

# Algebra II Course Notes

Isaac Holt

January 17, 2023

# 1 Rings and fields

## 1.1 Rings, subrings and fields

**Definition 1.1.1.** A **ring**  $(R, +, \cdot)$  is a set  $R$  with two binary operations: addition  $(+)$  and multiplication  $(\cdot)$ , such that  $(R, +)$  is an abelian group and these conditions hold:

1. (**Identity**) for some element  $1 \in R$ ,  $\forall x \in R$ ,  $1 \cdot x = x \cdot 1 = x$ .
2. (**Associativity**)  $\forall (x, y, z) \in R^3$ ,  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ .
3. (**Distributivity**)  $\forall (x, y, z) \in R^3$ ,  $x \cdot (y + z) = x \cdot y + x \cdot z$  and  $(y + z) \cdot x = y \cdot x + z \cdot x$ .

**Remark.** Often we write  $R$  to mean the entire ring instead of just the set of the ring.

**Definition 1.1.2.** A ring  $R$  is **commutative** if  $\forall x, y \in R$ ,  $x \cdot y = y \cdot x$  and is **non-commutative** otherwise.

## 2 Homomorphisms between Rings

Let  $R$  and  $S$  be two rings. A map  $f : R \rightarrow S$  is called a (ring)-homomorphism if:

1.  $f(1) = 1$
2.  $f(a + b) = f(a) + f(b)$
3.  $f(ab) = f(a)f(b)$

**Lemma 2.0.1.**  $f(0) = 0$  and  $f(-a) = -f(a)$

*Proof.*  $f(0) = f(0 + 0) = f(0) + f(0)$

$$0 = f(0) = f(a + (-a)) = f(a) + f(-a)$$

$$\text{Hence } -f(a) = f(-a)$$

□

**Definition 2.0.2.** Two rings  $R$  and  $S$  are **isomorphic** if there exists a bijective homomorphism between  $R$  and  $S$ . The map between them is an **isomorphism**. We write  $R \cong S$ .

**Lemma 2.0.3.** A homomorphism  $f : R \rightarrow S$  is injective iff  $\ker f = 0$ .

*Proof.* If  $f$  is injective,  $f(x) = f(y) \Rightarrow x = y$ . Assume  $f$  is injective.  $\ker f = a \in R : f(a) = 0$  so  $f(a) = 0 \Rightarrow f(a) = f(0) \Rightarrow a = 0$ .

For the other direction: assume  $\ker f = 0$ .  $f(x) = f(y) \Rightarrow f(x) - f(y) = 0 \Rightarrow f(x) + f(-y) = 0 \Rightarrow f(x - y) = 0 \Rightarrow x - y \in \ker f$ . Since  $\ker f = 0$ ,  $x - y = 0$  and so  $x = y$ . □

**Definition 2.0.4.** Let  $R$  and  $S$  be two rings.

- The **product** of  $R$  and  $S$  is defined as  $R \times S := \{(r, s) : r \in R, s \in S\}$  which is itself a ring.
- **Addition** is defined as  $(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2)$ .
- **Multiplication** is defined as  $(r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2, s_1 s_2)$
- The multiplicative identity is  $(1, 1)$ .

**Definition 2.0.5.** We have two ring homomorphisms:

1.  $p_1 : R \times S \rightarrow R = (r, s) \rightarrow r$
2.  $p_2 : R \times S \rightarrow S = (r, s) \rightarrow s$

$$\ker p_1 = \{(r, s) \in R \times S : p_1((r, s)) = 0\} = \{(r, s) \in R \times S : r = 0\} = \{(0, s) : s \in S\}$$

**Remark.** Note  $\ker p_1$  is not a subring of  $R \times S$  since  $(1, 1) \notin \ker p_1$ .

But we can consider  $\ker p_1$  as a ring by taking  $(0, 1)$  as the multiplicative identity. Then  $\ker p_1 \cong S$  as we map  $(0, s) \rightarrow s$ .

Similarly,  $\ker p_2 \cong R$  and so  $\ker p_1 \times \ker p_2 \cong S \times R \cong R \times S$ .

**Lemma 2.0.6.** Let  $f : R \rightarrow S$  be a ring homomorphism. Then  $\ker f$  has the following two properties:

1.  $\ker f$  is closed under addition.

2. For every  $r \in R$  and  $x \in \ker f$  we have  $r \cdot x \in \ker f$  and  $x \cdot r \in \ker f$ .

*Proof.*

1. If  $x, y \in \ker f$  then  $f(x + y) = f(x) + f(y) = 0 + 0 = 0$ . That is  $x + y \in \ker f$ .
2. For every  $r \in R$  and  $x \in \ker f$ ,  $f(r \cdot x) = f(r) \cdot f(x) = f(r) \cdot 0 = 0$ . Thus  $r \cdot x \in \ker f$ . Similarly for  $x \cdot r$ .

□

**Definition 2.0.7.** Let  $I$  be an ideal in a ring  $R$ . Then for an element  $x \in R$ , the **coset** of  $I$  generated by  $x$  to be the set  $\bar{x} := x + I := \{x + r : r \in I\} \subset R$ .

$x$  is said to be a representative of this coset.

**Lemma 2.0.8.** Let  $x \in R$  and  $y \in R$ . Then the following statements are equivalent

1.  $x + I = y + I$
2.  $x + I \cap y + I \neq \emptyset$
3.  $x - y \in I$

*Proof.* ((1)  $\Rightarrow$  (2)) is obvious

((2)  $\Rightarrow$  (3)): if  $x + I \cap y + I \neq \emptyset$ , for some  $r_1 \in I, r_2 \in I$ ,  $x + r_1 = y + r_2$  and so  $x - y = r_2 - r_1 \in I$ .

((3)  $\Rightarrow$  (1)): since  $x - y \in I$ , for some  $r' \in I$ ,  $x = y + r'$ . Then  $x + I = \{x + r : r \in I\} = \{y + r' + r : r \in I\} \subseteq y + I$  as ideals are closed under addition, and  $r' + r \in I$ .  $y + I = \{y + r : r \in I\} = \{x - r' + r : r \in I\} \subseteq x + I$  and so  $x + I = y + I$ . □

Notation:  $\bar{x} = \bar{y} \Leftrightarrow x + I = y + I \Leftrightarrow x \equiv y \pmod{I} \Leftrightarrow x - y \in I$

**Definition 2.0.9.**  $R/I := \{\bar{x} : x \in R\} = \{x + I : x \in R\}$  is the set of all distinct cosets of  $R \pmod{I}$

**Remark.** If  $R = \mathbb{Z}$  and  $I = (n)$ ,  $n \in \mathbb{N}$ ,  $R/I = \mathbb{Z}/n = \{\bar{0}, \dots, \bar{n-1}\}$ .

**Definition 2.0.10.**

- Addition:  $(x + I) + (y + I) = x + y + I$
- Multiplication:  $(x + I) \cdot (y + I) = xy + I$

A coset  $x + I$  has many representatives, for example  $x + r$  with  $r \in I$  gives the same coset, since  $x + r - x = r \in I$ .

Assume  $x, x' \in R$  such that  $x + I = x' + I$  and  $y, y' \in R$  such that  $y + I = y' + I$ .

*Proof.* • Addition:  $x + I = x' + I \Leftrightarrow x - x' \in I$  and similarly  $y - y' \in I$ .  $I$  is closed under addition so  $(x - x') + (y - y') \in I \Leftrightarrow (x + y) - (x' + y') \in I \Leftrightarrow x + y + I = x' + y' + I$ .

- $x - x' \in I$  and  $y - y' \in I$ , so  $(x - x')y \in I$  and  $x(y - y') \in I$ .  $(x - x')y + x(y - y') = xy - x'y' \in I \Leftrightarrow xy + I = x'y' + I$ .

□

$R/I$  with the two binary operations of addition and multiplication is a ring:

- The zero element is  $0 + I$  as  $(x + I) + (0 + I) = x + I$ .
- The multiplicative identity is  $1 + I$ .
- All properties follow from the corresponding properties of  $R$ :
- e.g. distributivity:  $\bar{x} = x + I$ ,  $\bar{y} = y + I$ ,  $\bar{z} = z + I$ .  $\bar{x}(\bar{y} + \bar{z}) = \bar{x}(\overline{y + z}) = \overline{x(y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \bar{x}\bar{y} + \bar{x}\bar{z}$ .

**Definition 2.0.11.** Let  $R$  be a ring, and  $I \subseteq R$  be an ideal of  $R$ . Then the ring  $R/I$  is called the **quotient** of  $R$  by  $I$  ( $R \bmod I$ ). Its elements,  $x + I$ ,  $x \in R$  are called cosets (or residue classes or equivalence classes) and we denote them  $\bar{x}$ .

$R/I$  may be commutative or non-commutative, but if  $R$  is commutative, so is  $R/I$ .

If  $I = R$ , then  $R/R$  consists of a single element, since for every  $x \in R$ ,  $y \in R$ , we have  $x - y \in R$  and hence  $x + R = y + R$ .

If  $I = 0 = \{0\}$  is the zero ideal, if  $x \in R$ ,  $x + I = x + 0 = x$ . Hence  $R/I = R$ .

**Definition 2.0.12.** Given  $R$ ,  $I \subseteq R$  an ideal, the **quotient map** (or **canonical homomorphism**) is defined as  $\Pi : R \rightarrow R/I = x \rightarrow \bar{x} = x + I$  and is a ring homomorphism.

$$\ker \Pi = \{r \in R : \bar{r} = \bar{0}\} = \{r \in R : r - 0 = r \in I\} = I.$$

Hence, given a ring  $R$  and an ideal  $I \subseteq R$ , there exists a ring homomorphism ( $\Pi$ ) such that  $\ker \Pi = I$ .

**Theorem 2.0.13.** (First Isomorphism Theorem - FIT) Let  $\phi : R \rightarrow S$  be a ring homomorphism. The map  $\bar{\phi} : R/\ker \phi \rightarrow \text{Im } \phi = \bar{x} \rightarrow \phi(x)$  is well-defined and it is a ring isomorphism:  $R/\ker \phi \cong \text{Im } \phi$ .

*Proof.* Let  $x, x' \in R$  such that  $\bar{x} = \bar{x'}$ , i.e.  $x + \ker \phi = x' + \ker \phi$ . So  $x - x' \in \ker \phi$ , hence  $\phi(x - x') = 0 \Leftrightarrow \phi(x) - \phi(x') = 0 \Leftrightarrow \phi(x) = \phi(x')$ . Hence  $\bar{\phi}$  is well-defined.

$$1. \bar{\phi}(\bar{1}) = \phi(1) = 1$$

$$2. \bar{\phi}(\bar{x} + \bar{y}) = \bar{\phi}(\overline{x + y}) = \phi(x + y) = \phi(x) + \phi(y) = \bar{\phi}(\bar{x}) + \bar{\phi}(\bar{y}).$$

$$3. \text{ Similarly, } \bar{\phi}(\bar{x} \cdot \bar{y}) = \bar{\phi}(\overline{x \cdot y}) = \phi(x \cdot y) = \phi(x) \cdot \phi(y) = \bar{\phi}(\bar{x}) \cdot \bar{\phi}(\bar{y}).$$

Hence  $\bar{\phi}$  is a ring homomorphism.

$\bar{\phi}(\bar{x}) = 0 \Leftrightarrow \phi(x) = 0 \Leftrightarrow x \in \ker \phi \Leftrightarrow \bar{x} = \bar{0}$ , hence  $\ker \bar{\phi} = \{\bar{0}\}$ . Let  $y \in \text{Im } \bar{\phi} \Leftrightarrow$  for some  $x \in R$ ,  $\bar{\phi}(\bar{x}) = y$ . Hence  $\bar{\phi}(\bar{x}) = \phi(x) = y$ , hence  $\bar{\phi}$  is also surjective, hence it is bijective.  $\square$

**Definition 2.0.14.** Let  $R$  be a commutative ring. An ideal  $I \subseteq R$  is a **prime ideal** if  $I \neq R$  ( $I$  is proper) and for every  $a, b \in R$  such that  $a \cdot b \in I$  then  $a \in I$  or  $b \in I$ .

The ideal  $I \neq R$  is **maximal** if the only ideals that contain  $I$  is  $I$  itself and  $R$ . i.e. there is no ideal  $J$  such that  $I \subsetneq J \subsetneq R$ .

**Theorem 2.0.15.** Recall  $x \in R$  is prime if  $0 \neq x \notin R^\times$  and  $x|ab \Rightarrow x|a$  or  $x|b$ .

If  $x$  is a prime element then  $(x)$  is a prime ideal.

*Proof.*  $ab \in (x) \Rightarrow$  for some  $r \in R$ ,  $ab = rx \Rightarrow x|ab$  so because  $x$  is prime,  $x|a$  or  $x|b$  so  $a \in (x)$  or  $b \in (x)$ .  $\square$

**Lemma 2.0.16.** Let  $(x)$  be a non-zero prime ideal. The  $x$  is a prime element.

*Proof.* If  $x|ab$ ,  $ab \in (x)$ , so because  $(x)$  is a prime ideal,  $a \in (x)$  or  $b \in (x)$ , so  $x|a$  or  $x|b$ .  $\square$

**Remark.**  $x|a \Leftrightarrow a \in (x) \Leftrightarrow (a) \subseteq (x)$ .

This can be described as “to divide is to contain”.

**Corollary 2.0.17.** The zero ideal  $(0) = 0$  is a prime ideal iff  $R$  is an integral domain, since an integral means  $ab = 0 \Rightarrow a = 0$  or  $b = 0$ .

**Theorem 2.0.18.** Let  $R$  be a commutative ring and  $I \subseteq R$  an ideal.

1.  $I$  is prime iff  $R/I$  is an integral domain.
2.  $I$  is maximal iff  $R/I$  is a field.

*Proof.*

1. Assume  $I$  is prime. Assume  $\bar{a}\bar{b} = \bar{0}$  with  $a, b \in R$ ,  $\bar{a}, \bar{b} \in R/I$ .  $\bar{a}\bar{b} = \bar{0} \Rightarrow \overline{ab} = \bar{0} \Rightarrow ab \in I \Rightarrow a \in I$  or  $b \in I \Rightarrow \bar{a} = \bar{0}$  or  $\bar{b} = \bar{0}$ , hence  $R/I$  is an integral domain.

Now assume  $R/I$  is an integral domain.  $ab \in I \Rightarrow \overline{ab} = \bar{0}$ . Since  $R/I$  is an integral domain,  $\bar{a} = \bar{0}$  or  $\bar{b} = \bar{0} \Rightarrow a \in I$  or  $b \in I$ .

2.  $(\Rightarrow)$ : Assume that  $I$  is maximal. Let  $\bar{x} \neq \bar{0}$ ,  $\bar{x} \in R/I$ , then  $x \in R$  with  $x \notin I$ . Consider  $(I, x) := \{r + r'x : r \in I, r' \in R\}$ . This is an ideal, as  $r_1 + r'_1x + r_2 + r'_2x = (r_1 + r_2) + (r'_1 + r'_2)x \in R$ , and  $r''(r + r'x) = r''r + r''r'x \in R$ .  $I \subsetneq (I, x) \subseteq R$ .  $I$  is maximal so  $(I, x) = R \Rightarrow 1 \in (I, x)$ . Hence for some  $y \in R$ ,  $yx + m = 1$  for some  $m \in I$ .

Hence  $yx - 1 \in I \Rightarrow \bar{y}\bar{x} = \bar{y}\bar{x} = \bar{1}$  hence  $\bar{x}$  is invertible, so  $R/I$  is a field.

$(\Leftarrow)$ : Assume  $R/I$  is a field. If  $\bar{0} \neq \bar{x} \in R/I$ , then for some  $y \in R/I$ ,  $\bar{x}\bar{y} = \bar{1} \Rightarrow xy - 1 \in I \Rightarrow xy = 1 + m$  for some  $m \in I$ . That is,  $1 = xy - m$  hence  $1 \in (I, x) \Rightarrow (I, x) = R$ .

Now let  $J$  be an ideal such that  $I \subsetneq J \subseteq R$ . Since  $I \subsetneq J$ , for some  $x \in J$ ,  $x \notin I$ . Then  $I \subsetneq (I, x) \subseteq J \subseteq R$ . But  $(I, x) = R$ , hence  $J = R$ . Hence there is no ideal  $J$  such that  $I \subsetneq J \subsetneq R$ , hence  $I$  is maximal.  $\square$

**Corollary 2.0.19.** If  $I$  is maximal then  $I$  is prime.

*Proof.*  $I$  is maximal  $\Rightarrow R/I$  is a field  $\Rightarrow R/I$  is an integral domain  $\Rightarrow I$  is a prime ideal.  $\square$

## 2.1 Principal Ideal Domains (PIDs)

**Example 2.1.1.** Let  $a, b \in \mathbb{Z}$ . Then let  $d = (a, b) = \gcd(a, b)$ .  $(a, b) \subseteq (d)$  since  $d|a$  and  $d|b \Leftrightarrow a = dr_1$  and  $b = dr_2$ ,  $r_1, r_2 \in \mathbb{Z} \Rightarrow a \in (d)$  and  $b \in (d)$ .

Moreover, for some  $r_1, r_2 \in \mathbb{Z}$ ,  $d = r_1 + r_2b \Rightarrow d \in (a, b) \Rightarrow (d) \subseteq (a, b)$ .

The same argument holds for  $F[x]$  with  $F$  a field.

i.e.  $(f(x), g(x)) = (\gcd(f(x), g(x)))$ .

**Definition 2.1.2.** An integral domain in which **all** ideals are principle is called a **principle ideal domain (PID)**.

**Theorem 2.1.3.** Let  $R$  be a either  $\mathbb{Z}$  or  $F[x]$  with  $F$  a field. Then  $R$  is a PID.

*Proof.* Define the following “degree” function  $d : R \setminus \{0\} \rightarrow \mathbb{N}$  by

$$d(a) := \begin{cases} |a| & \text{if } a \in \mathbb{Z} \\ \deg(a) & \text{if } a \in F[x] \end{cases}$$

By division, for every  $a, m \in R \setminus \{0\}$ , we can find unique  $q, r \in R$  such that  $a = qm + r$  with  $r = 0$  or  $d(r) < d(m)$ .

Let  $I \subseteq R$  be an ideal. If  $I = 0 = \{0\}$  we are done. So now let  $I \neq 0$ . Let  $0 \neq m \in I$  such that  $d(m)$  is minimal among elements of  $I$ . We claim that  $I = (m)$ .

Let  $a \in I$ .  $a \in (m) \Leftrightarrow m|a$ . Dividing  $a$  by  $m$ , we get  $a = qm + r$ , with  $r = 0$  or  $d(r) < d(m)$ . But since  $r = a - qm \in I$ ,  $d(r) < d(m)$  would contradict the minimality of  $d(m)$ . Hence  $r = 0$ , so  $m|a \Leftrightarrow a \in (m)$ .  $(m) \subseteq I$  so  $a \in I \Leftrightarrow a \in (m)$ .  $\square$

**Theorem 2.1.4.** (Stated without proof) Any PID is a UFD.

**Remark.** There are integral domains which are not PIDs, e.g.  $\mathbb{Z}[\sqrt{-5}]$  which is not a UFD and hence not a PID.

**Proposition 2.1.5.** Let  $R$  be a PID and  $a, b \in R$ . Then  $\gcd(a, b)$  exists and  $(a, b) = (\gcd(a, b))$ .

*Proof.* Since  $R$  is a PID, for some  $d \in R$ ,  $(a, b) = (d)$ . We claim that  $d = \gcd(a, b)$ .

$(a, b) = (d) \Rightarrow a \in (d)$  and  $b \in (d) \Rightarrow d|a$  and  $d|b$ . Suppose  $e \in R$  such that  $e|a \Rightarrow a \in (e)$  and  $e|b \Rightarrow b \in (e)$ .  $(d) = (a, b) \subseteq (e) \Rightarrow e|d$ . Therefore  $d = \gcd(a, b)$ .  $\square$

**Theorem 2.1.6.** (Stated without proof):  $\mathbb{Z}[i], \mathbb{Z}[\pm\sqrt{2}]$  are PID's.

**Lemma 2.1.7.** Let  $R$  be a PID and let  $a \in R$  be irreducible. Then the principle ideal generated by  $a$  is a maximal ideal.

*Proof.* Suppose  $(a) \subseteq I$ , with  $I$  an ideal. We must show  $I = (a)$  or  $I = R$ . Since  $R$  is a PID, for some  $t \in R$ ,  $I = (t)$ . So  $(a) \subseteq (t)$  so for some  $m \in R$ ,  $a = tm$ . But  $a$  is irreducible, so either  $t$  is a unit or  $m$  is a unit.

If  $t \in R^\times$  then  $I = (t) = R$ . If  $m \in R^\times$  then  $(a) = (t) = I$  (last question of assignment 3).  $\square$

## 2.2 Fields on quotients

**Theorem 2.2.1.** Let  $F$  be a field and  $f(x) \in F[x]$ , with  $f(x)$  irreducible. Then  $F[x]/(f(x))$  is a field and a vector space over  $F$  with basis

$$B := \{\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}\}$$

where  $n = \deg f$ .

That is, every element of  $F[x]/(f(x))$  can be uniquely written as

$$\overline{a_0 1 + a_1 x + \dots + a_{n-1} x^{n-1}}$$

*Proof.* Since  $f(x)$  is irreducible,  $F[x]/(f(x))$  is a field.  $F[x]/(f(x))$  is a vector space over  $F$  and an abelian group with respect to addition and scalar multiplication with elements of  $F$ : if  $\overline{g(x)} \in F[x]/(f(x))$  and  $\alpha \in F$  then  $\alpha \overline{g(x)} = \overline{\alpha g(x)} \in F[x]/(f(x))$ .

We must prove  $B$  spans  $F[x]/(f(x))$ . For every  $\overline{g(x)} \in F[x]/(f(x))$ ,  $g(x) = q(x)f(x) + r(x)$  with  $\deg(r) < \deg(f) = n \Rightarrow g(x) - r(x) = q(x)f(x) \in (f(x)) \Rightarrow \overline{g(x)} = \overline{r(x)}$ ,  $\deg(r) < n$ . Hence  $\overline{g(x)} = \overline{r(x)} = a_0 + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1}$  with  $a_i \in F$ . Hence  $B$  spans  $F[x]/(f(x))$ .

We must show  $B$  is linearly independent over  $F$ , i.e. show if  $\sum_{i=0}^{n-1} a_i \bar{x}^i = \bar{0}$  then  $\forall i, a_i = 0$ .

$\sum_{i=0}^{n-1} a_i \bar{x}^i = \bar{0} \Leftrightarrow \sum_{i=0}^{n-1} a_i x^i \in (f(x)) \Rightarrow f(x) \mid \sum_{i=0}^{n-1} a_i x^i$ . But  $\deg(f) = n$  and  $\deg(\sum_{i=0}^{n-1} a_i x^i) < n$  so  $\sum_{i=0}^{n-1} a_i x^i$  is the zero polynomial so  $\forall i, a_i = 0$ . Therefore  $B$  is linearly independent.

So  $B$  is a basis. □



### 3 Finite fields

**Theorem 3.0.1.** For every prime  $p$  and  $n \in \mathbb{N}$ , for some irreducible polynomial  $f(x) \in (\mathbb{Z}/p)[x]$ ,  $\deg(f) = n$ . Thus  $(\mathbb{Z}/p)[x]/(f(x))$  is a field with  $p^n$  elements (since there are  $p$  choices for each  $a_i$  in  $a_0 + a_1\bar{x} + \dots + a_{n-1}\bar{x}^{n-1}$ ).

Any two such fields are isomorphic and we denote the unique, up to isomorphism, field with  $p^n$  elements with  $\mathbb{F}_{p^n}$ .

*Proof.* Not examinable. □

**Remark.** If  $n = 1$  then  $\mathbb{F}_p \cong \mathbb{Z}/p$  with  $p$  prime. However if  $n > 1$  then  $\mathbb{F}_{p^n} \not\cong \mathbb{Z}/p^n$  since  $\mathbb{Z}/p^n$  is not a field.

**Example 3.0.2.** Find an irreducible polynomial  $f$  in  $(\mathbb{Z}/3)[x]$  of degree 3.

$f(x) = x^3 + x^2 + x + \bar{2}$ . This has no roots in  $\mathbb{Z}/3$  so  $f(x)$  is irreducible since  $\deg(f) = 3$ . Then  $\mathbb{F}_{27} = \mathbb{F}_{3^3} \cong (\mathbb{Z}/3)[x]/(f(x))$ . All elements can be written as  $a_0 + a_1\bar{x} + a_2\bar{x}^2$ ,  $a_i \in \mathbb{Z}/3$ .

$$\overline{f(x)} = \bar{0} = \overline{x^3 + x^2 + x + \bar{2}} \Rightarrow \bar{x}^3 = -\bar{x}^2 - \bar{x} - \bar{2}.$$

#### 3.1 The Chinese Remainder Theorem (CRT)

**Definition 3.1.1.** Let  $a, b \in R$ .  $a$  and  $b$  are **coprime** if  $\nexists r$  irreducible in  $R$  such that  $r|a$  and  $r|b$ .

**Lemma 3.1.2.** Let  $R$  be a PID and  $a, b \in R$  be coprime. Then  $(a, b) = R$  and hence  $\exists x, y \in R$  such that  $xa + yb = 1$ .

*Proof.* Since  $R$  is a PID,  $(a, b) = (r)$  for some  $r \in R$ . So  $a, b \in (r) \Rightarrow r|a$  and  $r|b$ . So  $a = rn$  and  $b = rm$  for some  $n, m \in R$ .  $r$  must be a unit in  $R$  since otherwise,  $r = p_1 \cdots p_k$  for some  $p_i$  irreducible, but then  $a = p_1 \cdots p_k n$ ,  $b = p_k \cdot p_k m$ , which would contradict  $a$  and  $b$  being coprime.

So  $r \in R^\times \Rightarrow (r) = R \Rightarrow (a, b) = R$ . □

**Corollary 3.1.3.** For  $a, b \in R$  coprime, any  $\gcd(a, b) \in R^\times$ .

*Proof.* In a PID,  $(a, b) = (\gcd(a, b))$ . By the lemma above, if  $a$  and  $b$  are coprime,  $(a, b) = R \Rightarrow (\gcd(a, b)) = R = (1) \Rightarrow \gcd(a, b) \in R^\times$ . □

**Theorem 3.1.4.** (CRT for PID's) Let  $R$  be a PID and let  $a_1, \dots, a_k \in R$  be pairwise coprime elements. Then the map from  $R/(a_1, \dots, a_k) \rightarrow R/(a_1) \times \dots \times R/(a_k)$  given by  $r + (a_1, \dots, a_k) \rightarrow (r + (a_1), \dots, r + (a_k))$  is a ring isomorphism.

*Proof.* Let  $\psi : R \rightarrow R/(a_1) \times \dots \times R/(a_k)$ ,  $\psi(r) = (r + (a_1), \dots, r + (a_k))$ . Clearly,  $\psi$  is a ring homomorphism.

For every  $i = 1, 2, \dots, k$ , the elements  $a_i$  and  $a_1 \dots a_{i-1}a_{i+1} \dots a_k$  are coprime. (If not, there exists an irreducible  $p$  such that  $p|a_i$  and  $p|a_1 \dots a_{i-1}a_{i+1} \dots a_k$ . But then  $p$  irreducible  $\Leftrightarrow p$  prime hence  $p|a_j$  for some  $j \neq i$ , but this contradicts that  $a_i$  and  $a_j$  are coprime).

By the above lemma, for some  $x_i, y_i \in R$ ,  $x_i a_i + y_i (a_1 \dots a_{i-1} a_{i+1} \dots a_k) = 1$ . Set  $e_i := 1 - a_i x_i$  for each  $i = 1, \dots, k$ . Then  $e_i = 1 + (a_i)$  and  $e_i = 0 + (a_j)$  for  $j \neq i$ , since  $e_i = 1 - a_i x_i = y_i (a_1 \dots a_{i-1} a_{i+1} \dots a_k)$ .

Let  $(r_1 + (a_1), \dots, r_k + (a_k))$  be any element in  $R/(a_1) \times \dots \times R/(a_k)$ . We claim that

$$\psi \left( \sum_{i=1}^k r_i e_i \right) = (r_1 + (a_1), \dots, r_k + (a_k))$$

$$\psi \left( \sum_{i=1}^k r_i e_i \right) = \sum_{i=1}^k \psi(r_i e_i) = \sum_{i=1}^k \psi(r_i) \psi(e_i)$$

$$\psi(e_i) = (0 + (a_1), \dots, 1 + (a_i), 0 + (a_{i+1}), \dots, 0 + (a_k))$$

since  $e_i = 1 + (a_i)$  and  $e_i = 0 + (a_j)$  for  $j \neq i$  and

$$\psi(r_i) = (r_i + (a_1), \dots, r_i + (a_k))$$

so

$$\psi(e_i) \psi(r_i) = \text{TODO finish and check this proof}$$

Thus  $\psi$  is surjective.  $\ker \psi = \{r \in R : r \in (a_i), i = 1, \dots, k\} = \{r \in R : a_i | r, i = 1, \dots, k\} = \{r \in R : a_1 \dots a_k | r\}$  since  $a_i$  and  $a_j$  are coprime.  $\ker \psi = (a_1 a_2 \dots a_k)$ . Then by the FIT,  $R / \ker \psi \cong R / (a_1) \times \dots \times R / (a_k)$ .  $\square$

## 4 Group Theory

**Definition 4.0.1.** A **group** is a pair  $(G, \circ)$  where  $G$  is a set and  $\circ$  is a map

$$\circ : G \times G \rightarrow G, \quad \circ(g, h) = g \circ h$$

Satisfying these properties:

1. **Closure:**  $g, h \in G \Rightarrow g \circ h \in G$ .
2. **Associativity:**  $x, y, z \in G \Rightarrow (x \circ y) \circ z = x \circ (y \circ z)$ .
3. **Identity element:**  $\exists e \in G, \forall g \in G, e \circ g = g \circ e = g$ .
4. **Existence of inverse:**  $\forall g \in G, \exists h \in G, g \circ h = h \circ g = e$ .  $h$  is called the **inverse** of  $g$  and is written as  $g^{-1}$ .

**Definition 4.0.2.** A group  $(G, \circ)$  is an **Abelian group** if  $\forall g, h \in G, g \circ h = h \circ g$ . Otherwise, it is called **non-Abelian**.

**Remark.** Often,  $G$  is written to refer to a group, not just the set of a group.

**Lemma 4.0.3.** Let  $(R, +, \cdot)$  be a ring. Then  $(G, \circ) = (R, +)$  is a group.

*Proof.* Properties 1 and 2 of a group are automatically satisfied. The identity element is  $0 \in R$ . The inverse element for any element will be the same inverse element in the ring.  $\square$

**Lemma 4.0.4.** Let  $(F, +, \cdot)$  be a field. Then  $(G, \circ) = (R, \cdot)$  is a group.

*Proof.* Again, group properties 1 and 2 are automatic. The identity element is  $1 \in F$ . The inverse element for any element will be the same inverse element in the field.  $\square$

**Example 4.0.5. (Symmetries of a square):** The following are all symmetries of a square:

- Rotation by  $\frac{\pi}{2}$ .
- Reflection about the  $y$ -axis,  $x$ -axis,  $y = x$  axis,  $y = -x$  axis.
- Any of the above symmetries can be combined to form a new symmetry.

Define the group  $G(\circ)$  where  $G$  is the symmetries of the square and  $\circ$  is composition of the symmetries. The identity  $e$  is the map which does nothing to the square. The inverse of a rotation is rotation in the opposite direction, and the inverse of a reflection is the same reflection.

**Definition 4.0.6.** The group in the above example is the **dihedral group**.

**Definition 4.0.7.** The **general linear group** is defined as the set  $GL_2(\mathbb{R}) := \{A \in M_2(\mathbb{R}) : \det A \neq 0\}$  together with  $\circ$  being matrix multiplication.

**Lemma 4.0.8.** The general linear group is a group.

*Proof.*

1.  $\det(AB) = \det A \det B \neq 0$  so  $A, B \in GL_2(\mathbb{R}) \Rightarrow AB \in GL_2(\mathbb{R})$ .
2. Matrix multiplication is associative.
3. The identity is  $I_2$ .
4. The inverse of  $A \in GL_2(\mathbb{R})$  is  $A^{-1}$ , which exists since  $\det A \neq 0$ .

$\square$

**Remark.**  $GL_2(\mathbb{R})$  is non-abelian.

## 4.1 Subgroups

**Definition 4.1.1.** A subset  $H \subseteq G$  is a **subgroup** of  $(G, \circ)$  if  $(H, \circ)$  is also a group. We write  $H \leq G$ .

**Remark.**  $H = G$  is a subgroup of a group  $G$ .

**Definition 4.1.2.** Every group  $(G, \circ)$  has a **trivial subgroup**,  $H = \{e\}$ , where  $e \in G$  is the identity element.

**Definition 4.1.3.** A subgroup  $H$  of  $G$  is **proper** if  $H \neq \{e\}$  and  $H \neq G$ . We write  $H < G$ .

**Proposition 4.1.4. (Subgroup criteria)** Let  $(G, \circ)$  be a group. Then  $H \subseteq G$  is a subgroup iff all these conditions hold:

1.  $H \neq \emptyset$
2.  $h_1, h_2 \in H \Rightarrow h_1 \circ h_2 \in H$ .
3.  $h \in H \Rightarrow h^{-1} \in H$ .

*Proof.* We only need to show that  $H$  contains an identity:  $h \in H \Rightarrow h^{-1} \in H \Rightarrow e = h \circ h^{-1} \in H$ .  $\square$

**Example 4.1.5.** If  $(S, +, \cdot)$  is a subring, then  $(S, +)$  is a subgroup.

**Proposition 4.1.6.** Let  $I \subseteq R$  be a non-empty ideal of a ring  $(R, +, \cdot)$ . Then  $(I, +)$  is a subgroup of  $(R, +)$ .

*Proof.* Criteria 1 and 2 are satisfied by definition. Now we must show that  $x \in I \Rightarrow -x \in I$ : if  $x \in I$ , then  $(-1_R)x = -x \in I$  where  $-1_R + 1_R = 0_R$ .  $\square$

**Definition 4.1.7.** The **special linear group** is defined as  $SL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det A = 1\}$ , which satisfies  $(SL_2(\mathbb{R}), \cdot) \leq (Gl_2(\mathbb{R}), \cdot)$ .

**Example 4.1.8.** Let  $q \in \mathbb{N}$ , then  $q\mathbb{Z} = \{mq : m \in \mathbb{Z}\}$  is an ideal in  $\mathbb{Z}$ . For example, the even numbers,  $2\mathbb{Z}$ , is a subgroup.

However, the odd numbers are not subgroup, as they do not contain 0, nor is  $\bar{a} = \{a + mq : m \in \mathbb{Z}\}$  for  $1 \leq a \leq q - 1$ .

## 4.2 Cosets

**Definition 4.2.1.** Let  $(G, \circ)$  be a group and  $H \leq G$ . A **left coset** of  $H$  is a set of the form

$$g \circ H := \{g \circ h : h \in H\} \quad \text{for } g \in G$$

A **right coset** of  $H$  is a set of the form

$$H \circ g := \{h \circ g : h \in H\} \quad \text{for } g \in G$$

**Remark.**  $x \in g \circ H \iff g^{-1} \circ x \in H$ .

**Remark.** If  $G$  is Abelian, then  $g \circ H = H \circ g$ , but this isn't true in general for non-Abelian groups.

**Proposition 4.2.2.** Let  $(G, \circ)$  be a group and  $H \leq G$ . Then:

1. For every  $g \in G$ ,  $g \circ H$  and  $H$  are in bijection. (So  $|H| < \infty \Rightarrow |g \circ H| = |H|$ ).
2. If  $g \in G$ , then  $g \in H \iff g \circ H = H$ .
3. If  $g_1, g_2 \in G$ , then either  $g_1 \circ H = g_2 \circ H$  or  $(g_1 \circ H) \cap (g_2 \circ H) = \emptyset$ .

**Theorem 4.2.3.** If  $G$  is a **finite** group and  $H \leq G$ , then  $|H|$  divides  $|G|$ . So if  $|H| \nmid |G|$  then  $H \not\leq G$ .