Z}$  is prime.

*Proof.* Let  $p \in \mathbb{Z}$  be nonzero.

( $\implies$ ) Suppose  $(p) \subsetneq \mathbb{Z}$  is a prime ideal. Consider  $ab \in (p)$ . Then either  $a \in (p)$  or  $b \in (p)$ . By definition, we can write  $ab = pr$  for some  $r \in \mathbb{Z}$ , so  $p \mid ab$ . But we also have that either  $a = pq$  or  $b = ps$  for some  $q, s \in \mathbb{Z}$ , so either  $p \mid a$  or  $p \mid b$ . Then, since these two statements:

(1)  $p$  is prime.

(2) If  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .

are equivalent,  $p \in \mathbb{Z}$  is prime.

( $\impliedby$ ) Suppose  $p \in \mathbb{Z}$  is prime and consider the ideal  $(p) \subsetneq \mathbb{Z}$ . Consider  $ab \in \mathbb{Z}$  such that  $p \mid ab$ . Then either  $p \mid a$  or  $p \mid b$ . Since  $p \mid ab$ , we have that  $ab = pr$  for some  $r \in \mathbb{Z}$ , so  $ab \in (p)$ . By a similar argument, either  $a \in (p)$  or  $b \in (p)$ , so  $(p) \subsetneq \mathbb{Z}$  is a prime ideal.  $\square$

### Theorem

Let  $R$  be a commutative ring and let  $I \subsetneq R$  be a proper ideal. The quotient ring  $R/I$  is an integral domain if and only if  $I$  is prime.

*Proof.* Let  $R$  be a commutative ring and let  $I \subsetneq R$  be a proper ideal.

( $\implies$ ) Suppose  $R/I$  is an integral domain. Take  $ab \in I$ . Then  $(a+I)(b+I) = ab+I = 0+I$ . Since  $R/I$  is an integral domain, we have that either  $a+I = 0+I$  or  $b+I = 0+I$ . This implies that either  $a \in I$  or  $b \in I$ , so  $I \subsetneq R$  is prime.

( $\impliedby$ ) Suppose  $I$  is a prime ideal. Take  $ab+I \in R/I$ . Then  $ab+I = (a+I)(b+I) = 0+I$ . Since  $I$  is a prime ideal, either  $a \in I$  or  $b \in I$ . This implies that either  $a+I = I$  or  $b+I = I$ , so  $R/I$  has no zero divisors. This implies that  $R/I$  is an integral domain.  $\square$

### Definition: Maximal Ideal

Let  $R$  be a commutative ring and let  $I \subsetneq R$  be a proper ideal.  $I$  is a **maximal ideal** if, whenever there is an ideal  $J$  such that  $I \subsetneq J \subseteq R$ , we must have  $J = R$ .

### Theorem

Let  $R$  be a commutative ring and  $I \subsetneq R$  be a maximal ideal. Then  $I$  is a prime ideal.

*Proof.* Let  $R$  be a commutative ring and suppose  $I \subsetneq R$  is a maximal ideal. Take  $ab \in I$ . If  $a \in I$ , then we are done, so suppose not. Then consider  $I + (a) \supsetneq I$ . Since  $I$  is maximal, we have that  $I + (a) = R$ . Then  $1 = x + ar$  for some  $x \in I$ ,  $ar \in (a)$ . Multiplying both sides by  $b \in R$ , we get  $\underline{b} = b(x + ar) = \underline{bx} + \underline{abr}$ . Since  $ab \in I$ , we have that  $(ab)r \in I$ . Further, since  $x \in I$ ,  $xb \in I$ , so  $bx + abr = b \in I$ . This implies that  $I$  is a prime ideal.  $\square$

**Note:** From now on, I will only state “ $I$  is prime/maximal” instead of saying “ $I$  is a prime/maximal ideal”.

### Theorem

Let  $R$  be a commutative ring and  $I \subsetneq R$  be a proper ideal.  $I$  is maximal if and only if  $R/I$  is a field.

*Proof.* Let  $R$  be a commutative ring and suppose  $I \subsetneq R$  is a proper ideal.

( $\implies$ ) Suppose  $I$  is maximal. Pick a nonzero  $a+I \in R/I$ . Since  $a+I \neq 0+I$ ,  $a \notin I$ . Consider  $I+(a) \supsetneq I$ . Since  $I$  is maximal, we have that  $I+(a) = R$ . Then  $1 = x+ab$  for some  $x \in I$ ,  $ab \in (a)$ , so we have  $(x+ab)+I = (x+I)+(ab+I) = 1+I$ . Since  $x \in I$ , we have that  $x+I = 0+I$ . This implies that  $(x+I)+(ab+I) = (0+I)+(ab+I) = (a+I)(b+I) = 1+I$ . So  $a+I \in R/I$  is a unit. Since  $a+I \in R/I$  was arbitrary,  $R/I$  is a field.

( $\impliedby$ ) Suppose  $R/I$  is a field. Pick  $a \in R \setminus I$ . Then  $a+I \in R/I$  is nonzero, so there exists  $b+I \in R/I$  such that  $(a+I)(b+I) = ab+I = 1+I$ . Then  $ab-1 \in I$ , so there exists  $x \in I$  such that  $x = ab-1$ , or  $1 = ab-x$ . Then since  $-x \in I$  and  $ab \in (a)$ , we have that  $ab-x = 1 \in I+(a)$ , so  $I+(a) = R$ . Therefore,  $I$  is maximal.  $\square$



### 3 Polynomial Rings over Fields

**Preface:** Throughout this section,  $F$  is a field and  $F[x]$  are the polynomials with coefficients in  $F$ . Recall that given  $f \in F[x]$ , we can uniquely express  $f(x)$  as  $\sum_{i=0}^n a_i x^i$ , where  $a_n$  is nonzero.

**Note:** The notation  $f(x)$  and  $f$  are interchangeable.

#### Definition: Associate

Let  $f, g \in F[x]$ .  $f$  and  $g$  are **associates** if there is some nonzero  $c \in F$  such that  $g = cf$ .

#### Definition: Degree

Let  $f \in F[x]$  be expressed as  $f(x) = \sum_{i=0}^n a_i x^i$ , where  $a_n \neq 0$ . The **degree** of  $f$  is written as  $\deg(f) = n$ .

Let  $f, g \in F[x]$ . The following hold:

- (1)  $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ .
- (2)  $\deg(fg) = \deg(f) + \deg(g)$ .

**Note:** The zero polynomial has a degree of  $-\infty$  by convention.

#### Definition: Monic Polynomial

Let  $f \in F[x]$ .  $f$  is **monic** if its leading term is 1.

### Theorem (Division Algorithm [Polynomials])

Let  $f, g \in F[x]$  such that  $g \neq 0$ . Then there are unique polynomials  $q, r \in F[x]$  such that  $f = gq + r$ , where  $\deg(r) < \deg(g)$ .

*Proof. Existence:* Let  $f, g \in F[x]$  such that  $g \neq 0$  and consider  $S := \{f - sg : s \in F[x]\}$ . If  $s$  is the zero polynomial, then  $f - sg = f - 0g = f \in S$ , so  $S$  is not empty. Choose  $f - sg \in S$  to be of least degree, and define  $q := s, r := f - sg$ . Then  $r = f - sg = f - qg$ , or  $f = gq + r$ . Since  $g \neq 0$ , we have that  $\deg(g) \geq 0$ . Suppose for the sake of contradiction that  $\deg(r) \geq \deg(g)$ . Then  $r = \sum_{i=0}^n r_i x^i$  and  $g = \sum_{i=0}^m g_i x^i$  where  $n \geq m$ . Since  $\deg(r) = n, \deg(g) = m$ , we have that  $r_n \neq 0$  and  $g_m \neq 0$ ; i.e. they are units. Now consider  $t := r_n x^n \cdot (g_m x^m)^{-1} = r_n g_m^{-1} x^{n-m}$ . Then

$$tg = (r_n g_m^{-1} x^{n-m}) \cdot \left( \sum_{i=0}^m g_i x^i \right) = \left( \sum_{i=0}^{m-1} r_n g_m^{-1} g_i x^{n-m+i} \right) + r_n x^n$$

so

$$\begin{aligned} r - tg &= \left( \sum_{i=0}^{n-1} r_i x^i \right) + r_n x^n - \left( \left( \sum_{i=0}^{m-1} r_n g_m^{-1} g_i x^{n-m+i} \right) + r_n x^n \right) \\ &= \left( \sum_{i=0}^{n-1} r_i x^i \right) - \sum_{i=0}^{m-1} r_n g_m^{-1} g_i x^{n-m+i} \end{aligned}$$

so  $\deg(r - tg) \leq n - 1 < n = \deg(r)$ . But we have that  $r = f - gs$ , so we get

$$r - tg = (f - gs) - tg = f - g(s + t)$$

Since  $s + t \in F[x]$ , we have that  $r - tg \in S$ , but  $r$  was chosen to have the lowest degree and  $\deg(r - tg) < \deg(r)$ , a contradiction. Therefore,  $\deg(r) < \deg(g)$ .

**Uniqueness:** Suppose  $f = gq + r = gq' + r'$  for  $q, q', r, r' \in F[x]$ . Then

$$\begin{aligned} gq + r &= gq' + r' \\ g(q - q') &= r - r' \end{aligned}$$

so  $g \mid (r - r')$ . But  $\deg(r - r') < \deg(g)$ , so  $r = r'$ . Since  $F$  is a field and  $g \neq 0$ , this implies that  $q = q'$ . Therefore,  $q, r \in F[x]$  are unique.  $\square$

### Definition: Divides (Polynomials)

Let  $f, g \in F[x]$ .  $f$  **divides**  $g$  if there is a polynomial  $s \in F[x]$  such that  $fs = g$ . Then  $f$  is a **divisor** of  $g$ . We write  $f \mid g$ .

**Proposition:** Let  $f, g \in F[x]$ ,  $g \neq 0$ , and suppose  $f$  divides  $g$ . Then  $\deg(f) \leq \deg(g)$ .

*Proof.* Let  $f, g \in F[x]$ ,  $g \neq 0$  and suppose  $f \mid g$ . Then there exists  $s \in F[x]$  such that  $fs = g$ . Since  $g \neq 0$ , we have that  $\deg(g) \geq 0$ . Since  $F$  is a field, we have that  $f \neq 0$  and  $s \neq 0$ , so  $\deg(f) \geq 0$  and  $\deg(s) \geq 0$ . Then  $\deg(g) = \deg(fs) = \deg(f) + \deg(s)$ . This implies that  $\deg(f) \leq \deg(g)$ .  $\square$

### Definition: Greatest Common Divisor (gcd) (Polynomials)

Let  $f, g \in F[x]$  be polynomials such that either  $f \neq 0$  or  $g \neq 0$ . The **greatest common divisor** of  $f$  and  $g$  is the monic polynomial of largest degree that divides  $f$  and  $g$ . That is, the greatest common divisor  $d$  of  $f$  and  $g$  is the monic polynomial that satisfies the following:

- (1)  $d \mid f$  and  $d \mid g$ .
- (2) If  $a \mid f$  and  $a \mid g$ , then  $a \mid d$ .

If  $d$  is the greatest common divisor of  $f$  and  $g$ , we write  $d = \gcd(f, g) = (f, g)$ .

### Theorem (Bezout's Identity [Polynomials])

Let  $f, g \in F[x]$  such that either  $f \neq 0$  or  $g \neq 0$ . There exist  $m, n \in F[x]$  such that  $fm + gn = d$ , where  $d = (f, g)$ .

*Proof.* Let  $f, g \in F[x]$  such that either  $f \neq 0$  or  $g \neq 0$ . Consider the set  $S = \{fm + gn : m, n \in F[x]\}$ . If  $m = f, n = g$ , then since at least one of  $f, g$  is nonzero, we have  $0 \neq fm + gn = f^2 + g^2 \in S$ , so  $S$  is not empty. By the well-ordering principle, choose the polynomial  $s = fm + gn \in S$  of smallest degree, and consider  $f = sq + r$  for  $\deg(r) < \deg(g)$ . Rearranging the second equation, we get

$$\begin{aligned} f &= sq + r \\ r &= f - sq \\ &= f - (fm + gn)q \\ r &= f(1 - mq) + g(-nq) \end{aligned}$$

This implies that  $r \in S$ . We also have that  $\deg(r) < \deg(g)$ , but since  $s$  was chosen to be the smallest element in  $S$ , this forces  $r = 0$ . Then  $f = sq + r = sq$ , so  $s \mid f$ . Similarly,  $s \mid g$ . Since  $s \mid f$  and  $s \mid g$ ,  $s \leq d$ . But  $d \mid f$  and  $d \mid g$  by definition, so  $d \mid s$  which implies that  $d \leq s$ . Therefore,  $d = s$ , where  $s$  is a linear combination of  $f$  and  $g$ . So, there exist  $m, n \in F[x]$  such that  $d = fm + gn$ , where  $d = (f, g)$ .  $\square$

### Theorem

Let  $a, b, c \in F[x]$ . Suppose  $a \mid bc$  such that  $(a, b) = 1$ . Then  $a \mid c$ .

*Proof.* Let  $a, b, c \in F[x]$ , and suppose  $a \mid bc$  such that  $(a, b) = 1$ . Then we can write 1 as a linear combination of  $a$  and  $b$ ; i.e.  $am + bn = 1$  for  $m, n \in F[x]$ . We also have that  $aq = bc$  for some  $q \in F[x]$ . Then

$$\begin{aligned} 1 &= am + bn \\ c &= c(am + bn) \\ &= acm + (bc)n \\ &= acm + (aq)n \\ c &= a(cm + qn) \end{aligned}$$

which implies that  $a \mid c$ . □

## 3.1 Irreducibility

### Definition: Irreducible

Let  $f \in F[x]$  be nonzero and nonconstant.  $f$  is **irreducible** if its only factors are units and associates. Otherwise,  $f$  is **reducible**. That is,  $f$  is reducible if there exist polynomials  $a, b \in F[x]$  of lower degree such that  $ab = f$ .

### Theorem

Let  $p \in F[x]$ . The following are equivalent statements:

- (1)  $p$  is irreducible.
- (2) If  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .
- (3) If  $p = ab$ , then either  $a$  or  $b$  is a unit.

*Proof.* Let  $p \in F[x]$ .

(1)  $\implies$  (2) Suppose  $p$  is irreducible and  $p \mid ab$ . If  $p \mid a$ , then we are done, so suppose not. Then  $p \nmid a$  and  $(p, a) = 1$  which implies  $p \mid b$ .

(2)  $\implies$  (3) Suppose that if  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ . Let  $p = ab$ . Then  $p \mid p = ab$ , so  $p \mid a$  or  $p \mid b$ . Without loss of generality, suppose  $p \mid a$ . Then  $\deg(p) \leq \deg(a)$ . But since  $p = ab$ , we have that  $\deg(a), \deg(b) \leq \deg(p)$ . So,  $\deg(p) = \deg(a)$ , which implies that  $b$  is a unit.

(3)  $\implies$  (1) Suppose that if  $p = ab$ , then either  $a$  or  $b$  is a unit. Without loss of generality, suppose  $a$  is a unit. Then  $\deg(a) = 0$ , so  $\deg(p) = \deg(ab) = \deg(a) + \deg(b) = \deg(b)$ . This implies that  $b$  is an associate of  $p$ . Therefore, the only factors of  $p$  are units and associates, so  $p$  is irreducible. □

### Corollary

Let  $p \in F[x]$  be irreducible. If  $p \mid a_1 \cdots a_n$ , then  $p \mid a_i$  for some  $i$ .

*Proof.* Let  $p \in F[x]$  be irreducible. We will induct on  $n \in \mathbb{N}$ . At  $n = 2$ , if  $p \mid a_1 a_2$ , then  $p \mid a_1$  or  $p \mid a_2$ . Assume the base case holds for some  $n \geq 2$ . At  $n = n + 1$ , consider  $p \mid a_1 \cdots a_n \cdot a_{n+1}$ . Then if  $p \mid a_{n+1}$ , we are done. Otherwise, by the inductive hypothesis, we have that  $p \mid a_i$  for some  $i \leq n$ . Therefore, if  $p \mid a_1 \cdots a_n$ , then  $p \mid a_i$  for some  $i$ .  $\square$

### Theorem (Unique Factorization [Polynomials])

Let  $f \in F[x]$  be nonzero and nonconstant.  $f$  can be written as a product of irreducible polynomials. Moreover, if  $f = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$  are two irreducible factorizations, then  $n = m$  and there is a permutation  $\sigma$  on  $\{1, \dots, n\}$  such that  $p_i$  and  $q_{\sigma(i)}$  are associates.

*Proof. Existence:* Suppose for the sake of contradiction that there exist polynomials that cannot be written as a product of irreducible polynomials. Let  $S$  contain such polynomials. Then since  $S$  is not empty, pick  $f$  to be the polynomial of least degree. Then if  $f = pq$ , we have that  $\deg(p), \deg(q) \leq \deg(f)$ . But  $f$  was chosen to be the polynomial with smallest degree, so  $p, q \notin S$ . Then  $p, q$  can be written as a product of irreducible polynomials which implies that  $f$  can be written as a product of irreducible polynomials, a contradiction. Therefore,  $S$  is empty which implies that all nonzero and nonconstant  $f \in F[x]$  can be written as a product of irreducible polynomials.

**Uniqueness:** Suppose  $p_1 \cdots p_n = q_1 \cdots q_m$ . Without loss of generality, suppose  $n \leq m$ . Then  $p_1 \mid q_1 \cdots q_m$ . Without loss of generality, let  $p_1 \mid q_1$ . Then  $p_1$  and  $q_1$  are associates since they are both irreducible. Then  $q_1 = c_1 p_1$  for some unit  $c_1 \in F$ , so we have that  $p_1 \cdots p_n = c_1 p_1 \cdot q_2 \cdots q_m$ . Since  $F$  is a field, we can apply the cancellation property to cancel  $p_1$ , which yields  $p_2 \cdots p_n = c_1 q_2 \cdots q_m$ . Continuing this process inductively, we have that  $p_{m+1} \cdots p_n = c_1 \cdots c_m$ . Suppose for the sake of contradiction that  $m < n$ . Then  $0 < \deg(p_{m+1} \cdots p_n) = \deg(c_1 \cdots c_m) = 0$ , a contradiction. Therefore,  $m = n$  and there is a unique permutation  $\sigma$  on  $\{1, \dots, n\}$  such that  $p_i = q_{\sigma(i)}$ .  $\square$

## 3.2 Roots

### Definition: Root

Let  $f \in F[x]$ .  $a \in F$  is a **root** of  $f$  if  $f(a) = 0$ .

### Lemma

Let  $f \in F[x]$  and let  $a \in F[x]$  be a root of  $f$ . The remainder of  $f(x)$  divided by  $x - a$  is  $f(a)$ .

*Proof.* Let  $f \in F[x]$ . We can express  $f$  as  $f(x) = (x - a)q(x) + r(x)$  for unique  $q, r \in F[x]$ . Then  $f(a) = (a - a)q(a) + r = 0 + r = \underline{r}$ .  $\square$

### Theorem

Let  $f \in F[x]$  and  $a \in F$ .  $a$  is a root of  $f$  if and only if  $x - a$  is a factor of  $f$ .

*Proof.* Let  $f \in F[x]$  and  $a \in F$ .

( $\implies$ ) Suppose  $a$  is a root of  $f$ . We can express  $f$  as  $f(x) = (x - a)q(x) + r(x)$  for unique  $q, r \in F[x]$ . Then from the **Lemma** above, we have that  $f(a) = r$ , but since  $a$  is a root,  $f(a) = 0$ , so  $r = 0$  which implies that  $f(x) = (x - a)q(x)$ , or  $(x - a) \mid f$ .

( $\impliedby$ ) Suppose  $x - a$  is a factor of  $f$ . Then  $(x - a) \mid f$ , or  $f(x) = (x - a)q(x)$ . Then  $f(a) = (a - a)q(a) = 0$ .  $\square$

### Corollary

Let  $f \in F[x]$  such that  $\deg(f) = n > 0$ .  $f$  has at most  $n$  roots.

*Proof.* Let  $f \in F[x]$  such that  $\deg(f) = n > 0$ . We will induct on  $n \in \mathbb{N}$ . At  $n = 1$ , we have  $f(x) = a_0 + a_1x$ . Clearly,  $f$  has at most one root. Assume the base case holds for all  $1 \leq k < n$ . At  $k = n$ , we can express  $f$  as  $f(x) = (x - r)q(x)$ , where  $r \in F$  is a root of  $f$ . We have that  $\deg(q) = n - 1$ , so by the inductive hypothesis,  $q$  has at most  $n - 1$  roots. Then  $f$  has at most  $1 + (n - 1) = n$  roots. Since  $k$  was arbitrary, this holds for all  $n \in \mathbb{N}$ .  $\square$

### 3.3 Quotienting by Irreducibles

#### Theorem

Let  $p \in F[x]$  be a nonzero, nonconstant polynomial. The following are equivalent:

- (1)  $p$  is irreducible.
- (2)  $(p)$  is maximal.
- (3)  $(p)$  is prime.

*Proof.* Let  $p \in F[x]$ .

(1)  $\implies$  (2) Suppose  $p$  is irreducible. Consider the ideal  $(p) \subseteq F[x]$ . Take  $a \in F[x] \setminus (p)$ . If  $a$  is a unit, then  $(p) + (a) = F[x]$ , so suppose not. Then we have that  $(p, a) = 1$ , so we can write  $pf + ag = 1$  for  $f, g \in F[x]$ , so  $(p) + (a) = (1) = F[x]$ . Therefore,  $(p)$  is maximal.

(2)  $\implies$  (3) Suppose  $(p)$  is maximal. Since all maximal ideals are prime,  $(p)$  is prime.

(3)  $\implies$  (1) Suppose  $(p)$  is prime. Consider  $ab \in (p)$ . Then  $ab = pr$  for some  $r \in F[x]$ , so  $p \mid ab$ . Then since  $p$  is prime, we have that either  $a \in (p)$  or  $b \in (p)$ . Without loss of generality, suppose  $a \in (p)$ . Then  $a = ps$  for some  $s \in F[x]$ , so  $p \mid a$ . Since the following statements:

- (1)  $p$  is irreducible.
- (2) If  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .
- (3) If  $p = ab$ , then either  $a$  or  $b$  is a unit.

are equivalent,  $p$  is irreducible. □

#### Corollary

Let  $p \in F[x]$  be a nonzero, nonconstant polynomial. The following are equivalent:

- (1)  $p$  is irreducible.
- (2)  $F[x]/(p)$  is a field.
- (3)  $F[x]/(p)$  is prime.

**Note:** Let  $p \in F[x]$  be an irreducible with  $p(x) = \sum_{i=0}^n a_i x^i$ ,  $a_n \neq 0$ . The field  $F[x]/(p)$  consists of elements that are of the form  $(p) + \sum_{i=0}^n c_i x^i$ ,  $c_n, c_i \in F$ . Moreover,  $\sum_{i=0}^n a_i x^i + (p)$  is the zero element. So,  $F[x]/(p)$  is  $F[x]$  rooted at  $p$ .

## 4 Integral Domains

**Preface:** Recall that a commutative ring  $R$  is an integral domain if, whenever  $ab = 0$  for  $a, b \in R$ , we have either  $a = 0$  or  $b = 0$ .

### Definition: Associate (Integral Domains)

Let  $R$  be an integral domain, and let  $a, b \in R$ .  $a$  and  $b$  are **associates** if there exists a unit  $c$  such that  $a = bc$ .

**Proposition:** Let the relation that two elements are associates be defined above, and written as  $a \sim b$ .  $\sim$  is an equivalence relation.

*Proof.* Let  $R$  be an integral domain, and let  $a, b, c \in R$ .

- (1) Pick  $d = 1$ . Then  $\underline{a} = a \cdot 1 = \underline{a}$ , so  $a$  and  $a$  are associates. Therefore,  $\sim$  is **reflexive**.
- (2) Suppose  $a \sim b$ . Then  $a = bd$  for some unit  $d \in R$ , so there exists  $d^{-1} \in R$  such that  $dd^{-1} = 1$ . Multiplying both sides of the equation by  $d^{-1}$ , we get  $\underline{ad^{-1}} = bd \cdot d^{-1} = b \cdot 1 = \underline{b}$ , so  $b$  and  $a$  are associates. Therefore,  $\sim$  is **symmetric**.
- (3) Suppose  $a \sim b$  and  $b \sim c$ . Then  $a = bd$ ,  $b = ce$  for units  $d, e \in R$ . Then  $\underline{a} = bd = (ce)d$ . Since  $d, e$  are units, there exist  $d^{-1}, e^{-1} \in R$ . Consider  $d^{-1}e^{-1} \in R$ . Multiplying  $\underline{d^{-1}e^{-1}}$  to both sides of the equation, we get  $\underline{a \cdot d^{-1}e^{-1}} = c(ed) \cdot d^{-1}e^{-1} = ce \cdot 1 \cdot e^{-1} = c \cdot 1 = \underline{c}$ , so  $a$  and  $c$  are associates. Therefore,  $\sim$  is **transitive**.

Because  $\sim$  satisfies (1) - (3),  $\sim$  is an equivalence relation. □

### Definition: Divides (Integral Domains)

Let  $R$  be an integral domain, and let  $a, b \in R$ .  $a$  **divides**  $b$  if we can find  $q \in R$  such that  $aq = b$ . We write  $a \mid b$ .

### Definition: Irreducible (Integral Domains)

Let  $R$  be an integral domain, and let  $p \in R$  be a nonunit.  $p$  is **irreducible** if the only divisors of  $p$  are units and associates of  $p$ .

**Proposition:** Let  $R$  be an integral domain.  $p \in R$  is irreducible if and only if whenever  $p = ab$ , either  $a$  or  $b$  is a unit.

*Proof.* Let  $R$  be an integral domain and  $p \in R$ .

( $\implies$ ) Suppose  $p$  is irreducible. Then  $p \mid p = ab$ . If  $a$  is a unit, then we are done, so suppose not. Then  $a$  is an associate of  $p$ , so  $b$  is a unit.

( $\impliedby$ ) Suppose “ $p = ab$  implies that either  $a$  or  $b$  is a unit”. Let  $a \in R$  such that  $a \mid p$ . Then  $p = ab$  for some  $b \in R$ . If  $a$  is a unit, then  $b$  is an associate of  $p$ . If  $b$  is a unit, then  $a$  is an associate of  $p$ . In either case, the only factors of  $p$  are units and associates, so  $p$  is irreducible. □



### Definition: Prime (Integral Domains)

Let  $R$  be an integral domain and let  $p \in R$  be a nonunit.  $p$  is prime if, whenever  $p \mid ab$ , then either  $p \mid a$  or  $p \mid b$ .

### Theorem

Let  $R$  be an integral domain, and let  $p \in R$  be prime. Then  $p$  is irreducible.

*Proof.* Let  $R$  be an integral domain. Let  $p \in R$  is prime and suppose  $p = ab$ . Then either  $p \mid a$  or  $p \mid b$ . Without loss of generality, suppose  $p \mid a$ . Then  $a = pc$  for some  $c \in R$ . Then  $p = ab = (pc)b$ . Since  $R$  is an integral domain, we apply the cancellation property to get  $1 = cb$ . This implies that  $b$  is a unit.  $\square$

**Note:** Irreducibles need not be prime. Take, for example, this bullshit:  $R = \mathbb{Z}[\sqrt{-5}]$ . Here, 2 and 3 are irreducible but not prime since  $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ , and  $2, 3 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$  but  $2, 3 \nmid (1 + \sqrt{-5})$  and  $2, 3 \nmid (1 - \sqrt{-5})$ .

### Theorem

Let  $R$  be an integral domain, and let  $p \in R$ . The principal ideal  $(p)$  is prime if and only if  $p$  is prime.

*Proof.* Let  $R$  be an integral domain and  $p \in R$  such that  $(p) \subseteq R$  is principal.

( $\implies$ ) Suppose  $(p)$  is prime. Take  $ab \in (p)$ . Then  $ab = pr$  for some  $r \in R$ , so  $p \mid ab$ . Since  $(p)$  is prime, either  $a \in (p)$  or  $b \in (p)$ . Then either  $p \mid a$  or  $p \mid b$ , so  $p$  is prime.

( $\impliedby$ ) Suppose  $p$  is prime. Let  $a, b \in R$  such that  $ab \in (p)$ . Then  $ab = pr$  for some  $r \in R$ , so  $p \mid ab$ . Since  $p$  is prime, either  $p \mid a$  or  $p \mid b$ ; that is, either  $a \in (p)$  or  $b \in (p)$ . This implies that  $(p)$  is prime.  $\square$

**Notation:** Let  $R$  be an integral domain. Define  $R^*$  to be the nonzero elements of  $R$ .

### Lemma

Let  $R$  be an integral domain. Consider  $S(R) := \{(a, b) : a, b \in R; b \neq 0\}$ . The relation  $(a, b) \sim (a', b')$  if and only if  $ab' = a'b$  forms an equivalence relation.

*Proof.* Let  $R$  be an integral domain, and consider  $S(R) := \{(a, b) : a, b \in R; b \neq 0\}$ . Let  $(a, b), (c, d), (e, f) \in S(R)$ .

(1)  $(a, b) \sim (a, b) \iff ab = ba \iff ab = ab \iff (a, b) \sim (a, b)$ . Therefore,  $\sim$  is **reflexive**.

(2)  $(a, b) \sim (c, d) \iff ad = bc \iff ad = bc \iff bc = ad \iff (c, d) \sim (a, b)$ . Therefore,  $\sim$  is **symmetric**.

(3) Suppose  $(a, b) \sim (c, d) \iff ad = bc$  and  $(c, d) \sim (e, f) \iff cf = de$ . Then

$$\begin{aligned} ad &= bc \\ (ad)f &= b(cf) \\ (bc)f &= b(de) \\ (af)d &= (be)d \\ af = be &\iff (a, b) \sim (e, f) \quad d \neq 0, \text{ so apply cancellation property} \end{aligned}$$

Therefore,  $\sim$  is **transitive**.

Because  $\sim$  satisfies (1) - (3),  $\sim$  is an equivalence relation.  $\square$

### Definition: Addition and Multiplication in $S(R)$

Define  $+$  and  $\cdot$  in  $S(R)$  by  $(a, b) + (c, d) = (ad + bc, bd)$  and  $(a, b) \cdot (c, d) = (ab, cd)$ .

### Lemma

Suppose  $R$  is an integral domain. Suppose  $(a, b) \sim (a', b')$  and  $(c, d) \sim (c', d')$ , where  $(a, b), (a', b'), (c, d), (c', d') \in S(R)$ . Then  $(ad, bc) \sim (a'd', b'c')$  and  $(ad + bc, bd) \sim (a'd' + b'c', b'd')$ .

*Proof.* Suppose  $R$  is an integral domain and let  $(a, b) \sim (a', b')$  and  $(c, d) \sim (c', d')$ , where  $(a, b), (a', b'), (c, d), (c', d') \in S(R)$ . By definition, we have that  $ab' = a'b$  and  $cd' = c'd$ . Then

$$\underline{ad \cdot b'd'} = (ab')(cd') = (a'b)(c'd) = \underline{a'd' \cdot b'c'}$$

and

$$\begin{aligned} (ad + bc) \cdot b'd' &= adb'd' + bcb'd' \\ &= (ab')dd' + (cd')bb' \\ &= (a'b)dd' + (c'd)bb' & ab' = a'b, cd' = c'd \\ &= (a'd')(bd) + (b'c')(bd) \\ (ad + bc) \cdot b'd' &= (a'd' + b'c') \cdot bd \end{aligned}$$

So  $(ad, bc) \sim (a'd', b'c')$  and  $(ad + bc, bd) \sim (a'd' + b'c', b'd')$ .  $\square$

### Definition: Field of Fractions

Let  $R$  be an integral domain. Define  $\text{Frac}(R) = S(R)/\sim$  as the **field of fractions** for  $R$ , where addition and multiplication are defined by  $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$  and  $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$ , respectively. **Notation:** We will refer to  $[(a, b)]$  as  $\frac{a}{b}$ .

### Theorem

Let  $R$  be an integral domain.  $\text{Frac}(R)$  forms a field, and  $R$  can be viewed as a subring.

*Proof.* I'm not checking the ring axioms for  $\text{Frac}(R)$  lol.

Let  $R$  be an integral domain. Take  $\frac{a}{b} \in \text{Frac}(R)$  to be nonzero. Then since  $a, b \neq 0$ , the inverse of  $\frac{a}{b}$  is  $\frac{b}{a}$ . Consider the function  $f : R \rightarrow \text{Frac}(R)$  with  $r \mapsto \frac{r}{1}$ . Then

- (1)  $f(a + b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$ , so  $f$  is **closed under addition**.
- (2)  $f(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a) \cdot f(b)$ , so  $f$  is **closed under multiplication**.
- (3)  $f(1_R) = \frac{1_R}{1} = 1_{\text{Frac}(R)}$ , so the **multiplicative identity is preserved**.

so  $f$  is a ring homomorphism. Therefore,  $R$  is a subring of  $\text{Frac}(R)$ . □

### Corollary

Let  $F$  be a field.  $\text{Frac}(F) \simeq F$ .

*Proof.* Let  $F$  be a field. Consider the ring homomorphism  $f : F \rightarrow \text{Frac}(F)$  with  $r \mapsto \frac{r}{1}$ . Take a nonzero  $r \in R$ . Then  $f(r) = \frac{r}{1} \neq 0$ , so  $r \notin \ker(f)$ . This implies that  $\ker(f) = \{0\}$ , so  $f$  is **injective**. Take any  $\frac{a}{b} \in \text{Frac}(R)$  for  $a, b \in R$ . Since  $b \neq 0$ , there exists  $b^{-1} \in R$  such that  $bb^{-1} = 1$ . Consider  $x = ab^{-1} \in R$ . Then

$$\begin{aligned} a &= a \cdot 1 \\ &= a \cdot bb^{-1} \\ &= ab^{-1} \cdot b \\ a \cdot 1 &= x \cdot b \iff (a, b) \sim (x, 1) \end{aligned}$$

so  $\underline{f(x)} = \frac{x}{1} = \frac{ab^{-1}}{1} = \frac{a}{b}$ , which shows that  $f$  is **surjective**. Since  $f$  is injective and surjective,  $f$  is a **bijection**. □

## 4.1 Euclidean Domains

### Definition: Norm

Let  $R$  be an integral domain. A **norm** is a non-negative function  $N : R \rightarrow \mathbb{Z}$  such that

- (1)  $N(0_R) = 0$ .
- (2) Given  $a, b \in R$  with  $b \neq 0$ , there exists  $q$  such that  $a = bq + r$  where  $r = 0$  or  $N(r) < N(b)$ .

### Definition: Euclidean Domain

Let  $R$  be an integral domain.  $R$  is a **Euclidean domain** if there exists a norm function  $N : R \rightarrow \mathbb{Z}$ .

### Theorem

Let  $R$  be a Euclidean domain, and let  $I \subseteq R$  be an ideal.  $I$  is principal.

*Proof.* If  $I = \{0\}$ , then  $I = (0)$  which is principal, so we are done. If  $I \neq \{0\}$ , Then pick a nonzero  $d \in I$  to have the smallest nonzero norm.

$((d) \subseteq I)$  Since  $d \in I$ , we have that  $ad, da \in I$  for all  $a \in R$  by definition, so  $(d) \subseteq I$ .

$((d) \supseteq I)$  Take  $a \in I$ . Since  $d \neq 0$ , we can write  $a = dq + r$  for some  $q \in R$ . Then since  $a, dq \in I$ , we necessarily have that  $r \in I$ . Then  $N(r) < N(d)$ , but  $d$  was chosen to have the smallest norm, so  $r$  is necessarily 0. Then,  $I \ni a = dq \in (d)$ , so we have that  $I \subseteq (d)$ .

Therefore,  $(d) = I$ , so  $I$  is principal. □

### Definition: Greatest Common Divisor (Euclidean Domains)

Let  $R$  be a commutative ring, and  $a, b \in R$  with  $b \neq 0$ . A **greatest common divisor** of  $a$  and  $b$  is an element of  $d \in R$  such that

- (1)  $d \mid a$  and  $d \mid b$ .
- (2) Whenever there is another  $c \in R$  such that  $c \mid a$  and  $c \mid b$ , then  $c \mid d$ .

**Proposition:** Let  $R$  be a Euclidean domain and let  $a, b \in R$  such that  $b \neq 0$ , and let  $d$  be a greatest common divisor of  $a$  and  $b$ . Then  $d' \in R$  is also a greatest common divisor of  $a$  and  $b$  if and only if  $d'$  is an associate of  $d$ .

*Proof.* Let  $R$  be a Euclidean domain and let  $a, b \in R$  such that  $b \neq 0$ , and let  $d$  be a greatest common divisor of  $a$  and  $b$ . Consider  $d' \in R$ .

( $\implies$ ) Suppose  $d'$  is also a greatest common divisor of  $a$  and  $b$ . Then since  $d' \mid a$  and  $d' \mid b$ , by definition, we have  $d' \mid d$ , so  $d = d'p$  for some  $p \in R$ . But we also have that  $d \mid a$  and  $d \mid b$ , and by definition  $d \mid d'$ , so  $d' = dq$  for some  $q \in R$ . Then

$$d = d'p$$

$$d = (dq)p$$

$$1 = qp \quad d \neq 0, R \text{ is an integral domain, so apply the cancellation property}$$

so  $d'$  and  $d$  are associates.

( $\impliedby$ ) Suppose  $d'$  is an associate of  $d$ . Then there exists a unit  $c \in R$  such that  $d = d'c$ , so  $d' \mid d$  by definition. Since  $d$  is a greatest common divisor, we have that  $d \mid a$  and  $d \mid b$ , so  $a = dp$ ,  $b = dq$  for  $p, q \in R$ . This implies that  $d' \mid dp = a$  and  $d' \mid dq = b$ , so  $d' \mid a$  and  $d' \mid b$ , so  $d'$  is also a greatest common divisor of  $a$  and  $b$ .

Therefore,  $d'$  is another greatest common divisor for  $a$  and  $b$  if and only if  $d'$  is an associate of  $d$ .  $\square$

### Theorem

Let  $R$  be a Euclidean domain, and let  $a, b \in R$  such that  $b \neq 0$ . Suppose  $d$  is such that  $(d) = (a, b)$ . Then  $d$  is a greatest common divisor of  $a$  and  $b$ .

*Proof.* Let  $R$  be a Euclidean domain, and let  $a, b \in R$  such that  $b \neq 0$ . Suppose  $d$  is a such that  $(d) = (a, b)$ . Then  $a, b \in (a, b) = (d)$ , so we can express them as  $a = dp, b = dq$  for  $p, q \in R$ . This means  $d \mid a$  and  $d \mid b$ . Now suppose that we have  $c \in R$  such that  $c \mid a$  and  $c \mid b$ . Then  $a = cr, b = cs$  for  $r, s \in R$ , so we can write  $d = ap + bq = (cr)p + (cs)q = c(rp + sq)$ , which implies that  $c \mid d$ . Therefore,  $d$  is a greatest common divisor of  $a$  and  $b$ .  $\square$

## 4.2 Principal Ideal Domains

### Definition: Principal Ideal Domain (PID)

Let  $R$  be an integral domain.  $R$  is a **principal ideal domain (PID)** if every ideal of  $R$  is principal. That is, given an ideal  $I \subseteq R$ , we can find  $a \in R$  such that  $I = (a)$ .

**Note:** Since all ideals in a Euclidean domain are principal, they are also PID's.

### Theorem

Let  $R$  be a PID, and let  $a, b \in R$  with  $b \neq 0$ . Let  $d \in R$  be such that  $(d) = (a, b)$ . Then  $d$  is a greatest common divisor of  $a$  and  $b$ . Moreover,  $d' \in R$  is a greatest common divisor of  $a$  and  $b$  if and only if  $d'$  is an associate of  $d$ .

*Proof.* Let  $R$  be a principal ideal domain and let  $a, b \in R$  such that  $b \neq 0$ , and let  $d$  be a greatest common divisor of  $a$  and  $b$ . Consider  $d' \in R$ .

( $\implies$ ) Suppose  $d'$  is also a greatest common divisor of  $a$  and  $b$ . Then since  $d' \mid a$  and  $d' \mid b$ , by definition, we have  $d' \mid d$ , so  $d = d'p$  for some  $p \in R$ . But we also have that  $d \mid a$  and  $d \mid b$ , and by definition  $d \mid d'$ , so  $d' = dq$  for some  $q \in R$ . Then

$$d = d'p$$

$$d = (dq)p$$

$$1 = qp \quad d \neq 0, R \text{ is an integral domain, so apply the cancellation property}$$

so  $d'$  and  $d$  are associates.

( $\impliedby$ ) Suppose  $d'$  is an associate of  $d$ . Then there exists a unit  $c \in R$  such that  $d = d'c$ , so  $d' \mid d$  by definition. Since  $d$  is a greatest common divisor, we have that  $d \mid a$  and  $d \mid b$ , so  $a = dp$ ,  $b = dq$  for  $p, q \in R$ . This implies that  $d' \mid dp = a$  and  $d' \mid dq = b$ , so  $d' \mid a$  and  $d' \mid b$ , so  $d'$  is also a greatest common divisor of  $a$  and  $b$ .

Therefore,  $d'$  is another greatest common divisor for  $a$  and  $b$  if and only if  $d'$  is an associate of  $d$ .  $\square$

**Proposition:** Let  $R$  be a PID and  $P \subseteq R$  be a nonzero prime ideal. Then  $P$  is maximal.

*Proof.* Let  $R$  be a PID and suppose that  $(p) = P \subseteq R$  is a nonzero prime ideal. Suppose  $(p) = P \subsetneq M = (m)$ . Since  $p \in (p) \subsetneq (m)$ ,  $p = mr$  for some  $r \in R$ . But since  $(p)$  is prime, either  $m \in P$  or  $r \in P$ . If  $m \in P$ , then we are done since  $M = (m) \subseteq (p) = P$ . If  $r \in P$ , then  $r = ps$  for  $s \in R$ . Then  $p = mr = mps$ . Since  $R$  is an integral domain and  $p \neq 0$ , apply the cancellation property to get  $1 = ms$ , which shows that  $(m) = M = R$ . Therefore,  $P$  is maximal.  $\square$

### Corollary

Let  $R$  be a commutative ring and suppose the polynomial ring  $R[x]$  is a PID. Then  $R$  is a field.

*Proof.* Let  $R$  be an integral domain and  $R[x]$  a principal ideal domain. Consider the principal ideal  $(x) \subseteq R[x]$  and a function  $f : R[x] \rightarrow R$  with  $f(p(x)) = p(0)$ . Then

- $f(p(x) + q(x)) = p(0) + q(0) = f(p(x)) + f(q(x))$ , so  $f$  is **closed under addition**.
- $f(p(x) \cdot q(x)) = p(0) \cdot q(0) = f(p(x)) \cdot f(q(x))$ , so  $f$  is **closed under multiplication**.
- $f(1(x)) = 1$ , so  $f$  **preserves the multiplicative identity**.

so  $f$  is a ring homomorphism. We have that  $\ker(f) = \{p(x) : f(p(x)) = 0\} = (x)$ , so  $\ker(f) = (x)$ . To show  $\text{Im}(f) = R$ , take  $a \in R$ . Then consider  $p \in R$  such that  $p(0) = a$ . Then  $f(p(x)) = p(0) = a \in R$ . Therefore,  $\text{Im}(f) = R$ . Then we have that  $R[x]/(x) \simeq R$  by the **First Isomorphism Theorem**.

Note that since  $1 \notin (x)$ ,  $(x) \neq R[x]$ , so  $(x) \subsetneq R[x]$  is a proper ideal. To show that  $(x)$  is maximal, consider  $(y) \subseteq R[x]$  such that  $(y) \supseteq (x)$ . If  $\deg(y) = 0$ , then  $y$  is a unit, so  $(y) = R[x]$ . If  $\deg(y) > 0$ , then since  $x \in (x) \subseteq (y)$ , we can write  $x = fy$  for some  $f \in R[x]$ . Then since  $\deg(x) = 1$ ,  $\deg(y) \leq \deg(x) = 1$ , which means we necessarily have  $\deg(y) = 1$ . Then  $x$  and  $y$  are associates, so  $(x) = (y)$ . Therefore,  $(x)$  is maximal, so  $R[x]/(x)$  is a field. But since  $R[x]/(x) \simeq R$ , we have that  $R$  is a field.  $\square$

**Proposition:** Let  $R$  be a PID and  $p \in R$  be irreducible. Then  $p$  is prime.

*Proof.* Suppose  $p$  is irreducible and consider  $(p) \subseteq I = (a)$ . Because  $p \in (a)$ , we have that  $p = ab$  for some  $b \in R$ . Then  $a$  or  $b$  is a unit. If  $a$  is a unit, then  $(a) = I = R$ . If  $b$  is a unit, then  $a$  and  $b$  are associates, so  $(a) = (p)$ . Then either  $I = R$  or  $I = (p)$ , so  $(p)$  is maximal and therefore prime.  $\square$

### Definition: Ascending Chain Condition

Let  $R$  be an integral domain.  $R$  satisfies the **ascending chain condition** on principal ideals if, whenever we have a chain of inclusions of ideals given by

$$(a_1) \subseteq (a_2) \subseteq \cdots$$

where each  $a_i \in R$ , there exists a positive integer  $n$  such that for all  $m \geq n$ , we have  $(a_m) = (a_n)$ .

### Lemma

Let  $R$  be an integral domain and  $I_1 \subseteq I_2 \subseteq \cdots$  be a chain of ideals in  $R$ . Their union  $\bigcup_j I_j$  is also an ideal.

*Proof.* Let  $R$  be an integral domain and  $I_1 \subseteq I_2 \subseteq \cdots$  a chain of ideals in  $R$ .

- (1) Since  $I_1$  is an ideal,  $0 \in I_1 \subseteq \bigcup_j I_j$ , so  $\bigcup_j I_j$  **preserves the additive identity**.
- (2) Take  $a \in I_n$  and  $b \in I_m$ . Without loss of generality, suppose  $n \leq m$ . Then  $a, b \in I_m$ , so  $a - b \in I_m \subseteq \bigcup_j I_j$ , so  $\bigcup_j I_j$  is **closed under subtraction**.
- (3) Take  $a \in I_n$  and  $r \in R$ . Since  $I_n$  is an ideal,  $ar, ra \in I_n \subseteq \bigcup_j I_j$ , so  $\bigcup_j I_j$  is **closed under absorption**.

Since  $\bigcup_j I_j$  satisfies (1)-(3),  $\bigcup_j I_j$  is an ideal. □

### Theorem

A PID satisfies the ascending chain condition on principal ideals.

*Proof.* Suppose we have an ascending chain of ideals given by

$$(a_1) \subseteq (a_2) \subseteq \cdots$$

Consider their union,  $I = \bigcup_j (a_j)$ . Because  $I \subseteq R$  is principal, we can represent  $I = (a)$  for  $a \in R$ . Then  $a \in (a_n)$  for some positive  $n \in \mathbb{N}$ . This implies that  $a \subseteq (a_m)$  for  $m \geq n$ , so  $(a) \subseteq (a_m)$ . But we also have that  $(a_m) \subseteq I = (a)$ , so  $(a_m) = (a)$  for every  $m \geq n$ . In particular,  $(a_m) = (a_n)$  for all  $m \geq n$ . □

**Note:** This tells us that we do not have ideals that are arbitrarily big but not the entire ring itself. More concretely, the ascending chain condition gives us prime factorizations a PID.

### Theorem

Let  $R$  be an integral domain that satisfies the ascending chain condition on principal ideals. Let  $r \in R$  be nonzero and a nonunit.  $r$  can be expressed as a product of irreducible elements.

*Proof.* Let  $R$  be an integral domain that satisfies the ascending chain condition on principal ideals. Let  $r \in R$  be nonzero and a nonunit. If  $r$  is irreducible, we are done, so suppose not. Suppose for the sake of contradiction that  $r$  cannot be written as a product of irreducibles. Then since  $r$  is not irreducible, we can express  $r = r_1^1 r_2^1$  such that neither  $r_1^1$  nor  $r_2^1$  are units. Then at least one of  $r_1^1$  or  $r_2^1$  cannot be a product of irreducibles, since otherwise,  $r$  would be a product of irreducibles. Without loss of generality, suppose  $r_1^1$  is not a product of irreducibles. Then  $r_1^1$  can be written as  $r_1^2 r_2^2$  where neither  $r_1^2$  nor  $r_2^2$  are units. We continue this process inductively to get  $r_1^1, \dots$  where  $r_1^{i+1}$  is a proper factor of  $r_1^i$  for each  $i$ . This gives us a chain of principal ideals given by  $(r_1^1) \subsetneq (r_1^2) \subsetneq \cdots$ . This is a contradiction to the claim that  $R$  satisfies the ascending chain condition. Therefore,  $r$  can be expressed as a product of irreducibles. □