

# Algebra II: Rings and Fields

MATH 340

Steven Xia

November 26, 2022

## Contents

1	Fundamental Definitions . . . . .	1
2	Basic Proofs . . . . .	3
3	Unique Factorization . . . . .	4
4	Ring Homomorphisms . . . . .	8
5	Fields and Stuff . . . . .	12

## 1 Fundamental Definitions

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

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

*Remark 1.1.2.* Similarly, we can prove that the inverse is unique for every element of the set.

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2 Basic Proofs

**Definition 2.1.** The **characteristic** of a ring is the least positive integer  $c$  such that  $\underbrace{1 + 1 + \cdots + 1}_{c \text{ times}} = 0$ . If this number does not exist, define the characteristic to be 0.

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

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

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

*Proof.* We have  $R^* = \{r_1, \dots, r_n\} = \{ar_1, \dots, ar_n\}$  since  $a$  is not a zero-divisor (it is a unit) so  $ar_i \neq ar_j$ . Then,  $r_1 \cdots r_n = (ar_1) \cdots (ar_n) = a^n(r_1 \cdots r_n) \implies a^n = 1$ .  $\square$

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

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

*Remark 2.1.1.* It follows from Theorem 2.1.3 that every finite integral domain is a field.

## 3 Unique Factorization

**Definition 3.1.** A **quadratic ring** extension  $R[\gamma]$  of some ring  $R$  is created by adding an element  $\gamma$  to  $R$  such that  $\gamma^2 = c$  for some  $c \in R$  and  $\gamma \notin R$ .

*Remark 3.1.1.* Elements in  $R[\gamma]$  are denoted  $a + \gamma b$  for  $a, b \in R$ . This means elements in  $R[\gamma]$  can be seen as elements in  $R \times R$ .

**Theorem 3.1.1.** *The norm map<sup>1</sup>  $N : R[\gamma] \rightarrow R$  is defined as  $N(a + \gamma b) = a^2 - cb^2$  and has the property that  $N(a + \gamma b)$  is a unit in  $R$  if and only if  $a + \gamma b$  is a unit in  $R[\gamma]$ .*

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

*Remark 3.1.2.* Theorem 3.1.1 shows the quadratic ring extension of any field or integral domain maintains that status.

**Definition 3.2.** An element in an integral domain is called **irreducible** if it cannot be written as a product of two non-units.

---

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

**Definition 3.3.** Elements  $a, b$  in an integral domain  $R$  are called **associates** if there exists a unit  $u \in R$  such that  $a = ub$ .

**Definition 3.4.** An integral domain has **unique factorization** if every element can be written as a product of irreducibles which are unique up to order and associates.

**Theorem 3.4.1.** *An integral domain  $R$  has unique factorization if all irreducible elements are prime.*

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

**Definition 3.5.** A **polynomial ring**  $R[x]$  of some ring  $R$  is created by using polynomials of the variable  $x$  using coefficients from  $R$ .

*Remark 3.5.1.* For some field  $F$ , Euclidean division works on  $F[x]$  because all non-zero coefficients are units. It then follows that irreducible elements are prime, so unique factorization exists in  $F[x]$ .

**Theorem 3.5.1** (Fundamental Theorem of Algebra). *The only irreducible polynomials in  $\mathbb{C}[x]$  are linear.*

*Remark 3.5.2.* It follows from Theorem 3.5.1 that the only irreducible polynomials in  $\mathbb{R}[x]$  are linear or quadratic. This can be proven using  $\mathbb{R}[x] \subset \mathbb{C}[x]$  and that multiplying some linear  $f(x) \in \mathbb{C}[x]$  with its conjugate results in some  $g(x) \in \mathbb{R}[x]$  with  $\deg(g(x)) = 2$ .

**Definition 3.6.** A subring  $I$  of ring  $R$  is called an **ideal** if for all  $a \in I$  and  $r \in R$ ,  $ra, ar \in I$ .

**Definition 3.7.** For a commutative ring  $R$  and  $a \in R$ , a **principal ideal** generated by  $a$  is defined as  $aR = \{ar : r \in R\}$ . For  $a, b \in R$ , we can also generate  $(a, b)R = \{xa + yb : x, y \in R\}$ .

*Remark 3.7.1.* For  $a \in R$  with integral domain  $R$ ,  $aR = 1R = R$  if and only if  $a$  is a unit.

*Remark 3.7.2.* For  $a, b \in R$ ,  $b \mid a \implies aR \subseteq bR$ . Furthermore,  $aR = bR$  if and only if  $a$  and  $b$  are associates.

*Remark 3.7.3.* For  $a, b \in R$ , if  $a$  is irreducible and  $b \mid a$ , then  $aR \subseteq bR \subseteq R$  so either  $aR = bR$  or  $bR = R$ . Therefore,  $aR$  is not properly contained in any other principal ideal. Also, if  $a$  is not irreducible and  $b$  is not a unit, then  $aR \subset bR \subset R$ .

**Theorem 3.7.1.** *If an element  $a \in R$  cannot be written as a finite product of irreducibles, then  $R$  has an infinite ascending chain of principal ideals.*

*Proof.* Assume that  $a$  cannot be written as a finite product of irreducibles. Then,  $a = r_1a_1 = r_1r_2a_2 = \dots$  for non-units  $r_i, a_i$  and reducible  $a_i$ . This implies  $aR \subset a_1R \subset a_2R \subset \dots$ .  $\square$

*Remark 3.7.4.* This tells us that every element in  $\mathbb{N}$  has a factorization into irreducibles since every proper divisor is “smaller” so there cannot be an infinite chain.

**Definition 3.8.** An integral domain  $R$  is a **principal ideal domain** if every ideal in  $R$  is a principal ideal.

**Proposition 3.8.1.** *The ring  $\mathbb{Z}$  is a principal ideal domain.*

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

Let  $b \in I$  be some other element in  $I$ . Then we have  $b = qa + r$  for  $0 \leq r < a$ . This also means  $b - qa = r$  so  $r \in I$ . However,

by the minimality of  $a$ , this implies  $r = 0$  so  $b$  is a multiple of  $a$  and  $b \in a\mathbb{Z}$ .  $\square$

**Corollary 3.8.1.** *For field  $F$ ,  $F[x]$  is a principal ideal domain.*

**Theorem 3.8.1.** *For a principal ideal domain, every ascending chain of ideals stabilizes.*

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

**Definition 3.9.** Let  $I, J$  be ideals of  $R$ . Then,  $I + J$  is the smallest ideal which contains both  $I$  and  $J$ . Therefore,  $I + J = \{a + b : a \in I \text{ and } b \in J\}$ .

*Remark 3.9.1.* Since  $\mathbb{Z}$  is a principal ideal domain,  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ . Then,  $d\mathbb{Z} = \{xa + yb : x, y \in \mathbb{Z}\}$ . Therefore,  $d = \gcd(a, b)$  since it is the least positive element (by proof of Theorem 3.8.1).

**Definition 3.10.** An ideal  $I$  of ring  $R$  is a **prime ideal** if  $ab \in I$  implies  $a \in I$  or  $b \in I$  for all  $a, b \in R$ .

*Remark 3.10.1.* An element  $p \in R$  is prime if and only if  $pR$  is prime. Why?

*Remark 3.10.2.* Not all prime ideals are principal (eg.  $(x, y) \subset \mathbb{Q}[x, y]$ ).

**Definition 3.11.** An ideal  $I$  in ring  $R$  is called **maximal** if for any ideal  $J \subseteq R$  where  $I \subseteq J \subseteq R$ , it follows that  $I = J$  or  $J = R$ .

*Remark 3.11.1.* In a principal ideal domain, the principal ideal generated by an irreducible element is maximal.

**Theorem 3.11.1.** *In an integral domain, maximal ideals are prime.*

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

*Remark 3.11.2.* For a principal ideal domain  $R$ , this gives us that  $a \in R$  is irreducible implies  $aR$  is maximal implies  $aR$  is prime implies  $a$  is prime. Therefore, by Theorem 3.4.1, every principal ideal domain has unique factorization.

**Definition 3.12.** A ring is a unique factorization domain if every non-zero non-unit can be written uniquely as a product of irreducible elements, up to order and associates. Duplicate of Definition 3.4; don't ask why.

*Remark 3.12.1.* Not all unique factorization domains are principal ideal domains. (eg.  $\mathbb{Z}[x]$  with  $2\mathbb{Z}[x] + x\mathbb{Z}[x]$ ).

## 4 Ring Homomorphisms

**Definition 4.1.** A **ring homomorphism** for rings  $R, S$  is a map  $\varphi : R \rightarrow S$  satisfying  $\varphi(a + b) = \varphi(a) + \varphi(b)$  and  $\varphi(ab) = \varphi(a)\varphi(b)$  for all  $a, b \in R$ .

**Definition 4.2.** If there exists a  $\varphi^{-1} : S \rightarrow R$  for a ring homomorphism  $\varphi : R \rightarrow S$  such that  $\varphi^{-1}(\varphi(a)) = a$  for all  $a \in R$ , we call  $R$  and  $S$  **isomorphic**.

*Remark 4.2.1.* We can show the inverse of a bijective ring homomorphism  $\varphi : R \rightarrow S$  is also a ring homomorphism, therefore,  $R$  and  $S$  are isomorphic.



*Remark 4.2.2.* For ring homomorphism  $\varphi : R \rightarrow S$ , we have  $\varphi(0_R) = 0_S$ ,  $\varphi(-a) = -\varphi(a)$  for all elements  $a \in R$ , and  $\varphi(a^{-1}) = \varphi(a)^{-1}$  for all units  $a \in R$ . We can also show  $\varphi(R) = \{\varphi(r) : r \in R\}$  is a subring of  $S$ .

**Definition 4.3.** The **kernel** of  $\varphi : R \rightarrow S$  is defined as  $\ker(\varphi) = \{\varphi(r) = 0_S : r \in R\}$ .

*Remark 4.3.1.* We can show that  $\ker(\varphi)$  is an ideal.

**Theorem 4.3.1.** *A ring homomorphism  $\varphi : R \rightarrow S$  is injective if and only if  $\ker(\varphi) = \{0_R\}$ .*

*Proof.* Suppose, towards a contradiction, that  $\varphi$  is not injective, that is, there exists  $a, b \in R$  satisfying  $\varphi(a) = \varphi(b)$  and  $a \neq b$ . Then,  $a - b \in \ker(\varphi)$  but  $a - b \neq 0_R$ .  $\square$

**Theorem 4.3.2.** *Let  $R$  be a commutative ring with unity and  $\varphi : R \rightarrow S$  be a surjective ring homomorphism. Then,  $S$  is an integral domain if and only if  $\ker(\varphi)$  is a prime ideal.*

*Proof.* Let  $a, b \in S$  with  $\varphi(x) = a$  and  $\varphi(y) = b$ . Suppose  $\ker(\varphi)$  is a prime ideal. Then,  $ab = 0 \implies \phi(x)\phi(y) = 0 \implies \phi(xy) = 0$  so either  $x \in \ker(\varphi)$  or  $y \in \ker(\varphi)$ . Without loss of generality, let  $x \in \ker(\varphi)$  so  $\varphi(x) = a = 0$ .

Suppose  $\ker(\varphi)$  is not a prime ideal. There exists  $xy \in \ker(\varphi)$  such that  $x \notin \ker(\varphi)$  and  $y \notin \ker(\varphi)$ . Then,  $0 = \varphi(xy) = \varphi(x)\varphi(y) = ab = 0$  but  $\varphi(x) \neq 0$  and  $\varphi(y) \neq 0$ .  $\square$

**Theorem 4.3.3.** *Let  $R$  be a commutative ring with unity,  $S$  a non-zero ring, and  $\varphi : R \rightarrow S$  a surjective ring homomorphism. Then,  $S$  is a field if and only if  $\ker(\varphi)$  is a maximal ideal.*

*Proof.* Suppose  $\ker(\varphi)$  is maximal. Let  $b \in S$  be non-zero and define  $J = \varphi^{-1}(bS) = \{\varphi(r) \in bS : r \in R\}$ . We can show that  $J$  is an ideal satisfying  $\ker(\varphi) \subseteq J \subseteq R$ . Then, by maximality of  $J$ ,  $\ker(\varphi) = J$  or  $J = R$ . However, since  $b \neq 0$ ,  $J = R$  so  $b$  is a unit. It then follows that  $S$  is a field.

Now suppose  $\ker(\varphi)$  is not maximal, that is, there exists an ideal  $I$  such that  $\ker(\varphi) \subset I \subset R$ . Pick  $y \in I \setminus \ker(\varphi)$  and assume, for a contradiction, that  $S$  is a field. Then, there exists  $x \in R$  such that  $\varphi(x)\varphi(y) = 1_S$  so  $\varphi(xy) = \varphi(1_R)$ . It follows that  $xy - 1_R = r \in \ker(\varphi)$  so  $1_R = xy - r \in I$  since  $xy, r \in I$ . Therefore,  $I = R$ , a contradiction.  $\square$

**Theorem 4.3.4** (First Isomorphism Theorem). *If  $\varphi : R \rightarrow S_1$  and  $\psi : R \rightarrow S_2$  are surjective ring homomorphisms with  $\ker(\varphi) = \ker(\psi)$ , there is a ring isomorphism  $\sigma : S_1 \rightarrow S_2$  where  $\sigma(\varphi(x)) = \psi(x)$  for all  $x \in R$ .*

*Proof.* Since  $\sigma$  is a composition of ring homomorphisms, it itself is a ring homomorphism. Therefore, it suffices to show  $\sigma$  is both injective and surjective.

Let  $x, y \in R$  such that  $\sigma(\varphi(x)) = \sigma(\varphi(y))$ . Then,  $\psi(x) = \psi(y)$  so  $\psi(x - y) = 0_{S_2}$  and  $x - y \in \ker(\psi)$ . Since  $\ker(\psi) = \ker(\varphi)$ ,  $x - y \in \ker(\varphi)$  so  $\varphi(x) = \varphi(y)$ . Therefore,  $\sigma$  is injective.

For any  $b \in S_2$ , we have  $\psi(x) = b$  for some  $x \in R$ . Then,  $\sigma(\varphi(x)) = b$  so  $\sigma$  is surjective.  $\square$

*Remark 4.3.2.* It follows from Theorem 4.3.4 that, for a surjective homomorphism  $\varphi : R \rightarrow S$ ,  $S$  is entirely determined (up to isomorphism) by  $R$  and  $\ker(\varphi)$ .

**Definition 4.4.** For ring  $R$ , ideal  $I \subseteq R$ , and  $a \in R$ , the **coset** of  $a$  modulo  $I$  is defined  $a + I = \{a + x : x \in I\} = [a]_I$ .

**Theorem 4.4.1.** *Let  $a + I$  and  $b + I$  be cosets. Then, either  $a + I = b + I$  or  $(a + I) \cap (b + I) = \emptyset$ .*

*Proof.* Suppose  $(a + I) \cap (b + I) \neq \emptyset$  and let  $c \in (a + I) \cap (b + I)$ . Then,  $c = a + x = b + y \implies a - b = y - x \in I$ . Now, for all  $a + z \in a + I$ ,  $a + z - (a - b) = z + b \in b + I$ .  $\square$

**Definition 4.5.** The **quotient ring** for ring  $R$  by an ideal  $I \subseteq R$  is denoted  $R/I = \{a + I : a \in R\}$  and represents the collection of cosets modulo  $I$ .

*Remark 4.5.1.* It follows from Theorem 4.4.1 that the map for  $\varphi : R \rightarrow R/I$  where  $a \mapsto a + I$  is well defined. Furthermore, we can show  $\varphi$  is a surjective ring homomorphism with  $\ker(\varphi) = I$ .

**Theorem 4.5.1** (Chinese Remainder Theorem). *Let  $R$  be a commutative ring with unity and  $I, J \subset R$  be ideals satisfying  $I + J = R$ . Then,  $R/(I + J) \cong R/I \times R/J$ .*

*Proof.* We explain the isomorphism via Theorem 4.3.4. Define  $\varphi : R \rightarrow R/(I \cap J)$  as  $\varphi(a) \mapsto a + (I \cap J)$  and  $\psi : R \rightarrow R/I \times R/J$  as  $\psi(a) \mapsto (a + I, a + J)$ . Then,  $\ker(\varphi) = \ker(\psi)$  since  $c \in (I \cap J) \iff c \in I$  and  $c \in J$ . Also,  $\varphi$  is surjective by definition. Therefore, it suffices to show  $\psi$  is surjective.

We want that for all  $a + I$  and  $b + J$ , there exists  $c \in R$  such that  $c + I = a + I$  and  $c + J = b + J$ . Since  $I + J = R$ ,  $1_R \in I + J$  so there exists  $x \in I$  and  $y \in J$  such that  $x + y = 1$ . We will choose  $c = ax + by$  and show that  $c - a \in I$ . Then, by symmetry,  $c - b \in J$  and we are done.

$$c - a = (ay + bx) - a(x + y) = (b - a)x \in I$$

$\square$

## 5 Fields and Stuff

**Theorem 5.0.1.** *Let  $R$  be a ring with unity and define the ring homomorphism  $\varphi : \mathbb{Z} \rightarrow R$  as  $\varphi(n) = \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}$ . Then,  $\ker(\varphi) = c\mathbb{Z}$  for  $c$  the characteristic of  $R$ .*

*Remark 5.0.1.* We see, from Theorem 5.0.1, that every ring with unity and characteristic  $c$  contains a subring isomorphic to  $\mathbb{Z}/c\mathbb{Z}$ . Furthermore, for field  $F$  with characteristic  $p$  ( $p$  is prime by Theorem 2.1.1),  $F$  contains a subring of  $\mathbb{Z}/p\mathbb{Z}$  or  $\mathbb{Q}$ .

**Definition 5.1.** The **prime fields**  $F_p$  are defined to be  $\mathbb{Q}$  and  $\mathbb{Z}/p\mathbb{Z}$  (for any prime  $p$ ).

*Remark 5.1.1.* Every field contains a prime field.

**Definition 5.2.** A **field extension** of field  $F$  is a field  $E$  such that  $F \subseteq E$ .

**Definition 5.3.** An  **$F$ -vector space** for a field  $F$  is a commutative group  $V$  with scalar multiplication between  $F$  and  $V$  such that, for  $a, b \in F$  and  $u, v \in V$ ,  $a(u + v) = au + av$ ,  $(a + b)v = av + bv$ ,  $(ab)v = a(bv)$ , and  $\exists 1 \in F$  such that  $1v = v$ .

**Definition 5.4.** For an  $F$ -vector space  $V$ , an element  $w \in V$  is an  **$F$ -linear combination** of  $v_1, \dots, v_n \in V$  if there exist  $a_1, \dots, a_n \in F$  such that  $a_1v_1 + \cdots + a_nv_n = w$ .

**Definition 5.5.** We say  $U \subseteq V$  **generates**  $V$  over  $F$  if every  $w \in V$  can be written as an  $F$ -linear combination of  $U$ .

**Definition 5.6.** For an  $F$ -vector space  $V$ , we say that the set  $U = \{v_1, \dots, v_n\} \subset V$  is **linearly independent** if, for  $a_1, \dots, a_n \in F$ ,  $a_1v_1 + \cdots + a_nv_n = 0$  implies  $a_1 = \cdots = a_n = 0$ .

**Definition 5.7.** We say  $U \subseteq V$  is an  **$F$ -basis** for  $V$  if  $U$  is linearly independent and generates  $V$ .

**Theorem 5.7.1.** *All finite  $F$ -bases of  $V$  are the same size.*

**Definition 5.8.** If  $U = \{v_1, \dots, v_n\}$  is a finite  $F$ -basis of  $V$ , we say that  $V$  is an  **$n$ -dimensional  $F$ -vector space**.

*Remark 5.8.1.* If  $V$  can be generated by a finite basis, it is finite dimensional as an  $F$ -vector space.

**Theorem 5.8.1.** *A finite field  $E$  has a positive prime characteristic  $p$  and contains  $p^n$  elements for some  $n$ .*

**Theorem 5.8.2.** *Since  $E$  is finite, it must contain some prime field  $F = \mathbb{Z}/p\mathbb{Z}$ , so  $E$  is an  $F$ -vector space. Since  $E$  is finite and generates itself, it must contain a finite basis  $\{v_1, \dots, v_n\}$ .*

*We define  $\varphi : F^n \rightarrow E$  as  $\varphi(a_1, \dots, a_n) = a_1v_1 + \dots + a_nv_n$ . By definition,  $\varphi$  is surjective. Furthermore,  $a_1v_1 + \dots + a_nv_n = b_1v_1 + \dots + b_nv_n$  implies  $(a_1 - b_1)v_1 + \dots + (a_n - b_n)v_n = 0$ , so  $a_1 = b_1, \dots, a_n = b_n$  by the linear independence of the basis. Therefore,  $\varphi$  is also injective. Since there are  $p^n$  elements in  $F^n$ , we conclude that there are also  $p^n$  elements in  $E$  by the bijectivity of  $\varphi$ .*

**Definition 5.9.** For  $E$  a field extension of  $F$ ,  $\alpha \in E$  is **algebraic** if it is a root of some polynomial  $g \in F[x]$ . Otherwise, it is **transcendental**.

**Definition 5.10.** For  $\alpha \in E$  algebraic over  $F \subseteq E$ , the **minimal polynomial** of  $\alpha$  over  $F$  is the monic polynomial  $P \in F[x]$  of least degree for which  $P(\alpha) = 0$ .

**Theorem 5.10.1.** *The minimal polynomial of  $\alpha$  over  $F$  is unique and irreducible. Furthermore, any  $g \in F[x]$  satisfying  $g(\alpha) = 0$  is divisible by the minimal polynomial.*

*Proof.* Let  $P \in F[x]$  be the minimal polynomial of  $\alpha$  over  $F$ . Suppose the  $P$  is not unique, so we have another minimal polynomial  $Q \in F[x]$ . Then,  $(P - Q)(\alpha) = 0$  but  $\deg(P - Q) <$

$\deg(P)$ , contradicting the minimality of  $P$ . Now suppose  $P$  is reducible, then  $0 = P(\alpha) = f(\alpha)g(\alpha)$ . However,  $x - \alpha$  divides one of  $f(x), g(x)$  which contradicts the minimality of  $P$ .

Suppose  $g \in F[x]$  such that  $g(\alpha) = 0$ . Then, by Euclidean Division,  $g(x) = q(x)P(x) + r(x)$  with  $\deg(r) < \deg(P)$ . However,  $0 = g(\alpha) = \cancel{q(\alpha)P(\alpha)} + r(\alpha) = r(\alpha) = 0$ . Therefore, since  $\deg(r) < \deg(P)$ ,  $r(x) = 0$  by the minimality of  $P$ .  $\square$

**Theorem 5.10.2.** *For a field extension  $E$  of  $F$  and algebraic  $\alpha \in E$  over  $F$  with minimal polynomial  $P = a_0x^0 + \cdots + a_dx^d \in F[x]$ ,  $F(\alpha) = \{u_0\alpha^0 + \cdots + u_{d-1}\alpha^{d-1} : u_0, \dots, u_{d-1} \in F\}$  is a  $d$ -dimensional subfield of  $E$  as an  $F$ -vector space.*

*Proof.* It is clear that  $F(\alpha)$  contains 0 and is closed under addition and taking additive inverses. It suffices to show that it is closed under multiplication and taking multiplicative inverses.

See that  $P(\alpha) = 0$  so  $\alpha^d = -(a_0\alpha^0 + \cdots + a_{d-1}\alpha^{d-1})$ . Then, any expression with a term including  $\alpha^m$  where  $m > d - 1$  can be rewritten as an expression on  $\alpha^0, \dots, \alpha^{d-1}$ , therefore,  $F(\alpha)$  is closed over multiplication.

For some  $w \in F(\alpha)$ , choose  $f(x) \in F[x]$  such that  $f(\alpha) = w$ . Then, since  $F[x]$  are polynomials over a field, we can use the Euclidean Algorithm on  $f, P$  to find  $g(x), h(x) \in F[x]$  such that  $f(x)g(x) + h(x)P(x) = 1$ . Then,  $f(\alpha)g(\alpha) + \cancel{h(\alpha)P(\alpha)} = wg(\alpha) = 1$  with  $g(\alpha) \in F(\alpha)$ .  $\square$

**Theorem 5.10.3.** *For an algebraic  $\alpha \in E$  over  $F$ , with minimal polynomial of degree  $d$ , define  $\varphi : F[x] \rightarrow F(\alpha)$  such that  $\varphi(f(x)) = f(\alpha)$ . Then,  $\varphi$  is a surjective ring homomorphism with  $\ker(\varphi) = \langle P \rangle$  so  $F(\alpha)$  is isomorphic to  $F(\alpha)/\langle P \rangle$ .*

*Proof.* We know that polynomial evaluation is a ring homomorphism. We also know  $\varphi(F[x]) = F(\alpha)$  since  $\varphi(F[x]) \supseteq F(\alpha)$  trivially and every expression containing  $\alpha^d$  can be written as an expression on  $\alpha^0, \dots, \alpha^{d-1}$  so  $\varphi(F[x]) = F(\alpha)$  which means  $\varphi$  is surjective. Finally,  $\ker(\varphi) = \langle P \rangle$  because every  $g \in F[x]$  with  $g(\alpha) = 0$  is divisible by  $P$  (Theorem 5.10.1).  $\square$

**Theorem 5.10.4** (Kronecker). *Let  $F$  be a field and  $g \in F[x]$  be a polynomial of degree at least 1. There is a field extension  $E$  of  $F$  such that  $g$  has a root in  $E$ .*

*Proof.* It suffices to prove the theorem for irreducible polynomials  $g \in F[x]$  without a root in  $F$ . Let  $E = F[x]/\langle g \rangle$  and take  $\alpha = x + \langle g \rangle \in E$ . Then,  $g(\alpha) = 0$ .  $\square$

**Definition 5.11.** A **splitting field** of a polynomial  $g \in F[x]$  is an extension  $F(\alpha_1) \cdots (\alpha_r)$  such that  $g(x) = c \prod (x - \alpha_i)^{e_i}$ .

**Theorem 5.11.1.** *Let  $g \in F[x]$  be a polynomial. All splitting fields of  $g$  are isomorphic.*

*Proof.* Let  $E_1, E_2$  be two splitting fields of  $g$ . We proceed by induction on  $\deg(g)$  to show that they are isomorphic. If  $\deg(g) = 1$ ,  $F = E_1 = E_2$  so the fields are isomorphic.

Suppose  $g$  has degree at least 2. Choose  $P$  to be an irreducible factor of  $g$  satisfying  $\deg(P) \geq 2$ . Then,  $P$  must contain two roots, so let  $\alpha \in E_1$  and  $\beta \in E_2$  be two roots of  $P$ . Since  $F[x] \cong F(\alpha) \subseteq E_1$  and  $F[x] \cong F(\beta) \subseteq E_2$ , we have that both  $E_1$  and  $E_2$  contain subfields isomorphic to  $F[x]/\langle P \rangle$ . However, we also have  $g(x) = (x - \alpha)h_1(x) = (x - \beta)h_2(x)$  in  $F[x]/\langle P \rangle$ . It then follows that  $E_1 \cong E_2$ .  $\square$

*Remark 5.11.1.* In finite field  $F$  with  $m$  elements,  $a^m - a = 0$  for all  $a \in F$  (by Theorem 2.1.2). Therefore,  $F$  is a splitting field of  $x^m - x = 0$ . It follows from Theorem 5.11.1 that all fields with the same number of elements are isomorphic.

*Remark 5.11.2.* We want to show there exists a unique field with exactly  $p^n$  elements for all primes and positive integers  $n$ . Since we have Remark 5.11.1, it suffices to show there exists a field of  $p^n$  elements for all  $p^n$ . To do so, we show the splitting field of  $x^{p^n} - x \in (\mathbb{Z}/p\mathbb{Z})[x]$  has exactly  $p^n$  elements.

**Theorem 5.11.2.** *A splitting field of  $x^{p^n} - x \in (\mathbb{Z}/p\mathbb{Z})[x]$  has at least  $p^n$  elements.*

*Proof.* We will show  $g = x^{p^n} - x$  has  $p^n$  different roots, and it suffices to show  $g$  has no duplicate linear factors. Let  $h$  be a linear polynomial, then  $h^2 \mid g$  if and only if  $h \mid g$  and  $h \mid g'$ , where  $g'$  is the formal derivative of  $g$ . However,  $g' = p^n x^{p^n-1} - 1 = -1$  since  $\mathbb{Z}/p\mathbb{Z}$  is of characteristic  $p$ .  $\square$

**Theorem 5.11.3** (Freshman's Dream). *Let  $R$  be a commutative ring with unity and prime characteristic  $p$ . Then,  $(a+b)^p = a^p + b^p$  for all  $a, b \in R$ .*

*Proof.* Recall that  $p \mid \binom{p}{n}$  if and only if  $n \in \{1, \dots, p-1\}$ . Then, we easily see  $(a+b)^p = \sum_{n=0}^p \binom{p}{n} a^n b^{p-n} = a^p + b^p$ .  $\square$

**Theorem 5.11.4.** *If  $F$  is a finite field with characteristic  $p$ , then  $\phi(a) = a^p$  is a field automorphism.*

*Proof.* The fact that  $\phi$  is a homomorphism follows from Theorem 5.11.3. Also note  $\ker(\phi)$  is an ideal. Then, since  $F$  is a field and  $\phi(1) = 1$ , we see that  $1 \notin \ker(\phi)$  so  $\ker(\phi) = \{0\}$ .

From here, it suffices to show  $\phi$  is surjective. This follows from the fact that  $F$  has no zero divisors.  $\square$



**Theorem 5.11.5.** *Let  $F$  be a field with characteristic  $p$ . Then  $R = \{\alpha \in F : \alpha^{p^n} = \alpha\}$  is a subfield of  $F$ .*

**Theorem 5.11.6.** *There exists a field  $F$  with  $p^n$  elements.*

*Proof.* Let  $E$  be a splitting field of  $x^{p^n} - x = 0 \in (\mathbb{Z}/p\mathbb{Z})[x]$ . We see that the subfield  $R = \{\alpha \in E : \alpha^{p^n} = \alpha\} \subseteq E$  contains exactly  $p^n$  elements. However,  $R$  contains all the roots of  $x^{p^n} - x = 0$ , so  $R = E$ . This completes the proof.  $\square$