ADVANCED MODERN ALGEBRA

Joseph J. Rotman

June 20, 2020

Contents

1 Things Past

1.1 Some Number Theory

Least Integer Axiom (**Well-ordering Principle**). There is a smallest integer in every nonempty subset C of $\mathbb{N}$

1.2 Roots of Unity

Proposition 1.1 (Polar Decomposition). *Every complex number z has a factorization*

$$z = r(\cos\theta + i\sin\theta)$$

where $r = |z| \geq 0$ and $0 \leq \theta \leq 2\pi$

Proposition 1.2 (Addition Theorem). *If $z = \cos\theta + i\sin\theta$ and $w = \cos\psi + i\sin\psi$, then*

$$zw = \cos(\theta+\psi) + i\sin(\theta+\psi)$$

Theorem 1.3 (De Moivre). $\forall x \in \mathbb{R}, n \in \mathbb{N}$

$$\cos(nx) + i\sin(nx) = (\cos x + i\sin x)^n$$

Theorem 1.4 (Euler). $e^{ix} = \cos x + i\sin x$

Definition 1.5. If $n \in \mathbb{N} \geq 1$, an **nth root of unity** is a complex number ξ with $\xi^n = 1$

Corollary 1.6. *Every nth root of unity is equal to*

$$e^{2\pi ik/n} = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n})$$

for $k = 0, 1, \ldots, n-1$

$$x^n - 1 = \prod_{\xi^n=1}(x-\xi)$$

If ξ is an nth root of unity and if n is the smallest, then ξ is a **primitive nth root of unity**

Definition 1.7. If $d \in \mathbb{N}^+$, then the dth **cyclotomic polynomial** is

$$\Phi_d(x) = \prod(x-\xi)$$

where ξ ranges over all the *primitive dth* roots of unity

Proposition 1.8. *For every integer $n \geq 1$*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Definition 1.9. Define **Euler ϕ-function** as the degree of the nth cyclotomic polynomial

$$\phi(n) = \deg(\Phi_n(x))$$

Proposition 1.10. *If $n \geq 1$ is an integer, then $\phi(n)$ is the number of integers k with $1 \leq k \leq n$ and $(k, n) = 1$*

Proof. Suffice to prove $e^{2\pi ik/n}$ is a primitive nth root of unity if and only if k and n are relatively prime □

Corollary 1.11. *For every integer $n \geq 1$, we have*

$$n = \sum_{d|n} \phi(d)$$

1.3 Some Set Theory

Proposition 1.12.
1. *If $f : X \to Y$ and $g : Y \to X$ are functions s.t. $g \circ f = 1_X$, then f is injective and g is surjective*
2. *A function $f : X \to Y$ has an inverse $g : Y \to X$ if and only if f is a bijection*

2 Group I

2.1 Permutations

Definition 2.1. A **permutation** of a set X is a bijection from X to itself.

Definition 2.2. The family of all the permutations of a set X, denoted by S_X is called the **symmetric group** on X. When $X = \{1, 2, \ldots, n\}$, S_X is usually denoted by X_n and is called the **symmetric group on n letters**

Definition 2.3. Let $i_1, i_2, \ldots, i_r$ be distinct integers in $\{1, 2, \ldots, n\}$. If $\alpha \in S_n$ fixes the other integers and if

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \ldots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1$$

then α is called an **r-cycle**. α is a cycle of **length** r and denoted by

$$\alpha = (i_1\ i_2\ \ldots\ i_r)$$

2-cycles are also called the **transpositions**.

Definition 2.4. Two permutations $\alpha, \beta \in S_n$ are **disjoint** if every i moved by one is fixed by the other.

Lemma 2.5. *Disjoint permutations $\alpha, \beta \in S_n$ commute*

Proposition 2.6. *Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.*

Proof. Induction on the number k of points moved by α □

Definition 2.7. A **complete factorization** of a permutation α is a factorization of α into disjoint cycles that contains exactly one 1-cycle (i) for every i fixed by α

Theorem 2.8. *Let $\alpha \in S_n$ and let $\alpha = \beta_1 \dots \beta_t$ be a complete factorization into disjoint cycles. This factorization is unique except for the order in which the cycles occur*

Proof. for all i, if $\beta_t(i) \neq i$, then $\beta_t^k(i) \neq \beta_t^{k-1}(i)$ for any $k \geq 1$ □

Lemma 2.9. *If $\gamma, \alpha \in S_n$, then $\alpha\gamma\alpha^{-1}$ has the same cycle structure as γ. In more detail, if the complete factorization of γ is*

$$\gamma = \beta_1\beta_2 \dots (i_1\ i_2\ \dots) \dots \beta_t$$

then $\alpha\gamma\alpha^{-1}$ is permutation that is obtained from γ by applying α to the symbols in the cycles of γ

Example 2.1. Suppose

$$\beta = (1\ 2\ 3)(4)(5)$$
$$\gamma = (5\ 2\ 4)(1)(3)$$

then we can easily find the α

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}$$

and so $\alpha = (1\ 5\ 3\ 4)$. Now $\alpha \in S_5$ and $\gamma = (\alpha 1\ \alpha 2\ \alpha 3)$

Theorem 2.10. *Permutations γ and σ in S_n has the same cycle structure if and only if there exists $\alpha \in S_n$ with $\sigma = \alpha\gamma\alpha^{-1}$*

Proposition 2.11. *If $n \geq 2$ then every $\alpha \in S_n$ is a product of tranpositions*

Proof. $(1\ 2\ \ldots\ r) = (1\ r)(1\ r-1)\ldots(1\ 2)$ □

Example 2.2. The **15-puzzle** has a **starting position** that is a 4×4 array of the numbers between 1 and 15 and a symbol #, which we interpret as "blank". For example, consider the following starting position

3	15	4	8
10	11	1	9
2	5	13	12
6	7	14	#

A **simple move** interchanges the blank with a symbol adjacent to it. We win the game if after a sequence of simple moves, the starting position is transformed into the standard array $1, 2, \ldots, 15, \#$.

To analyze this game, note that the given array is really a permutation $\alpha \in S_{16}$. For example, the given starting position is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 15 & 4 & 8 & 10 & 11 & 1 & 9 & 2 & 5 & 13 & 12 & 6 & 7 & 14 & 16 \end{pmatrix}$$

To win the game, we need special transpositions $\tau_1, \ldots, \tau_m$ sot that

$$\tau_m \ldots \tau_1 \alpha = (1)$$

Definition 2.12. A permutation $\alpha \in S_n$ is **even** if it can be factored into a product of an even number of transpositions. Otherwise **odd**

Definition 2.13. If $\alpha \in S_n$ and $\alpha = \beta_1 \ldots \beta_t$ is a complete factorization, then **signum** α is defined by

$$\operatorname{sgn}(\alpha) = (-1)^{n-t}$$

Theorem 2.14. *For all $\alpha, \beta \in S_n$*

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$$

Theorem 2.15.
1. *Let $\alpha \in S_n$; if $\operatorname{sgn}(\alpha) = 1$ then α is even. otherwise odd*
2. *A permutation α is odd if and only if it's a product of an odd number of transpositions*

Corollary 2.16. *Let $\alpha, \beta \in S_n$. If α and β have the same parity, then $\alpha\beta$ is even while if α and β have distinct parity, $\alpha\beta$ is odd*

Example 2.3. An analysis of the 15-puzzle shows that if $\alpha \in S_{16}$ is the starting position, then the game can be won if and only if α is an even permutation that fixes 16.

The blank 16 starts in position 16. Each simple move takes 16 up, down, left or right. Thus the total number m of moves is $u + d + l + r$. If 16 is to return home, each one of these must be undone. Thus the total number of moves is even: $m = 2u + 2r$. Hence $\alpha = \tau_1 \dots \tau_m$ and so α is an even permutation. In example

$$\alpha = (1\ 3\ 4\ 8\ 9\ 2\ 15\ 14\ 7)(5\ 10)(6\ 11\ 13)(12)(16)$$

Now $\text{sgn}(\alpha) = (-1)^{16-5} = -1$.

2.2 Groups

Definition 2.17. A **binary operation** on a set G is a function

$$* : G \times G \to G$$

Definition 2.18. A **group** is a set G equipped with a binary operation * s.t.

1. the **associative law** holds
2. **identity**
3. every $x \in G$ has an **inverse**, there is a $x' \in G$ with $x * x' = e = x' * x$

Definition 2.19. A group G is called **abelian** if it satisfies the **commutative law**

Lemma 2.20. *Let G be a group*

1. *The **cancellation laws** holds: if either $x * a = x * b$ or $a * x = b * x$, then $a = b$*
2. *e is unique*
3. *Each $x \in G$ has a unique inverse*
4. *$(x^{-1})^{-1} = x$*

Definition 2.21. An expression $a_1 a_2 \dots a_n$ **needs no parentheses** if all the ultimate products it yields are equal

Theorem 2.22 (Generalized Associativity)**.** *If G is a group and $a_1, a_2, \dots, a_n \in G$ then the expression $a_1 a_2 \dots a_n$ needs no parentheses*

Definition 2.23. Let G be a group and let $a \in G$. If $a^k = 1$ for some $k > 1$ then the smallest such exponent $k \geq 1$ is called the **order** or a; if no such power exists, then one says that a has **infinite order**

Proposition 2.24. *If G is a finite group, then every $x \in G$ has finite order*

Definition 2.25. A **motion** is a distance preserving bijection $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$. If π is a polygon in the plane, then its **symmetry group** $\Sigma(\pi)$ consists of all the motions φ for which $\varphi(\pi) = \pi$. The elements of $\Sigma(\pi)$ are called the **symmetries** of π

Let π_4 be a square. Then the group $\Sigma(\pi_4)$ is called the **dihedral group** with 8 elements, denoted by D_8

Definition 2.26. If π_n is a regular polygon with n vertices $v_1, \ldots, v_n$ and center O, then the symmetry group $\Sigma(\pi_n)$ is called the **dihedral group** with $2n$ elements, and it's denoted by D_{2n}

Exercise 2.2.1. If G is a group in which $x^2 = 1$ for every $x \in G$, prove that G must be abelian

Exercise 2.2.2. If G is a group with an even number of elements, prove that the number of elements in G of order 2 is odd. In particular, G must contain an element of order 2.

Proof. 1 is an element of order 1. □

2.3 Lagrange's Theorem

Definition 2.27. A subset H of a group G is a **subgroup** if
1. $1 \in H$
2. if $x, y \in H$, then $xy \in H$
3. if $x \in H$, then $x^{-1} \in H$

If H is a subgroup of G, we write $H \leq G$. If H is a proper subgroup, then we write $H < G$

The four permutations

$$\mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$$

form a group because $\mathbf{V} \leq S_4$

Proposition 2.28. *A subset H of a group G is a subgroup if and only if H is nonempty and whenever $x, y \in H$, $xy^{-1} \in H$*

Proposition 2.29. *A nonempty subset H of a finite group G is a subgroup if and only if H is closed; that is, if $a, b \in H$, then $ab \in H$*

Example 2.4. The subset A_n of S_n, consisting of all the even permutations, is a subgroup called the **alternating group** on n letters

Definition 2.30. If G is a group and $a \in G$

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\text{all powers of } a\}$$

$\langle a \rangle$ is called the **cyclic subgroup** of G **generated** by a. A group G is called **cyclic** if there exists $a \in G$ s.t. $G = \langle a \rangle$, in which case a is called the **generator**

Definition 2.31. The **integers mod** m, denoted by $\mathbb{I}_m$ is the family of all congruence classes mod m

Proposition 2.32. *Let $m \geq 2$ be a fixed integer*

1. *If $a \in \mathbb{Z}$, then $[a] = [r]$ for some r with $0 \leq r < m$*
2. *If $0 \leq r' < r < m$, then $[r'] \neq [r]$*
3. *$\mathbb{I}_m$ has exactly m elements*

Theorem 2.33.

1. *If $G = \langle a \rangle$ is a cyclic group of order n, then a^k is a generator of G if and only if $(k, n) = 1$*
2. *If G is a cyclic group of order n and $\text{gen}(G) = \{\text{all generators of } G\}$, then*

$$\left|\text{gen}(G)\right| = \phi(n)$$

where ϕ is the Euler ϕ-function

Proof. 1. there is $t \in \mathbb{N}$ s.t. $a^{kt} = a$ hence $a^{kt-1} = 1$ and $n \mid kt - 1$

□

Proposition 2.34. *Let G be a finite group and let $a \in G$. Then the order of a is $\left|\langle a \rangle\right|$.*

Definition 2.35. If G is a finite group, then the number of elements in G, denoted by $|G|$ is called the **order** of G

Proposition 2.36. *The intersection $\bigcap_{i \in I} H_i$ of any family of subgroups of a group G is again a subgroup of G*

Corollary 2.37. *If X is a subset of a group G, then there is a subgroup $\langle X \rangle$ of G containing X tHhat is **smallest** in the sense that $\langle X \rangle \leq H$ for every subgroup H of G that contains X*

Definition 2.38. If X is a subset of a group G, then $\langle X \rangle$ is called the **subgroup generated by** X

A **word** on X is an element $g \in G$ of the form $g = x_1^{e_1} \dots x_n^{e_n}$ where $x_i \in X$ and $e_i = \pm 1$ for all i

Proposition 2.39. *If X is a nonempty subset of a group G, then $\langle X \rangle$ is the set of all words on X*

Definition 2.40. If $H \leq G$ and $a \in G$, then the **coset** aH is the subset aH of G, where

$$aH = \{ah : h \in H\}$$

aH **left coset**, Ha **right coset**

Lemma 2.41. $H \leq G, a, b \in G$

1. $aH = bH$ *if and only if* $b^{-1}a \in H$
2. *if* $aH \cap bH \neq \emptyset$, *then* $aH = bH$
3. $|aH| = |H|$ *for all* $a \in G$

Proof. define a relation $a \equiv b$ if $b^{-1}a \in H$ □

Theorem 2.42 (Lagrange's Theorem)**.** *If H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$*

Proof. Let $\{a_1 H, a_2 H, \dots, a_t H\}$ be the family of all the distinct cosets of H in G. Then

$$G = a_1 H \cup a_2 H \cup \dots \cup a_t H$$

hence

$$|G| = |a_1 H| + \dots + |a_t H|$$

But $|a_i H| = |H|$ for all i. Hence $|G| = t|H|$ □

Definition 2.43. The **index** of a subgroup H in G denoted by $[G : H]$, is the number of left cosets of H in G

Note that $|G| = [G : H]|H|$

Corollary 2.44. *If G is a finite group and $a \in G$, then the order of a is a divisor of $|G|$*

Corollary 2.45. *If G is a finite group, then $a^{|G|} = 1$ for all $a \in G$*

Corollary 2.46. *If p is a prime, then every group G of order p is cyclic*

Proposition 2.47. *The set $U(\mathbb{I}_m)$, defined by*

$$U(\mathbb{I}_m) = \{[r] \in \mathbb{I}_m : (r, m) = 1\}$$

is a multiplicative group of order $\phi(m)$. If p is a prime, then $U(\mathbb{I}_p) = \mathbb{I}_p^\times$, the nonzero elements of $\mathbb{I}_p$.

Proof. $(r, m) = 1 = (r', m)$ implies $(rr', m) = 1$. Hence $U(\mathbb{I}_m)$ is closed under multiplication. If $(x, m) = 1$, then $rs + sm = 1$. There fore $(r, m) = 1$. Each of them have inverse. □

Corollary 2.48 (Fermat)**.** *If p is a prime and $a \in \mathbb{Z}$, then*

$$a^p \equiv a \mod p$$

Proof. suffices to show $[a^p] = [a]$ in $\mathbb{I}_p$. If $[a] = [0]$, then $[a^p] = [a]^p = [0]$. Else, since $\left|\mathbb{I}_p^\times\right| = p - 1$, $[a]^{p-1} = [1]$ □

Theorem 2.49 (Euler)**.** *If $(r, m) = 1$, then*

$$r^{\phi(m)} \equiv 1 \mod m$$

Proof. Since $|U(\mathbb{I}_m)| = \phi(m)$. Lagrange's theorem gives $[r]^{\phi(m)} = [1]$ for all $[r] \in U(\mathbb{I}_m)$.

In fact we construct a group to prove this. □

Theorem 2.50 (Wilson's Theorem)**.** *An integer p is a prime if and only if*

$$(p - 1)! \equiv -1 \mod p$$

Proof. Assume that p is a prime. If $a_1, \ldots, a_n$ is a list of all the elements of finite abelian group, then product $a_1 a_2 \ldots a_n$ is the same as the product of all elements a with $a^2 = 1$. Since p is prime, $\mathbb{I}_p^\times$ has only one element of order 2, namely $[-1]$. It follows that the product of all the elements in $\mathbb{I}_p^\times$ namely $[(p - 1)!]$ is equal to $[-1]$.

Conversly assume that m is composite: there are integers a and b with $m = ab$ and $1 < a \leq b < m$. If $a < b$ then $m = ab$ is a divisor of $(m - 1)!$. If $a = b$, then $m = a^2$. if $a = 2$, then $(a^2 - 1)! \equiv 2 \mod 4$. If $2 < a$, then $2a < a^2$ and so a and $2a$ are factors of $(a^2 - 1)!$ □

Exercise 2.3.1. Let G be a group of order 4. Prove that either G is cyclic or $x^2 = 1$ for every $x \in G$. Conclude, using Exercise 2.2.1 that G must be abelian.

Proof. □

2.4 Homomorphisms

Definition 2.51. If $(G, *)$ and $(H, \circ)$ are groups, then a function $f : G \to H$ is a **homomorphism** if

$$f(x * y) = f(x) \circ f(y)$$

for all $x, y \in G$. If f is also a bijection, then f is called an **isomorphism**. G and H are called **isomorphic**, denoted by $G \cong H$

Lemma 2.52. *Let $f : G \to H$ be a homomorphism*

1. $f(1) = 1$
2. $f(x^{-1}) = f(x)^{-1}$
3. $f(x^n) = f(x)^n$ *for all* $n \in \mathbb{Z}$

Definition 2.53. If $f : G \to H$ is a homomorphism, define

$$\ker f = \{x \in G : f(x) = 1$$

and

$$\text{im } f = \{h \in H : h = f(x) \text{ for some } x \in G$$

Proposition 2.54. *Let $f : G \to H$ be a homomorphism*

1. $\ker f$ *is a subgroup of* G *and* $\text{im } f$ *is a subgroup of* H
2. *if* $x \in \ker f$ *and if* $a \in G$, *then* $axa^{-1} \in \ker f$
3. f *is an injection if and only if* $\ker f = \{1\}$

Proof. 3. $f(a) = f(b) \Leftrightarrow f(ab^{-1}) = 1$

□

Definition 2.55. A subgroup K of a group G is called a **normal subgroup** if $k \in K$ and $g \in G$ imply $gkg^{-1} \in K$, denoted by $K \triangleleft G$

Definition 2.56. If G is a group and $a \in G$, then a **conjugate** of a is any element in G of the form

$$gag^{-1}$$

where $g \in G$

Definition 2.57. If G is a group and $g \in G$, define **conjugation** $\gamma_g : G \to G$ by

$$\gamma_g(a) = gag^{-1}$$

for all $a \in G$

Proposition 2.58. *1. If G is a group and $g \in G$, then conjugation $\gamma_g : G \to G$ is an isomorphism*
2. Conjugate elements have the same order

Proof. 1. bijection: $\gamma_g \circ \gamma_{g^{-1}} = 1 = \gamma_{g^{-1}} \circ \gamma_g$.

□

Example 2.5. Define the **center** of a group G, denoted by $Z(G)$, to be

$$Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$$

Example 2.6. If G is a group, then an **automorphism** of G is an isomorphism $f : G \to G$. For example, every conjugation γ_g is an automorphism of G (it is called an **inner automorphism**), for its inverse is conjugation by g^{-1}. The set **Aut**(G) of all the automorphism of G is itself a group.

$$\text{Inn}(G) = \{\gamma_g : g \in G\}$$

is a subgroup of **Aut**(G)

Proposition 2.59. *1. If H is a subgroup of index 2 in a group G, then $g^2 \in H$ for every $g \in G$*
2. If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G

Definition 2.60. The group of **quaternions** is the group **Q** of order 8 consisting of the following matrices in $GL(2, \mathbb{C})$

$$\mathbf{Q} = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\}$$

where I is the identity matrix

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ and } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Example 2.7. Q is normal. By Lagrange's theorem the only possible orders of subgroups are 1,2,4 or 8. The only subgroup of order 2 is $\langle -I \rangle$ since $-I$ is the only element of order 2

Proposition 2.61. *The alternating group A_4 is a group of order 12 having no subgroup of order 6*

Exercise 2.4.1. Show that if there is a bijection $f : X \to Y$, then there is an isomorphism $\varphi : S_X \to S_Y$

Proof. If $\alpha \in S_X$, define $\varphi(\alpha) = f \circ \alpha \circ f^{-1}$. Since f, α, f^{-1} are bijections, $\varphi(\alpha)$ is an bijection. φ is a homomorphism. $\forall \beta \in S_Y$, we have $\alpha = f^{-1} \circ \beta \circ f$ □

2.5 Quotient group

$\mathcal{S}(G)$ is the set of all nonempty subsets of a group G. If $X, Y \in \mathcal{S}(G)$, define

$$XY = \{xy : x \in X \text{ and } y \in Y\}$$

Lemma 2.62. *$K \leq G$ is normal if and only if*

$$gK = Kg$$

A natural question is that whether HK is a subgroup when H and K are subgroups. The answer is no. Let $G = S_3$, $H = \langle(1\ 2)\rangle$, $K = \langle(1\ 3)\rangle$

Proposition 2.63. 1. *If H and K are subgroups of a group G, and if one of them is normal, then $HK \leq G$ and $HK = KH$*
2. *If $H, K \lhd G$, then $HK \lhd G$*

Theorem 2.64. *Let G/K denote the family of all the left cosets of a subgroup K of G. If $K \lhd G$, then*

$$aKbK = abK$$

for all $a, b \in G$ and G/K is a group under this operation

Proof. $aKbK = abKK = abK$ □

G/K is called the **quotient group** G mod K

Corollary 2.65. *Every $K \lhd G$ is the kernel of some homomorphism*

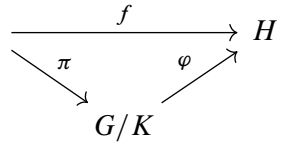
Proof. Define the **natural map** $\pi : G \to G/K, a \mapsto aK$ □

Theorem 2.66 (First Isomorphism Theorem)**.** *If $f : G \to H$ is a homomorphism, then*

$$\ker f \lhd G \quad \text{and} \quad G/\ker f \cong \operatorname{im} f$$

If $\ker f = K$ *and* $\varphi : G/K \to \operatorname{im} f \leq H, aK \mapsto f(a)$*, then φ is an isomorphism*

Remark.



Example 2.8. What's the quotient group $\mathbb{R}/\mathbb{Z}$? Define $f : \mathbb{R} \to S^1$ where S^1 is the circle group by

$$f : x \mapsto e^{2\pi i x}$$

$\mathbb{R}/\mathbb{Z} \cong S^1$

Proposition 2.67 (Product Formula). *If H and K are subgroups of a finite group G, then*

$$|HK||H \cap K| = |H||K|$$

Proof. Define a function $f : H \times K \to HK, (h,k) \mapsto hk$. Show that $\left|f^{-1}(x)\right| = |H \cap K|$.

Claim that if $x = hk$, then

$$f^{-1}(x) = \{(hd, d^{-1}k) : d \in H \cap K\}$$

□

Theorem 2.68 (Second Isomorphism Theorem). *If $H \triangleleft G$, $K \leq G$, then $HK \leq G$, $H \cap K \triangleleft G$ and*

$$K/(H \cap K) \cong HK/H$$

Proof. $hkH = kk^{-1}hkH = kh'H = kH$ □

Theorem 2.69 (Third Isomorphism Theorem). *If $H, K \triangleleft G$ with $K \leq H$, then $H/K \triangleleft G/K$ and*

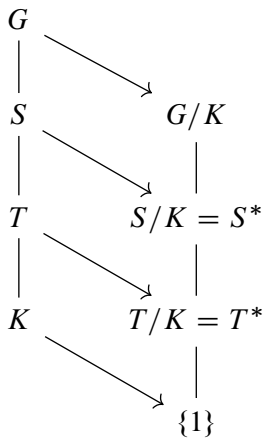
$$(G/K)/(H/K) \cong G/H$$

Theorem 2.70 (Correspondence Theorem). *If $K \triangleleft G, \pi : G \to G/K$ is the natural map, then*

$$S \mapsto \pi(S) = S/K$$

is a bijection between $Sub(G;K)$, the family of all those subgroups S of G that contain K, and $Sub(G/K)$, the family of all the subgroups of G/K. If we denote S/K by S^*, then

1. *$T \leq S \leq G$ if and only if $T^* \leq S^*$, in which case $[S:T] = [S^*:T^*]$*
2. *$T \triangleleft S$ if and only if $T^* \triangleleft S^*$, in which case $S/T \cong S^*/T^*$*



Proof. Use $\pi^{-1}\pi = 1$ and $\pi\pi^{-1} = 1$ to prove injectivity and surjectivity respectively.

For $[S : T] = [S^* : T^*]$, show there is a bijection between the family of all cosets of the form sT and the family of all the cosets of the form s^*T^*.

injective:

$$\begin{aligned}\pi(m)T^* = \pi(n)T^* &\Leftrightarrow \pi(m)\pi(n)^{-1} \in T^* \\ &\Leftrightarrow mn^{-1}K \in T/K \\ &\Rightarrow mn^{-1}t^{-1} \in K \\ &\Rightarrow mn^{-1} = tk \in T \\ &\Leftrightarrow mT = nT\end{aligned}$$

surjective:

If G is finite, then

$$\begin{aligned}[S^* : T^*] &= \left|S^*\right| / \left|T^*\right| \\ &= |S/K| / |T/K| \\ &= (|S| / |K|) / (|T| / |K|) \\ &= |S| / |T| \\ &= [S : T]\end{aligned}$$

If $T \triangleleft S$, by third isomorphism theorem, $T/S \cong (T/K)/(S/K) = T^*/S^*$

If $T^* \triangleleft S^*$,

$$\pi(sts^{-1}) \in \pi(s)T^*\pi(s)^{-1} = T^*$$

so that $sts^{-1} \in \pi^{-1}(T^*) = T$ □

Proposition 2.71. *If G is a finite abelian group and d is a divisor of $|G|$, then G contains a subgroup of order d*

Proof. Abelian group's subgroup is normal and hence we can build quotient groups. p90 for proof. Use the correspondence theorem □

Definition 2.72. If H and K are grops, then their **direct product**, denoted by $H \times K$, is the set of all ordered pairs (h, k) with the operation

$$(h, k)(h', k') = (hh', kk')$$

Proposition 2.73. *Let G and G' be groups and $K \triangleleft G$, $K' \triangleleft G'$. Then $K \times K' \triangleleft G \times G'$ and*

$$(G \times G')/(K \times K') \cong (G/K) \times (G'/K')$$

Proof. □

Proposition 2.74. *If G is a group containing normal subgroups H and K and $H \cap K = \{1\}$ and $HK = G$, then $G \cong H \times K$*

Proof. Note $|HK||H \cap K| = |H||K|$. Consider $\varphi : G \to H \times K$. Show it's homo and bijective. □

Theorem 2.75. *If m, n are relatively prime, then*

$$\mathbb{I}_{mn} \cong \mathbb{I}_m \times \mathbb{I}_n$$

Proof.

$$\begin{aligned} f :&\mathbb{Z} \to \mathbb{I}_m \times \mathbb{I}_n \\ &a \mapsto ([a]_m, [a]_n) \end{aligned}$$

is a homo. $\mathbb{Z}/\langle mn \rangle \cong \mathbb{I}_m \times \mathbb{I}_n$ □

Proposition 2.76. *Let G be a group, and $a, b \in G$ be commuting elements of orders m, n. If $(m, n) = 1$, then ab has order mn*

Corollary 2.77. *If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$*

Proof. Theorem 2.75 shows that $f : \mathbb{I}_{mn} \cong \mathbb{I}_m \times \mathbb{I}_n$. The result will follow if we prove that $f(U(\mathbb{I}_{mn})) = U(\mathbb{I}_m) \times U(\mathbb{I}_n)$, for then

$$\begin{aligned} \phi(mn) =& |U(\mathbb{I}_{mn})| = |f(U(\mathbb{I}_{mn}))| \\ =& |U(\mathbb{I}_m) \times U(\mathbb{I}_n)| = |U(\mathbb{I}_m)| \cdot |U(\mathbb{I}_n)| \end{aligned}$$

If $[a] \in U(\mathbb{I}_{mn})$, then $[a][b] = [1]$ for some $[b] \in \mathbb{I}_{mn}$ and

$$\begin{aligned} f([ab]) &= ([ab]_m, [ab]_n) = ([a]_m[b]_m, [a]_n[b]_n) \\ &= ([a]_m, [a]_n)([b]_m, [b]_n) = ([1]_m, [1]_n) \end{aligned}$$

Hence $f([a]) = ([a]_m, [a]_n) \in U(\mathbb{I}_m) \times U(\mathbb{I}_n)$

For the reverse inclusion, if $f([c]) = ([c]_m, [c]_n) \in U(\mathbb{I}_m) \times U(\mathbb{I}_n)$, then we must show that $[c] \in U(\mathbb{I}_{mn})$. There is $[d]_m \in \mathbb{I}_m$ with $[c]_m[d]_m = [1]_m$, and there is $[e]_n \mathbb{I}_n$ with $[c]_n[e]_n = [1]_n$. Since f is surjective, there is $b \in \mathbb{Z}$ with $([b]_m, [b]_n) = ([d]_m, [e]_n)$, so that

$$f([1]) = ([1]_m, [1]_n) = ([c]_m[b]_m, [c]_n[b]_n) = f([c][b])$$

Since f is an injection, $[1] = [c][b]$ and $[c] \in U(\mathbb{I}_{mn})$ □

Corollary 2.78. *1. If p is a prime, then $\phi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$*
2. If $n = p_1^{e_1} \dots p_t^{e_t}$, then

$$\phi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_t})$$

Lemma 2.79. *A cyclic group of order n has a unique subgroup of order d, for each divisor d of n, and this subgroup is cyclic.*

Define an equivalence relation on a group G by $x \equiv y$ if $\langle x \rangle = \langle y \rangle$. Denote the equivalence class containing x by $\text{gen}(C)$, where $C = \langle x \rangle$. Equivalence classes form a partition and we get

$$G = \prod_C \text{gen}(C)$$

where C ranges over all cyclic subgroups of G. Note $\big|\text{gen}(C)\big| = \phi(n)$

Theorem 2.80. *A group G of order n is cyclic if and only if for each divisor d of n, there is at most one cyclic subgroup of order d*

Theorem 2.81. *If G is an abelian group of order n having at most one cyclic subgroup of order p for each prime divisor p of n, then G is cyclic*

Exercise:

- 2.71 Suppose $H \leq G, |H| = |K|$. Since $|H| = [H : K]|K|$, $[H : K] = 1$. Hence $H = K$
- 2.67 1. $\text{Inn}(S_3) \cong S_3/Z(S_3) \cong S_3$ and $|\mathbf{Aut}(S_3)| \leq 6$. Hence $\mathbf{Aut}(S_3) = \text{Inn}(S_3)$

Exercise 2.5.1. Prove that if G is a group for which $G/Z(G)$ is cyclic, then G is abelian

Proof. Suppose $G/Z(G) = \langle a \rangle$, let $g = a^k z^{-1}, g' = a^{k'} z'^{-1}$, then $gg' = a^k z^{-1} z^{k'} z'^{-1} = a^{k+k'} z'^{-1} z^{-1} = g'g$. Hence G is abelian. □

2.6 Group Actions

Theorem 2.82 (Cayley)**.** *Every group G is isomorphic to a subgroup of the symmetric group S_G. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n*

Proof. For each $a \in G$, define $\tau_a(x) = ax$ for every $x \in G$. τ_a is a bijection for its inverse is $\tau_{a^{-1}}$

$$\tau_a \tau_{a^{-1}} = \tau_1 = \tau_{a^{-1}} \tau_a$$

□

Theorem 2.83 (Representation on Cosets)**.** *Let G be a group and $H \leq G$ having finite index n. Then there exists a homomorphism $\varphi : G \to S_n$ with* $\ker \varphi \leq H$

Proof. We still denote the family of all the cosets of H in G by G/H

For each $a \in G$, define "translation" $\tau_a : G/H \to G/H$ by $\tau_a(xH) = axH$ for every $x \in G$. For $a, b \in G$

$$(\tau_a \circ \tau_b)(xH) = a(bxH) = (ab)xH$$

so that

$$\tau_a \tau_b = \tau_{ab}$$

It follows that each τ_a is a bijection and so $\tau_a \in S_{G/H}$. Define $\varphi : G \to S_{G/H}$ by $\varphi(a) = \tau_a$. Rewriting

$$\varphi(a)\varphi(b) = \tau_a \tau_b = \tau_{ab} = \varphi(ab)$$

so that φ is a homomorphism. Finally if $a \in \ker \varphi$, then $\varphi(a) = 1_{G/H}$, so that $\tau_a(xH) = xH$, in particular, when $x = 1$, this gives $aH = H$ and $a \in H$. And $S_{G/H} \cong S_n$ □

When $H = \{1\}$, this is the Cayley theorem.
Four-group $\mathbf{V} = \{1, (12)(34), (13)(24), (14)(23)\}$

Proposition 2.84. *Every group G of order 4 is isomorphic to either $\mathbb{I}_4$ or the four-group $\boldsymbol{V}$. And $\mathbb{I}_4 \ncong \boldsymbol{V}$*

Proof. By lagrange's theorem, every element in G other than 1 has order 2 or 4. If 4, then G is cyclic.

Suppose $x, y \neq 1$, then $xy \neq x, y$. Hence $G = \{1, x, y, xy\}$. □

Proposition 2.85. *If G is a group of order 6, then G is isomorphic to either $\mathbb{I}_6$ or S_3. Moreover $\mathbb{I}_6 \ncong S_3$*

Proof. If G is not cyclic, since $|G|$ is even, it has some elements having order 2, say t by exercise 2.2.2

If G is abelian. Suppose it has another different element a with order 2. Then $H = \{1, a, t, at\}$ is a subgroup which contradict. Hence it must contain an element b of order 3. Then bt has order 6 and G is cyclic.

If G is not abelian. If G doesn't have elements of order 3, then it's abelian. Hence G has an element s of order 3.

Now $\left|\langle s\rangle\right| = 3$, so $[G : \langle s\rangle] = |G| / \left|\langle s\rangle\right| = 2$ and $\langle s\rangle$ is normal. Since $t = t^{-1}$, $tst \in \langle s\rangle$. If $tst = s^0 = 1$, $s = 1$. If $tst = s$, $\left|\langle st\rangle\right| = 6$. Therefore $tst = s^2 = s^{-1}$.

Let $H = \langle t\rangle$, $\varphi : G \to S_{G/\langle t\rangle}$ given by

$$\varphi(g) : x\langle t\rangle \mapsto gx\langle t\rangle$$

By representation on cosets, $\ker\varphi \leq \langle t\rangle$. Hence $\ker\varphi = \{1\}$ or $\ker\varphi = \langle t\rangle$. Since

$$\varphi(t) = \begin{pmatrix} \langle t\rangle & s\langle t\rangle & s^2\langle t\rangle \\ t\langle t\rangle & ts\langle t\rangle & ts^2\langle t\rangle \end{pmatrix}$$

If $\varphi(t)$ is the identity permutation, then $ts\langle t\rangle = s\langle t\rangle$, so that $s^{-1}ts \in \langle t\rangle = \{1, t\}$. But now $s^{-1}ts = t$. Therefore $t \notin \ker\varphi$ and $\ker\varphi = \{1\}$. Therefore φ is injective. Because $|G| = |S_3|$, $G \cong S_3$ □

Definition 2.86. If X is a set and G is a group, then G **acts** on X if there is a function $G \times X \to X$, denoted by $(g, x) \to gx$ s.t.

1. (gh)x=g(hx) for all $g, h \in G$ and $x \in X$
2. $1x = x$ for all $x \in X$

X is a G**-set** if G acts on X

If a group G acts on a set X, then fixing the first variable, say g, gives a function $\alpha_g : X \to X$, namely, $\alpha_g : x \mapsto gx$. This function is a permutation of X, for its inverse is $\alpha_{g^{-1}}$

$$\alpha_g\alpha_{g^{-1}} = 1 = \alpha_{g^{-1}}\alpha_g$$

If's easy to see that $\alpha : G \to S_X$ defined by $\alpha : g \mapsto \alpha_g$ is a homomorphism. Conversely, given any homomorphism $\varphi : G \to S_X$, define $gx = \varphi(g)(x)$. Thus an action of a group G on a set X is another way of viewing a homomorphism.

Definition 2.87. If G acts on X and $x \in X$, then the **orbit** of x, denoted by $\mathcal{O}(x)$, is the subset of X

$$\mathcal{O}(x) = \{gx : g \in G\} \subseteq X$$

the **stabilizer** of x, denoted by G_x, is the subgroup

$$G_x = \{g \in G : gx = x\} \leq G$$

Example 2.9.
1. Caylay's theorem says that G acts on itself by translation: $\tau_g : a \mapsto ga$. We say G acts **transitively** on X if there is only one orbit.
2. When G acts on G/H by translation $\tau_g : aH \mapsto gaH$, then the orbit $\mathcal{O}(aH) = G/H$
3. When a group G acts on itself by conjugation, then the orbit $\mathcal{O}(x)$ is

$$\{y \in G : y = axa^{-1} \text{ for some } a \in G\}$$

in this case, $\mathcal{O}(x)$ is called the **conjugacy class** of x, and it is commonly denoted by x^G.
centralizer $C_G(x) = \{g \in G : gxg^{-1} = x\}$
4. Let $X = \{1, 2, \ldots, n\}$, let $\alpha \in S_n$ and regard the cyclic group $G = \langle \alpha \rangle$ as acting on X. If $i \in X$, then

$$\mathcal{O}(i) = \{\alpha^k(i) : k \in \mathbb{Z}\}$$

Let the complete factorization of α be $\alpha = \beta_1 \ldots \beta_{t(\alpha)}$, and let $i = i_1$ be moved by α. If the cycle involving i_1 is $\beta_j = (i_1 i_2 \ldots i_r)$,

$$\mathcal{O}(i) = \{i_1, \ldots, i_r\}$$

where $i = i_1$. It follows that $|\mathcal{O}(i)| = r$. The stabilizer G_l of a number l is G if α fixes l

Normalizer

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

Proposition 2.88. *If G acts on a set X, then X is the disjoint union of the orbits. If X is finite, then*

$$|X| = \sum_i |\mathcal{O}(x_i)|$$

where x_i is chosen from each orbit

Proof. $x \equiv y \Leftrightarrow$ there exists $g \in G$ with $y = gx$ is an equivalence relation □

Theorem 2.89. *If G acts on a set X and $x \in X$ then*

$$|\mathcal{O}(x)| = [G : G_x]$$

Proof. Let G/G_x denote the family of cosets. Construct a bijection $\varphi : G/G_x \to \mathcal{O}(x)$ □

Corollary 2.90. *If a finite group G acts on a set X, then the number of elements in any orbit is a divisor of $|G|$.*

Corollary 2.91. *If x lies in a finite group G, then the number of conjugates of x is the index of its centralizer*

$$\left|x^G\right| = [G : C_G(x)]$$

and hence it's a divisor of G

Proof. x^G is the orbit, $C_G(x)$ is the stabilizer □

Proposition 2.92. *If H is a subgroup of a finite group G, then the number of conjugates of H in G is $[G : N_G(H)]$*

Proof. Similar to theorem 2.89 □

Theorem 2.93 (Cauchy)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p*

Proof. Prove by induction on $m \geq 1$, where $|G| = mp$. If $m = 1$, it's obvious.

If $x \in G$, then $\left|x^G\right| = [G : C_G(x)]$. If $x \notin Z(G)$, then x^G has more than one element, so $|C_G(x)| < |G|$. If $p \mid |C_G(x)|$, by inductive hypothesis, we are done. Else if $p \nmid |C_G(x)|$ for all noncentral x and $|G| = [G : C_G(x)]|C_G(x)|$, we have

$$p \mid [G : C_G(x)]$$

$Z(G)$ consists of all those elements with $\left|X^G\right| = 1$, we have

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

Hence $p \mid |Z(G)|$ and by proposition 2.71 □

Definition 2.94. The **class equation** of a finite group G is

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

where each x_i is selected from each conjugacy class having more than one element

Definition 2.95. If p is a prime, then a finite group G is called a **p-group** if $|G| = p^n$ for some $n \geq 0$

Theorem 2.96. *If p is a prime and G is a p-group, then $Z(G) \neq \{1\}$*

Proof. Consider

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

□

Corollary 2.97. *If p is a prime, then every group G of order p^2 is abelian*

Proof. If G is not abelian, then $Z(G)$ has order p. The center is always normal, and so $G/Z(G)$ is defined; it has order p and is cyclic by Lagrange's theorem. This contradicts Exercise 2.5.1 □

Example 2.10. Cauchy's theorem and Fermat's theorem are special cases of some common theorem.

If G is a finite group and p is a prime, define

$$X = \{(a_0, a_1, \ldots, a_{p-1}) \in G^p : a_0 a_1 \ldots a_{p-1} = 1\}$$

Note that $|X| = |G|^{p-1}$, for having chosen the last $p-1$ entries arbitrarily, the 0th entry must equal $(a_1 a_2 \ldots a_{p-1})^{-1}$. Introduce an action of $\mathbb{I}_p$ on X by defining, for $0 \leq i \leq p-1$,

$$[i](a_0, \ldots, a_{p-1}) = (a_{i+1}, \ldots, a_{p-1}, a_0, \ldots, a_i)$$

The product of the new p-tuple is a conjugate of $a_0 a_1 \ldots a_{p-1}$

$$a_{i+1} \ldots a_{p-1} a_0 \ldots a_i = (a_0 \ldots a_i)^{-1} (a_0 \ldots a_{p-1})(a_0 \ldots a_i)$$

This conjugate is 1 for $g^{-1} 1 g = 1$, and so $[i](a_0, \ldots, a_{p-1}) \in X$. By Corollary 2.90, the size of every orbit of X is a divisor of $\left|\mathbb{I}_p\right| = p$. Now orbits with just one element consists of a p-tuple all of whose entries a_i are equal, for all cyclic permutations of the p-tuple are the same. In other words, such an orbit corresponds to an element $a \in G$ with $a^p = 1$. Clearly $(1, 1, \ldots, 1)$ is such an orbit; if it were the only such , then we would have

$$|G|^{p-1} = |X| = 1 + kp$$

That is, $|G|^{p-1} \equiv 1 \mod p$. If p is a divisor of $|G|$, then we have a contradiction and thus proved Cauchy's theorem.

Proposition 2.98. *If G is a group of order $|G| = p^e$ then G has a normal subgroup of order p^k for every $k \leq e$*

Proof. We prove the result by induction on $e \geq 0$.

By Theorem 2.96, $Z(G) \neq \{1\}$. Let $Z \leq Z(G)$ be a subgroup of order p and Z is normal. If $k \leq e$, then $p^{k-1} \leq p^{e-1} = |G/Z|$. By induction, G/Z has a normal subgroup H^* of order p^{k-1}. The correspondence theorem says there is a subgroup H of G containing Z with $H^* = H/Z$; moreover $H^* \triangleleft G/Z$ implies $H \triangleleft G$. But$|H/Z| = p^{k-1}$ implies$|H| = p^k$ as desired. □

Definition 2.99. A group $G \neq \{1\}$ is called **simple** if G has no normal subgroups other than $\{1\}$ and G itself.

Proposition 2.100. *An abelian group G is simple if and only if it is finite and of prime order*

Proof. Assume G is simple. Since G is abelian, every subgroup is normal, and so G has no subgroups other than $\{1\}$ and G. Choose $x \in G$ with $x \neq 1$. Since $\langle x \rangle \leq G$, we have $\langle x \rangle = G$. If x has infinite order, then all the powers of x are distinct, and so $\langle x^2 \rangle < \langle x \rangle$ is a forbidden subgroup of $\langle x \rangle$, a contradiction. Therefore every $x \in G$ has finite order. If x has order m and if m is composite, say $m = kl$, then $\langle x^k \rangle$ is a proper subgroup of $\langle x \rangle$, a contradiction. Therefore $G = \langle x \rangle$ has prime order. □

Suppose that an element $x \in G$ has k conjugates, that is

$$\left|x^G\right| = \left|\{gxg^{-1} : g \in G\}\right| = k$$

If there is a subgroup $H \leq G$ with $x \in H \leq G$, how many conjugates does \$x \$ have in H?

Since

$$x^H = \{hxh^{-1} : h \in H\} \subseteq x^G$$

we have$\left|x^H\right| \leq \left|x^G\right|$. It is possible that there is a strict inequality$\left|x^H\right| < \left|x^G\right|$. For example, take $G = S_3, x = (1\ 2)$, and $H = \langle x \rangle$. Now let us consider this question, in particular, for $G = S_5, x = (1\ 2\ 3), H = A_5$

Lemma 2.101. *All 3-cycles are conjugate in A_5*

Proof. Let $G = S_5, \alpha = (1\ 2\ 3), H = A_5$. We know that$\left|\alpha^{S_5}\right| = 20$, for there are 20 3-cycles in S_5. Therefore, $20 = |S_5| / \left|C_{S_5}(\alpha)\right|$ by Corollary 2.91 , so that$\left|C_{S_5}(\alpha)\right| = 6$. Here they are

$$(1),\ (1\ 2\ 3),\ (1\ 3\ 2),\ (4\ 5),\ (4\ 5)(1\ 2\ 3),\ (4\ 5\ )(1\ 3\ 2)$$

The last there of these are odd permutations, so that $\left|C_{A_5}(\alpha)\right| = 3$. We conclude that

$$\left|\alpha^{A_5}\right| = |A_5| / \left|C_{A_5}(\alpha)\right| = 20$$

that is all 3-cycles are conjugate to α in A_5 □

Lemma 2.102. *If $n \geq 3$, every element in A_n is a 3-cycle or a product of 3-cycles*

Proof. Since each β equals $\tau_1 \dots \tau_{2q}$ □

Theorem 2.103. *A_5 is a simple group*

Proof. If $H \triangleleft A_5$ and $H \neq \{(1)\}$. Now if H contains a 3-cycle, then normality forces H to contain all its conjugates. Therefore it suffices to prove that H contains 3-cycle.

Since $\sigma \in H$, we may assume, after a harmless relabeling, that either $\sigma = (1\ 2\ 3), \sigma = (1\ 2)(3\ 4)$ or $\sigma = (1\ 2\ 3\ 4\ 5x)$

If $\sigma = (1\ 2)(3\ 4)$, define $\tau = (1\ 2)(3\ 5)$. Now $(3\ 5\ 4) = (\tau\sigma\tau^{-1})\sigma^{-1} \in H$. If $\sigma = (1\ 2\ 3\ 4\ 5)$, define $\rho = (1\ 3\ 2)$ and $(1\ 3\ 4) = \rho\sigma\rho^{-1}\sigma^{-1} \in H$ □

A_4 is not simple for $\mathbf{V} \triangleleft A_4$.

Lemma 2.104. *A_6 is a simple group*

Proof. Let $\{1\} \neq H \triangleleft A_6$; we must show that $H = A_6$. Assume that there is some $\alpha \in H$ with $\alpha \neq (1)$ that fixes some i, where $1 \leq i \leq 6$. Define

$$F = \{\sigma \in A_6 : \sigma(i) = i\}$$

Note that $\alpha \in H \cap F$, so that $H \cap F \neq \{(1)\}$. The second isomorphism theorem gives $H \cap F \triangleleft F$. But F is simple for $F \cong A_5$, we have $H \cap F = F$: that is $F \leq H$. It follows that H contains a 3-cycle, and so $H = A_6$ by Exercise 2.6.2.

If there is no $\alpha \in H$ with $\alpha \neq \{1\}$ that fixes some i with $1 \leq i \leq 6$. If we consider the cycle structures of permutations in A_6, however, any such α must have cycle structure (1 2)(3 4 5 6) or (1 2 3)(4 5 6). In the first case $\alpha^2 \in H, \alpha^2 \in H$ fixes 1. In the second case $\alpha(\beta\alpha^{-1}\beta^{-1})$ where $\beta = (2\ 3\ 4)$ fixes 1. □

Theorem 2.105. *A_n is a simple group for all $n \geq 5$*

Proof. If H is a nontrivial normal subgroup of A_n, then we must show that $H = A_n$. By Exercise 2.6.2 it suffices to prove that H contains a 3-cycle. If $\beta \in H$ is nontrivial, then there exists some i that β moves: say, $\beta(i) = j \neq i$. Choose a 3-cycle α that fixes i and moves j. The permutations α and β do not commute. It follows that $\gamma = (\alpha\beta\alpha^{-1})\beta^{-1}$ is a nontrivial element of H. But $\beta\alpha^{-1}\beta^{-1}$ is a 3-cycle, and so $\gamma = \alpha(\beta\alpha^{-1}\beta^{-1})$ is a product of two 3-cycles. Hence γ moves at most 6 symbols, say $i_1, \ldots, i_6$. Define

$$F = \{\sigma \in A_n : \sigma \text{ fixes all } i \neq i_1, \ldots, i_6\}$$

Now $F \cong A_6$ and $\gamma \in H \cap F$. Hence $H \cap F \lhd F$. But F is simple, and so $H \cap F = F$; that is $F \leq H$. Therefore H contains a 3-cycle □

Theorem 2.106 (Burnside's Lemma)**.** *Let G act on a finite set X. If N is the number of orbits, then*

$$N = \frac{1}{|G|} \sum_{\tau \in G} Fix(\tau)$$

where $Fix(\tau)$ is the number of $x \in X$ fixed by τ

Proof. List the elements of X as follows: Choose $x_1 \in X$ and then list all the elements $x_1, \ldots, x_r$ in the orbit $\mathcal{O}(x_1)$; then choose $x_{r+1} \notin \mathcal{O}(x_1)$, and so on until all the elements of X are listed. Now list the elements $\tau_1, \ldots, \tau_n$ of G and form the following array, where

$$f_{i,j} = \begin{cases} 1 & \text{if } \tau_i \text{ fixes } x_j \\ 0 & \text{if } \tau_i \text{ moves } x_j \end{cases}$$

	x_1	x_2	$\ldots$	x_{r+1}	x_{r+2}	$\ldots$
τ_1	$f_{1,1}$	$f_{1,2}$	$\ldots$	$f_{1,r+1}$	$f_{1,r+2}$	$\ldots$
$\vdots$						
τ_n	$f_{n,1}$	$f_{n,2}$	$\ldots$	$f_{n,r+1}$	$f_{n,r+2}$	$\ldots$

Now $Fix(\tau_i)$ is the number of 1's in the ith row. therefore $\sum_{\tau \in G} Fix(\tau)$ is the total number of 1's in the array. The number of 1's in column 1 is $\left|G_{x_1}\right|$. By Exercise 2.6.3 $\left|G_{x_1}\right| = \left|G_{x_2}\right|$. By Theorem 2.89 the number of 1's in the r columns labels by the $x_i \in \mathcal{O}(x_i)$ is thus

$$r\left|G_{x_1}\right| = |\mathcal{O}(x_1)| \cdot \left|G_{x_1}\right| = \left(|G| / \left|G_{x_1}\right|\right)\left|G_{x_1}\right| = |G|$$

Therefore

$$\sum_{\tau \in G} Fix(\tau) = N|G|$$

□

We are going to use Burnside's lemma to solve problems of the following sort. How many striped flags are there having six stripes each of which can be colored red, white or blue?

r	w	b	r	w	b

b	w	r	b	w	r

Let X be the set of all 6-tuples of colors: if $x \in X$, then

$$x = (c_1, c_2, c_3, c_4, c_5, c_6)$$

Let τ be the permutation that reserves all the indices:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 6)(2\ 5)(3\ 4)$$

(thus τ turns over each 6-tuple x of colored stripes). The cyclic group $G = \langle \tau \rangle$ acts on X; since$|G| = 2$, the orbit of any 6-tuple x consists of either 1 or 2 elements. Since a flag is unchanged by turning it over, it is reasonable to identify a flag with an orbit of 6-tuple. For example, the orbit consisting of the 6-tuples

$$(r, w, b, r, w, b) \text{ and } (b, w, r, b, w, r)$$

above. The number of flags is thus the number N of orbits; by Burnside's lemma, $N = \frac{1}{2}[Fix((1)) + Fix(\tau)]$. The identity permutation (1) fixes every $x \in X$, and so $Fix((1)) = 3^6$. Now τ fixes a 6-tuple x if it's a "palindrome". It follows that $Fix(x) = 3^3$. The number of flags is thus

$$N = \frac{1}{2}(3^6 + 3^3) = 378$$

Definition 2.107. If a group G acts on $X = \{1, \ldots, n\}$ and if $\mathcal{C}$ is a set of q colors, then G acts on the set $\mathcal{C}^n$ of all n-tuples of colors by

$$\tau(c_1, \ldots, c_n) = (c_{\tau 1}, \ldots, c_{\tau n}) \text{ for all } \tau \in G$$

An orbit of $(c_1, \ldots, c_n) \in \mathcal{C}^n$ is called a (q, G)**-coloring** of X.

Example 2.11. Color each square in a 4×4 grid red or black.

If X consists of the 16 squares in the grid and if $\mathcal{C}$ consists of the two colors red and black, then the cyclic group $G = \langle R \rangle$ or order 4 acts on X, where R is a clockwise rotation by 90°;

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

13	9	5	1
14	10	6	2
15	11	7	3
16	12	8	4

Figure shows how R acts: the right square is R)'s action on the left square. In cycle notation

$$R = (1,\ 4,\ 16,\ 13)(2,\ 8,\ 15,\ 9)(3,\ 12,\ 14,\ 5)(6,\ 7,\ 11,\ 10)$$
$$R^2 = (1,\ 16)(4,\ 13)(2,\ 15)(8,\ 9)(3,\ 14)(12,\ 5)(6,\ 11)(7,\ 10)$$
$$R^3 = (1,\ 13,\ 16,\ 4)(2,\ 9,\ 15,\ 8)(3,\ 5,\ 14,\ 12)(6,\ 10,\ 11,\ 7)$$

By Burnside's lemma, the number of chessboards is

$$\frac{1}{4}[Fix((1)) + Fix(R) + Fix(R^2) + Fix(R^3)]$$

Exercise 2.6.1. Prove that if p is a prime and G is a finite group in which every element has order a power of p, then G is a p-group. (A possibly infinite group G) is called a **p-group** if every element in G has order a power of p

Proof. By Cauchy's theorem 2.93 □

Exercise 2.6.2.
1. For all $n \geq 5$, prove that all 3-cycles are conjugate in A_n
2. Prove that if a normal subgroup $H \triangleleft A_n$ contains a 3-cycle, where $n \geq 5$, then $H = A_n$

Proof.
1. If (1 2 3) and $(i\ j\ k)$ are not disjoint. As Example 2.1 illustrated, $\alpha \in S_5$
   If they are disjoint, simple
2. By lemma 2.102

□

Exercise 2.6.3.
1. Let a group G act on a set X, and suppose that $x, y \in X$ lie in the same orbit: y=gx for some $g \in G$. Prove that $G_y = gG_xg^{-1}$
2. Let G be a finite group acting on a set X; prove that if $$x,y$\in$ X lie in the same orbit, then$|G_x| = \left|G_y\right|$

Proof.
1. If $f \in G_x$, then $gfg^{-1}(y) = gfg^{-1}gx = gx = y$
2. There is a bijection.

□

3 Commutative Rings I

3.1 First Properties

Definition 3.1. A **commutative ring** R is a set with two binary operations, addition and multiplication s.t.

1. R is an abelian group under addition
2. (**commutativity**) $ab = ba$ for all $a, b \in R$
3. (**associativity**) $a(bc) = (ab)c$ for every $a, b, c \in R$
4. there is an element $1 \in R$ with $1a = a$ for every $a \in R$
5. (**distributivity**) $a(b + c) = ab + ac$ for every $a, b, c \in R$

The element 1 in a ring R has several names: it is called **one**, the **unit** of R, or the **identity** in R

Example 3.1.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are commutative rings with the usual addition and multiplication
2. Consider the set R of all real numbers x of the form

$$x = a + b\omega$$

where $a, b \in \mathbb{Q}$ and $\omega = \sqrt[3]{2}$. R is closed under ordinary addition. However, if R is closed under multiplication, then $\omega^2 \in R$ and there are rationals a and b with

$$\begin{aligned} \omega^2 &= a + b\omega \\ 2 &= a\omega + b\omega^2 \\ b\omega^2 &= ab + b^2\omega \end{aligned}$$

Hence $2 - a\omega = ab + b^2\omega$ and so

$$2 - ab = (b^2 + a)\omega$$

A contradiction.

Proposition 3.2. *Let R be a commutative ring.*

1. $0 \cdot a = 0$ *for every* $a \in R$
2. *If* $1 = 0$ *then R consists of the single element 0. In this case R is called the* ***zero ring***
3. *If $-a$ is the additive inverse of a, then* $(-1)(-a) = a$
4. $(-1)a = -a$ *for every* $a \in R$
5. *If* $n \in \mathbb{N}$ *and* $n1 = 0$, *then* $na = 0$ *for all* $a \in R$

6. *The binomial theorem holds: if $a, b \in R$, then*

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

Proof. 6. $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$ □

Definition 3.3. A subset S of a commutative ring R is a **subring** of R if
1. $1 \in S$
2. if $a, b \in S$ then $a - b \in S$
3. if $a, b \in S$, then $ab \in S$

Notation. The tradition in ring theory is to write $S \subseteq R$ for a subring

Proposition 3.4. *A subring S of a commutative ring R is itself a commutative ring.*

Definition 3.5. A **domain** (often called an **integral domain**) is a commutative ring R that satisfies two extra axioms: first

$$1 \neq 0$$

second, the **cancellation law** for multiplication: for all $a, b, c \in R$

$$\text{if } ca = cb \text{ and } c \neq 0, \text{ then } a = b$$

Proposition 3.6. *A nonzero commutative ring R is a domain if and only if the product of any two nonzero elements of R is nonzero*

Proof. $ab = ac$ if and only if $a(b-c) = 0$ □

Proposition 3.7. *The commutative ring $\mathbb{I}_m$ is a domain if and only if m is a prime*

Proof. If $m = ab$, where $1 < a, b < m$, then $[a], [b] \neq [0]$ yet $[a][b] = [m] = [0]$
Conversely, if m is a prime and $[a][b] = [ab] = [0]$, then $m \mid ab$ □

Example 3.2. 1. Let $\mathcal{F}(\mathbb{R})$ be the set of all the function $\mathbb{R} \to \mathbb{R}$ equipped with the operations of **point-wise addition** and **point-wise multiplication**: Given $f, g \in \mathcal{F}(\mathbb{R})$, define functions $f + g$ and fg by

$$f + g : a \mapsto f(a) + f(b) \quad \text{and} \quad fg : a \mapsto f(a)g(a)$$

We claim that $\mathcal{F}(\mathbb{R})$ with these operations is a commutative ring. The zero element is the constant function z with value 0. $\mathcal{F}(\mathbb{R})$ is not a domain by

$$f(a) = \begin{cases} a & \text{if } a \leq 0 \\ 0 & \end{cases} \quad g(a) = \begin{cases} 0 & \text{if } a \leq 0 \\ a & \end{cases}$$

Definition 3.8. Let a and b be elements of a commutative ring R. Then a **divides** b **in** R (or a is a **divisor** of b or b is a **multiple** of a), denoted by $a \mid b$, if there exists an element $c \in R$ with $b = ca$

Definition 3.9. An element u in a commutative ring R is called a **unit** if $u \mid 1$ in R.

Proposition 3.10. *Let R be a domain, and let $a, b \in R$ be nonzero. Then $a \mid b$ and $b \mid a$ if and only if $b = ua$ for some unit $u \in R$*

Proposition 3.11. *If a is an integer, then $[a]$ is a unit in $\mathbb{I}_m$ if and only if a and m are relatively prime.*

Corollary 3.12. *If p is a prime, then every nonzero $[a]$ in $\mathbb{I}_p$ is a unit.*

Definition 3.13. If R is a commutative ring, then the **group of units** of R is

$$U(R) = \{\text{all units in } R\}$$

Definition 3.14. A **field** F is a commutative ring in which $1 \neq 0$ and every nonzero element a is a unit; that is, there is $a^{-1} \in F$ with $a^{-1}a = 1$

A commutative ring R is a field if and only if $U(R) = R^{\times}$, the nonzero elements of R.

Proposition 3.15. *Every field F is a domain*

Proof. $ab = ac, b = a^{-1}ab = a^{-1}(ac) = c$ □

Proposition 3.16. *The commutative ring $\mathbb{I}_m$ is a field if and only if m is prime*

Theorem 3.17. *If R is a domain then there is a field F containing R as a subring. Moreover, F can be chosen so that for each $f \in F$, there are $a, b \in R$ with $b \neq 0$ and $f = ab^{-1}$*

Proof. Let $X = \{(a,b) \in R \times R : b \neq 0\}$ and define a relation $\equiv$ on X by $(a,b) \equiv (c,d)$ if $ad = bc$. We claim that $\equiv$ is an equivalence relation. If $(a,b) \equiv (c,d)$ and $(c,d) \equiv (e,f)$, then $ad = bc, cf = de$ and $adf = b(cf) = bde$, gives $af = be$

Denote the equivalence class of (a,b) by $[a,b]$, define F as the set of all equivalence classes $[a,b]$ and equip F with the following addition and multiplication

$$[a,b] + [c,d] = [ad + bc, bd]$$
$$[a,b][c,d] = [ac, bd]$$

Show addition and multiplication are well-defined. □

Definition 3.18. The field F constructed from R in Theorem 3.17 is called the **fraction field** of R, denoted by Frac(R), and we denote $[a,b] \in \text{Frac}(R)$ by a/b

Note that $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$

3.2 Polynomials

Definition 3.19. If R is a commutative ring, then a **sequence** σ in R is

$$\sigma = (s_0, s_1, \ldots, s_i, \ldots)$$

the entries $s_i \in R$ for all $i \geq 0$ are called the **coefficients** of σ

Definition 3.20. A sequence $\sigma = (s_0, \ldots, s_i, \ldots)$ in a commutative ring R is called a **polynomial** if there is some integer $m \geq 0$ with $s_i = 0$ for all $i > m$; that is

$$\sigma = (s_0, \ldots, s_m, 0, \ldots)$$

A polynomial has only finitely many nonzero coefficients. The **zero polynomial**, denoted by $\sigma = 0$

Definition 3.21. If $\sigma(s_0, \ldots, s_n, 0, \ldots) \neq 0$ is a polynomial, we call s_n the **leading coefficient** of σ, we call n the **degree** of σ, an we denote n by $\deg(\sigma)$

Notation. If R is a commutative ring, then the set of all polynomials with coefficients in R is denoted by $R[x]$

Proposition 3.22. *If R is a commutative ring, then $R[x]$ is a commutative ring that contains R as a subring*

Proof. $\sigma = (s_0, s_1, \dots), \tau = (t_0, t_1, \dots)$

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, \dots)$$
$$\sigma\tau = (c_0, c_1, \dots)$$

where $c_k = \sum_{i+j=k} s_i t_j = \sum_{i=0}^{k} s_i t_{k-i}$. □

Lemma 3.23. *Let R be a commutative ring and let $\sigma, \tau \in R[x]$ be nonzero polynomials.*

1. *Either $\sigma\tau = 0$ or $deg(\sigma\tau) \leq deg(\sigma) + deg(\tau)$*
2. *If R is a domain, then $\sigma\tau \neq 0$ and*

$$deg(\sigma\tau) = deg(\sigma) + deg(\tau)$$

3. *If R is a domain, then $R[x]$ is a domain*

Proof. $\sigma = (s_0, s_1, \dots), \tau = (t_0, t_1, \dots)$ have degrees m and n respectively.

1. if $k > m + n$, then each term in $\sum_i s_i t_{k-i}$ is 0
2. Each term in $\sum_i s_i t_{m+n-i}$ is 0 with the possible exception of $s_m t_n$. Since R is a domain, $s_m \neq 0$ and $t_n \neq 0$ imply $s_m t_n \neq 0$.

□

Definition 3.24. If R is a commutative ring, then $R[x]$ is called the **ring of polynomials over** R

Definition 3.25. Define the element $x \in R[x]$ by

$$x = (0, 1, 0, 0, \dots)$$

Lemma 3.26. 1. *IF $\sigma = (s_0, \dots)$, then*

$$x\sigma = (0, s_0, s_1, \dots)$$

2. *If $n \geq 1$, then x^n is the polynomial having 0 everywhere except for 1 in the nth coordinate*
3. *If $r \in R$, then*

$$(r, 0, \dots)(s_0, s_1, \dots, s_j, \dots) = (rs_0, rs_1, \dots, rs_j, \dots)$$

Proposition 3.27. *If $\sigma = (s_0, \dots, s_n, 0, \dots)$, then*

$$\sigma = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n$$

where each element $s \in R$ is identified with the polynomial $(s, 0, \dots)$

As a customary, we shall write

$$f(x) = s_0 + s_1 x + \cdots + s_n x^n$$

instead of σ. s_0 is called its **constant term**. If $s_n = 1$, then $f(x)$ is called **monic**.

Corollary 3.28. *Polynomials $f(x) = s_0 + \cdots + s_n x^n$ and $g(x) = t_0 + \cdots + t_m x^m$ are equal if and only if $n = m$ and $s_i = t_i$ for all i.*

If R is a commutative ring, each polynomial $f(x) = s_0 + \cdots + s_n x^n$ defines a **polynomial function** $f : R \to R$ by evaluation: If $a \in R$, define $f(a) = s_0 + \cdots + s_n a^n \in R$.

Definition 3.29. Let k be a field. The fraction field of $k[x]$, denoted by $k(x)$, is called the **field of rational function** over k

Proposition 3.30. *If k is a field, then the elements of $k(x)$ have the form $f(x)/g(x)$ where $f(x), g(x) \in k[x]$ and $g(x) \neq 0$*

Proposition 3.31. *If p is a prime, then the field of rational functions $\mathbb{I}_p(x)$ is a n infinite field containing $\mathbb{I}_p$ as a subfield.*

Proof. By Lemma 3.23 (3), $\mathbb{I}_p[x]$ is an infinite domain for the powers x^n for $n \in \mathbb{N}$ are distinct. Thus its fraction filed $\mathbb{I}_p(x)$ is an infinite field containing $\mathbb{I}_p[x]$ as a subring. But $\mathbb{I}_p[x]$ contains $\mathbb{I}_p$ as a subring, by Proposition 3.22. □

$R[x]$ is often called the ring of all **polynomials over R in one variable**. If we write $A = R[x]$, then $A[y]$ is called the ring of all **polynomials over R in two variables x and y**, and it is denoted by $R[x, y]$.

Exercise 3.2.1. Show that if R is a commutative ring, then $R[x]$ is never a field

Proof. If $R[x]$ is a field, then $x^{-1} \in R[x]$ and $x^{-1} = \sum_i c_i x^i$. However

$$\deg(x x^{-1}) = \deg(1) = 1 = \deg(x) + \deg(x^{-1})$$

A contradiction. □

Exercise 3.2.2. Show that the polynomial function defined by $f(x) = x^p - x \in \mathbb{I}_p[x]$ is identically zero.

Proof. By Fermat's theorem 2.48, $a^p \equiv a \mod p$ □

Exercise 3.2.3. If R is a commutative ring and $f(x) = \sum_{i=0}^{n} s_i x^i \in R[x]$ has degree $n \geq 1$, define its **derivative** $f'(x) \in R[x]$ by

$$f'(x) = s_1 + 2s_2x + 3s_3x^2 + \cdots + ns_nx^{n-1}$$

if $f(x)$ is a constant polynomial, define its derivative to be the zero polynomial. Prove that the usual rules of calculus hold:

$$\begin{aligned}(f+g)' &= f' + g' \\ (rf)' &= r(f)' \quad \text{if } r \in R \\ (fg)' &= fg' + f'g \\ (f^n)' &= nf^{n-1}f' \quad \text{for all } n \geq 1\end{aligned}$$

Exercise 3.2.4. Let R be a commutative ring and let $f(x) \in R[x]$

1. Prove that if $(x-a)^2 \mid f(x)$, then $x - a \mid f'(x)$ in $R[x]$
2. Prove that if $x - a \mid f(x)$ and $x - a \mid f'(x)$, then $(x-a)^2 \mid f(x)$

3.3 Greatest Common Divisors

Theorem 3.32 (Division Algorithm)**.** *Assume that k is a field and that $f(x), g(x) \in k[x]$ with $f(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in k[x]$ with*

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

and either $r(x) = 0$ or $deg(r) < deg(f)$

Proof. We first prove the existence of such q and r. If $f \mid g$, then $g = qf$ for some q; define the remainder $r = 0$. If $f \nmid g$, then consider all polynomials of the form $g - qf$ as q varies over $k[x]$. The least integer axiom provides a polynomial $r = g - qf$ having least degree among all such polynomials. Since $g = qf + r$, it suffices to show that $\deg(r) < \deg(f)$. Write $f(x) = s_nx^n + \cdots + s_1x + s_0$ and $r(x) = t^m x^m + \ldots t_0$. Now $s_n \neq 0$ implies that s_n is a unit because k is a field and so $s_n^{-1} \in k$. If $\deg(r) \geq \deg(f)$, define

$$h(x) = r(x) - t_m s_n^{-1} x^{m-n} f(x)$$

that is, if $\mathrm{LT}(f) = s_nx^n$, where LT abbreviates **leading term**, then

$$h = r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f$$

note that $h = 0$ or $\deg(h) < \deg(r)$. If $h = 0$, then $r = [\mathrm{LT}(r)/\mathrm{LT}(f)]f$ and

$$\begin{aligned} g = qf + r &= qf + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f \\ &= \left[q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} \right] f \end{aligned}$$

contradicting $f \nmid g$. If $h \neq 0$, then $\deg(h) < \deg(r)$ and

$$g - qf = r = h + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f$$

Thus $g - [q + \mathrm{LT}(r)/\mathrm{LT}(f)]f = h$, contradicting r being a polynomial of least degree having this form. Therefore $\deg(r) < \deg(f)$

To prove uniqueness of $q(x)$ and $r(x)$ assume that $g = q'f + r'$, where $\deg(r') < \deg(f)$. Then

$$(q - q')f = r' - r$$

If $r' \neq r$, then each side has a degree. But $\deg((q - q')f) = \deg(q - q') + \deg(f) \geq \deg(f)$, while $\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(f)$, a contradiction. Hence $r' = r$ and $(q - q')f = 0$. As $k[x]$ is a domain and $f \neq 0$, it follows that $q - q' = 0$ and $q = q'$ □

Definition 3.33. If $f(x)$ and $g(x)$ are polynomials in $k[x]$, where k is a field, then the polynomials $q(x)$ and $r(x)$ occurring in the division algorithm are called the **quotient** and the **remainder** after dividing $g(x)$ by $f(x)$

The hypothesis that k is a filed is much too strong: long division can be carried out in $R[x]$ for every commutative ring R as long as the leading coefficient of $f(x)$ is a unit in R; in particular, long division is always possible when $f(x)$ is monic.

Corollary 3.34. *Let R be a commutative ring and let $f(x) \in R[x]$ be a monic polynomial. If $g(x) \in R[x]$, then there exists $q(x), r(x) \in R[x]$ with*

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

where either $r(x) = 0$ or $deg(r) < deg(f)$

Proof. Note that $\mathrm{LT}(r)/\mathrm{LT}(f) \in R$ because $f(x)$ is monic □

Definition 3.35. If $f(x) \in k[x]$, where k is a field, then a **root** of $f(x)$ **in** k is an element $a \in k$ with $f(a) = 0$

Lemma 3.36. *Let $f(x) \in k[x]$, where k is a field, and let $u \in k$. Then there is $q(x) \in k[x]$ with*

$$f(x) = q(x)(x-u) + f(u)$$

Proof. The division algorithm gives

$$f(x) = q(x)(x-u) + r$$

Now evaluate

$$f(u) = q(u)(u-u) + r$$

and so $r = f(u)$ □

Proposition 3.37. *If $f(x) \in k[x]$, where k is a field, then a is a root of $f(x)$ in k if and only if $x-a$ divides $f(x)$ in $k[x]$*

Proof. If a is a root of $f(x)$ in k, then $f(a) = 0$ and the lemma gives $f(x) = q(x)(x-a)$. □

Theorem 3.38. *Let k be a field and let $f(x) \in k[x]$. If $f(x)$ has degree n, then $f(x)$ has at most n roots in k*

Proof. We prove the statement by induction on $n \geq 0$. If $n = 0$, then $f(x)$ is a nonzero constant, and so the number of its roots in k is zero. Now let $n > 0$. If $f(x)$ has no roots in k, then we are done. Otherwise we may assume that there is $a \in k$ with a a root of $f(x)$; hence by Proposition 3.37

$$f(x) = q(x)(x-a)$$

moreover, $q(x) \in k[x]$ has degree $n-1$. □

Example 3.3. Theorem 3.38 is not true for polynomials with coefficients in an arbitrary commutative ring R. For example, if $R = \mathbb{I}_8$, then the quadratic polynomial $x^2 - 1$ has 4 roots: [1], [3], [5], [7]

Corollary 3.39. *Every nth root of unity in $\mathbb{C}$ is equal to*

$$e^{2\pi ik/n} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$$

where $k = 0, 1, \ldots, n-1$

Corollary 3.40. *Let k be an infinite field and let $f(x)$ and $g(x)$ be polynomials in $k[x]$. If $f(x)$ and $g(x)$ determine the same polynomial function, then $f(x) = g(x)$*

Proof. If $f(x) \neq g(x)$, then the polynomial $h(x) = f(x) - g(x)$ is nonzero, so that it has some degree, say n. Now every element of k is a root of $h(x)$; since k is infinite, $h(x)$ has more than n roots, a contradiction. □

Theorem 3.41. *If k is a field and G is a finite subgroup of the multiplicative group $k^\times$., then G is cyclic. In particular, if k itself is finite, then $k^\times$ is cyclic.*

Proof. Let d be a divisor of $|G|$. If there are two subgroups of G of order d, say S and T, then $|S \cup T| > d$. But each $a \in S \cup T$ satisfies $a^d = 1$ and hence it's a root of $x^d - 1$, a contradiction. Thus G is cyclic, by Theorem 2.80. □

Definition 3.42. If k is a finite field, a generator of the cyclic group $k^\times$ is called a **primitive element** of k

Definition 3.43. If $f(x)$ and $g(x)$ are polynomials in $k[x]$, where k is a field, then a **common divisor** is a polynomial $c(x) \in k[x]$ with $c(x) \mid f(x)$ and $c(x) \mid g(x)$. If $f(x)$ and $g(x)$ in $k[x]$ are not both 0, define their **greatest common divisor**, abbreviated gcd, to be the monic common divisor having largest degree. If $f(x) = 0 = g(x)$, define their gcd $= 0$. The gcd of $f(x)$ and $g(x)$ is often denoted by (f, g)

Theorem 3.44. *If k is a field and $f(x), g(x) \in k[x]$, then their* gcd $d(x)$ *is a nonlinear combination of $f(x)$ and $g(x)$; that is there are $s(x), t(x) \in k[x]$ with*

$$d(x) = s(x)f(x) + t(x)g(x)$$

Corollary 3.45. *Let k be a field and let $f(x), g(x) \in k[x]$. A monic common divisor $d(x)$ is the gcd if and only if $d(x)$ is divisible by every common divisor*

Definition 3.46. An element p in a domain R is **irreducible** if p is neither 0 nor a unit and in any factorization $p = uv$ in R, either u or v is a unit. Elements $a, b \in R$ are **associates** if there is a unit $u \in R$ with $b = ua$

For example, a prime p is irreducible in $\mathbb{Z}$

Proposition 3.47. *If k is a field, then a polynomial $p(x) \in k[x]$ is irreducible if and only if $deg(p) = n \geq 1$ and there is no factorization in $k[x]$ of the form $p(x) = g(x)h(x)$ in which both factors have degree smaller than n*

Proof. We show fist that $h(x) \in k[x]$ is a unit if and only if $\deg(h) = 0$. If $h(x)u(x) = 1$, then $\deg(h) + \deg(u) = \deg(1) = 0$, we have $\deg(h) = 0$. Conversely if $\deg(h) = 0$, then $h(x)$ is a nonzero constant; that is, $h \in k$; since k is a field, h has an inverse

If $p(x)$ is irreducible, then its only factorization are of the form $p(x) = g(x)h(x)$ where $g(x)$ or $h(x)$ is a unit; that is, either $\deg(g) = 0$ or $\deg(h) = 0$.

Conversely, if $p(x)$ is reducible, then it has factorization $p(x) = g(x)h(x)$ where neither $g(x)$ nor $h(x)$ is a unit; □

Corollary 3.48. *Let k be a field and let $f(x) \in k[x]$ be a quadratic or cubic polynomial. Then $f(x)$ is irreducible in $k[x]$ if and only if $f(x)$ does not have a root in k*

Proof. If $f(x) = g(x)h(x)$, then $\deg(f) = \deg(g) + \deg(h)$ □

Example 3.4. 1. We determine the irreducible polynomials in $\mathbb{I}_2[x]$ of small degree.

As always, the linear polynomials x and $x + 1$ are irreducible

There are four quadratics: $x^2, x^2 + x, x^2 + 1, x^2 + x + 1$. Since each of the first three has a root in $\mathbb{I}_2$, there is only one irreducible quadratic

There are eight cubics, of which four are reducible because their constant term is 0. The remaining polynomials are

$$x^3 + 1; \quad x^3 + x + 1; \quad x^3 + x^2 + 1; \quad x^3 + x^2 + x + 1$$

Since 1 is a root of the first and fourth, the middle two are the only irreducible cubics.

Lemma 3.49. *Let k be a field, let $p(x), f(x) \in k[x]$, and let $d(x) = (p, f)$. If $p(x)$ is a monic irreducible polynomial, then*

$$d(x) = \begin{cases} 1 & \text{if } p(x) \nmid f(x) \\ p(x) & \text{if } p(x) \mid f(x) \end{cases}$$

Theorem 3.50 (Euclid's Lemma)**.** *Let k be a field and let $f(x), g(x) \in k[x]$. If $p(x)$ is an irreducible polynomial in $k[x]$, and $p(x) \mid f(x)g(x)$, then either*

$$p(x) \mid f(x) \quad \text{or} \quad p(x) \mid g(x)$$

More generally, if $p(x) \mid f_1(x) \dots f_n(x))$, then $p(x) \mid f_i(x)$ for some i

Proof. Assume $p \mid fg$ but that $p \nmid f$. Since p is irreducible, $(p, f) = 1$, and so $1 = sp + tf$ for some polynomials s and t. Therefore

$$g = spg + tfg$$

and so $p \mid g$ □

Definition 3.51. Two polynomials $f(x), g(x) \in k[x]$ where k is a field, are called **relatively prime** if their gcd is 1

Corollary 3.52. *Let $f(x), g(x), h(x) \in k[x]$, where k is a field and let $h(x)$ and $f(x)$ be relatively prime. If $h(x) \mid f(x)g(x)$, then $h(x) \mid g(x)$*

Definition 3.53. If k is a field, then a rational function $f(x)/g(x) \in k(x)$ is in **lowest terms** if $f(x)$ and $g(x)$ are relatively prime

Proposition 3.54. *If k is a field, every nonzero $f(x)/g(x) \in k(x)$ can be put in lowest terms*

Theorem 3.55 (Euclidean Algorithm)**.** *If k is a field and $f(x), g(x) \in k[x]$, then there are algorithms for computing* $\gcd(f, g)$ *as well as for finding a pair of polynomials $s(x)$ and $t(x)$ with*

$$(f, g) = s(x)f(x) + t(x)g(x)$$

Proof.

$$\begin{aligned}
g &= q_1 f + r_1 \\
f &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2} \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

Since the degrees of the remainders are strictly decreasing, this procedure must stop after a finite number of steps. The claim is that $d = r_n$ is the gcd.

If c is any common divisor of f and g, then $c \mid r_i$ for every i. Also

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= (1 + q_{n-1})r_{n-2} - q_n r_{n-3} \\ &= (1 + q_{n-1})(r_{n-4} - q_{n-2}r_{n-3}) - q_n r_{n-3} \\ &= (1 + q_{n-1})r_{n-4} - [(1 + q_{n-1})q_{n-2} + q_n]r_{n-3} \\ &\vdots \\ &= sf + tg \end{aligned}$$

□

Corollary 3.56. *Let k be a subfield of a field K, so that $k[x]$ is a subring of $K[x]$. If $f(x), g(x) \in k[x]$, then their gcd in $k[x]$ is equal to their gcd in $K[x]$*

Proof. The division algorithm in $K[x]$ gives

$$g(x) = Q(x)f(x) + R(x)$$

$k[x]$ gives

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

and this also holds in $K[x]$. So that uniqueness of quotient and remainder gives $Q(x) = q(x), R(x) = r(x)$. □

Theorem 3.57 (Unique Factorization)**.** *If k is a field, then every polynomial $f(x) \in k[x]$ of degree ≥ 1 is a product of a nonzero constant and monic irreducibles. Moreover, if $f(x)$ has two such factorizations*

$$f(x) = ap_1(x)\dots p_m(x) \quad \text{and} \quad f(x) = bq_1(x)\dots q_n(x)$$

then $a = b, m = n$ and the q's may be reindexed so that $q_i = p_i$ for all i

Proof. We prove the existence of a factorization for a polynomial $f(x)$ by induction on $\deg(f) \geq 1$. If $\deg(f) = 1 =$, then $f(x) = ax + c = a(x + a^{-1}c)$. As every linear polynomial, $x + a^{-1}c$ is irreducible.

Assume now that $\deg(f) \geq 1$. If $f(x)$ is irreducible and its leading coefficient is a, write $f(x) = a(a^{-1}f(x))$; we are done. If $f(x)$ is not irreducible, then $f(x) = g(x)h(x)$, where $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$. By the inductive hypothesis, $g(x) = bp_1(x)\dots p_m(x)$ and $h(x) = cq_1(x)\dots q_n(x)$. It follows that

$$f(x) = (bc)p_1(x)\dots p_m(x)q_x(x)\dots q_n(x)$$

We now prove by induction on $M = \max\{m, n\} \geq 1$ if there is an equation

$$ap_1(x) \dots p_m(x) = bq_1(x) \dots q_n(x)$$

where a and b are nonzero constants and the p's and q's are monic irreducibles. For the inductive step, $p_m(x) \mid q_1(x) \dots q_n(x)$. By Euclid's lemma, there is i with $p_m(x) \mid q_i(x)$. But $q_i(x)$ are monic irreducible, so that $q_i(x) = p_m(x)$. Canceling this factor we will use inductive hypothesis □

Let k be a field and assume that there are $a, r_1, \dots, r_n \in k$ with

$$f(x) = a \prod_{i=1}^{n} (x - r_i)$$

If $r_1, \dots, r_s$ where $s \leq n$ are the distinct roots of $f(x)$, then collecting terms gives

$$f(x) = a(x - r_1)^{e_1} \dots (x - r_s)^{e_s}$$

where r_j are distinct and $e_j \geq 1$. We call e_j the **multiplicity** of the root r_j.

Theorem 3.58. *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Every rational root r of $f(x)$ has the form b/c, where $b \mid a_0$ and $c \mid a_n$*

Proof. We may assume that $r = b/c$ is in lowest form.

$$0 = f(b/c) = a_0 + a_1(b/c) + \cdots + a_n(b/c)^n$$
$$0 = a_0 c^n + a_1 b c^{n-1} + \cdots + a_n b^n$$

Hence $a_0 c^n = b(-a_1 c^{n-1} - \cdots - a_n b^{n-1})$, that is $b \mid a_0 c^n$. □

Definition 3.59. A complex number α is called an **algebraic integer** if α is a root of a monic $f(x) \in \mathbb{Z}[x]$

Corollary 3.60. *A rational number z that is an algebraic integer must lie in $\mathbb{Z}$. More precisely, if $f(x) \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ is a monic polynomial, then every rational root of $f(x)$ is an integer that divides the constant term*

Proof. $a_n = 1$ in Theorem 3.58 □

For example, consider $f(x) = x^3 + 4x^2 - 2x - 1 \in \mathbb{Q}[x]$. By Corollary 3.48, this cubic is irreducible if and only if it has no rational root. As $f(x)$ is monic, the candidates for rational roots are ± 1, for these are the only divisor of -1 in $\mathbb{Z}$. Thus $f(x)$ has no roots in $\mathbb{Q}$ and hence $f(x)$ is irreducible in $\mathbb{Q}[x]$

Exercise 3.3.1. 1. Let $f(x) = (x-a_1)\cdots(x-a_n) \in k[x]$ where k is a field. Show that $f(x)$ has **no repeated roots** if and only if $\gcd(f, f') = 1$ where $f'(x)$ is the derivative of f
2. Prove that if $p(x) \in \mathbb{Q}[x]$ is an irreducible polynomial, then $p(x)$ has no repeated roots in $\mathbb{C}$

Proof. 1. $f'(x) = \sum_{i=1}^{n}(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)$ □

3.4 Homomorphisms

Definition 3.61. If A and R are (commutative) rings, a **(ring) homomorphism** is a function $f : A \to R$ s.t.
1. $f(1) = 1$
2. $f(a+a') = f(a) + f(a')$
3. $f(aa') = f(a)f(a')$

Example 3.5. 1. Let R be a domain and let $F = \mathrm{Frac}(R)$. $R' = \{[a,1] : a \in R\} \subseteq F$, then the function $f : R \to R'$ given by $f(a) = [a,1]$, is an isomorphism
2. Complex conjugation $z = a + ib \mapsto \overline{z} = a - ib$ is an isomorphism $\mathbb{C} \to \mathbb{C}$.
3. Let R be a commutative ring, and let $a \in R$. Define the **evaluation homomorphism** $e_a : R[x] \to R$ by $e_a(f(x)) = f(a)$.

Lemma 3.62. *If $f : A \to R$ is a ring homomorphism, then for all $a \in A$*
1. *$f(a^n) = f(a)^n$*
2. *if a is a unit, then $f(a)$ is a unit and $f(a^{-1}) = f(a)^{-1}$*
3. *if $f : A \to R$ is a ring homomorphism, then*

$$f(U(A)) \leq U(R)$$

where $U(A)$ is the group of units of A; if f is an isomorphism, then

$$U(A) \cong U(R)$$

Proposition 3.63. *If R and S are commutative rings and $\varphi : R \to S$ is a ring homomorphism, then there is a ring homomorphism $\varphi^* : R[x] \to S[x]$ given by*

$$\varphi^* : r_0 + r_1x + r_2x^2 + \cdots \mapsto \varphi(r_0) + \varphi(r_1)x + \varphi(r_2)x^2 + \ldots$$

Definition 3.64. If $f : A \to R$ is a ring homomorphism, then its **kernel** is

$$\ker f = \{a \in A : f(a) = 0\}$$

and its **image** is

$$\text{im } f = \{r \in R : \exists a \in R \;\; r = f(a)\}$$

The kernel of a group homomorphism is not merely a subgroup; it is a **normal** subgroup. Similarly, the kernel of a ring homomorphism is almost a subring ($1 \notin \ker f$) and is closed under multiplication.

Definition 3.65. An **ideal** in a commutative ring R is a subset I of R s.t.

1. $0 \in I$
2. if $a, b \in I$, then $a + b \in I$
3. if $a \in I$ and $r \in R$, then $ra \in I$

An ideal $I \neq R$ is called a **proper ideal**

Example 3.6. If $b_1, \ldots, b_n \in R$, then the set of all linear combinations

$$I = \{r_1 b_1 + \cdots + r_n b_n : r_i \in R\}$$

is an ideal in R. We write $I = (b_1, \ldots, b_n)$ in this case and we call I the **ideal generated by** $b_1, \ldots, b_n$. In particular, if $n = 1$, then

$$I = (b) = \{rb : r \in R\}$$

is an ideal in R; (b) consists of all the multiplies of b and it is called the **principal ideal** generated by b. Notice that R and $\{0\}$ are always principal ideals: $R = (1), \{0\} = (0)$

Proposition 3.66. *If $f : A \to R$ is a ring homomorphism, then* ker f *is an ideal in A and* im f *is a subring of R. Moreover, if A and R are not zero rings, then* ker f *is a proper ideal.*

Example 3.7.

1. If an ideal I in a commutative ring R contains 1, then $I = R$
2. it follows from 1 that if R is a field, then the only ideals are $\{0\}$ and R

Proposition 3.67. *A ring homomorphism $f : A \to R$ is an injection if and only if* ker $f = \{0\}$

Corollary 3.68. *If $f : k \to R$ is a ring homomorphism, where k is a field and R is not the zero ring, then f is an injection*

Proof. the only proper ideal in k is $\{0\}$ □

Theorem 3.69. *If k is a field, then every ideal I in $k[x]$ is a principal ideal. Moreover, if $I \neq \{0\}$, there is a monic polynomial that generates I*

Proof. If k is a field, then $k[x]$ is an example of a **euclidean ring**. Follows Theorem 3.75 □

Definition 3.70. A domain R is a **principal ideal domain** (PID) if every ideal in R is a principal ideal.

Example 3.8.
1. The ring of integers is a PID
2. Every field is a PID
3. If k is a field, then the polynomial ring $k[x]$ is a PID
4. There are rings other than $\mathbb{Z}$ and $k[x]$ where k is a field that have a division algorithm; they are called **euclidean rings**.

Example 3.9. Let $R = \mathbb{Z}[x]$. The set of all polynomials with even constant term is an ideal in $\mathbb{Z}[x]$. We show that I is not a principal ideal.

Suppose there is $d(x) \in \mathbb{Z}[x]$ with $I = (d(x))$. The constant $2 \in I$, so that there is $f(x) \in \mathbb{Z}[x]$ with $2 = d(x)f(x)$. We have $0 = \deg(2) = \deg(d) + \deg(f)$. The candidates for $d(x)$ are ± 1 and ± 2. Suppose $d(x) = \pm 2$; since $x \in I$, there is $g(x) \in \mathbb{Z}[x]$ with $x = d(x)g(x) = \pm 2g(x)$. But every coefficients on the right side is even. This contradiction gives $d(x) = \pm 1$. Hence $I = \mathbb{Z}[x]$, another contradiction. Therefore I is not a principal ideal.

Definition 3.71. An element δ in a commutative ring R is a **greatest common divisor**, gcd, of elements $\alpha, \beta \in R$ if
1. δ is a common divisor of α and β
2. if γ is any common divisor of α and β, then $\gamma \mid \delta$

Remark. Let R be a PID and let $\pi, \alpha \in R$ with π irreducible. A gcd δ of π and α is a divisor of π. Hence $\pi = \delta\epsilon$. And irreducibility of π forces either δ or ϵ to be a unit. Now $\alpha = \delta\beta$. If δ is not a unit, then ϵ is a unit and so

$$\alpha = \delta\beta = \pi\epsilon^{-1}\beta$$

that is $\pi \mid \alpha$. We conclude that if $\pi \nmid \alpha$ then δ is a unit; that is 1 is a gcd of π and α

Theorem 3.72. *Let R be a PID*
1. *Every $\alpha, \beta \in R$ has a gcd, δ, which is a linear combination of α and β*

$$\delta = \sigma\alpha + \tau\beta$$

2. *If an irreducible element $\pi \in R$ divides a product $\alpha\beta$, then either $\pi \mid \alpha$ or $\pi \mid \beta$*

Proof. 1. We may assume that at least one of α and β is not zero. Consider the set I of all the linear combinations

$$I = \{\sigma\alpha + \tau\beta : \sigma, \tau \in R\}$$

I is an ideal and so there is $\delta \in I$ with $I = (\delta)$; we claim that δ is gcd of α and β. Note that $\alpha, \beta, \delta \in I$

2. If $\pi \nmid \alpha$, then the remark says that 1 is a gcd of π and α. Thus $1 = \sigma\pi + \tau\alpha$ and so
$$\beta = \sigma\pi\beta + \tau\alpha\beta$$
Since $\pi \mid \alpha\beta$, it follows that $\pi \mid \beta$

□

Definition 3.73. If f and g are elements in a commutative ring R, then a **common multiple** is an element $m \in R$ with $f \mid m$ and $g \mid m$. If f and g in R are not both 0, define their **least common multiple**, abbreviated lcm.

Exercise 3.4.1. If k is a field, prove that $\sqrt{1-x^2} \notin k(x)$, where $k(x)$ is the field of rational functions

Proof. If $\sqrt{1-x^2} \in k(x)$, then $1 - x^2 = p^2(x)/q^2(x)$ and $q^2(x) = p^2(x) + x^2q^2(x)$. However $\deg(x^2q^2(x) > \deg(q^2(x)))$ □

Exercise 3.4.2. 1. Show that every element $a \in \mathbb{I}_p$ has a pth root

2. Let k be a field that contains $\mathbb{I}_p$ as a subfield. For every positive integer n, show that the function $\varphi_n : k \to k$, given by $\varphi(a) = a^{p^n}$ is a ring homomorphism

Proof. 1. $a^p \equiv a \mod p$

2. stackexchange

□

Exercise 3.4.3. 1. If A and R are domains and $\varphi : A \to R$ is a ring homomorphism, prove that

$$[a, b] \to [\varphi(a), \varphi(b)]$$

is a ring homomorphism $\mathrm{Frac}(A) \to \mathrm{Frac}(R)$

2. Prove that if a field k contains an isomorphic copy of $\mathbb{Z}$ as a subring, then k must contain an isomorphic copy of $\mathbb{Q}$
3. Let R be a domain and let $\varphi : R \to k$ be an injective ring homomorphism, where k is a field. Prove that there exists a unique ring homomorphism $\Phi : \mathrm{Frac}(R) \to k$ extending φ ; that is, $\Phi|R = \varphi$

Proof. 1.

$$\begin{aligned} f([1,1]) &= [1,1] \\ f([a,b]+[c,d]) &= f([ad+bc,bd]) = [\varphi(ad+bc),\varphi(bd)] \\ &= [\varphi(a)\varphi(d)+\varphi(b)\varphi(c),\varphi(b)\varphi(d)] \\ &= [\varphi(a),\varphi(b)]+[\varphi(c),\varphi(d)] \\ &= f([a,b])+f([c,d]) \\ f([a,b][c,d]) &= f([ac,bd]) = [\varphi(ac),\varphi(bd)] = [\varphi(a)\varphi(c),\varphi(b)\varphi(d)] \\ &= f([a,b])\,f([c,d]) \end{aligned}$$

2. Suppose $k' \leq k$ and $k' \cong \mathbb{Z}$, then $\mathrm{Frac}(k') \cong \mathrm{Frac}(\mathbb{Z})$. Obviously.
3. k is a field and has inverse.

□

3.5 Euclidean Rings

Definition 3.74. A **euclidean ring** is a domain that is equipped with a function

$$\partial : R - \{0\} \to \mathbb{N}$$

called a **degree function**, s.t.

1. $\partial(f) \leq \partial(fg)$ for all $f, g \in R$ with $f, g \neq 0$
2. for all $f, g \in R$ with $f \neq 0$, there exists $q, r \in R$ with

$$g = qf + r$$

where either $r = 0$ or $\partial(r) < \partial(f)$

Example 3.10. 1. The integers $\mathbb{Z}$ is a euclidean ring with the degree function $\partial(m) = |m|$. In $\mathbb{Z}$ we have

$$\partial(mn) = |mn| = |m||n| = \partial(m)\partial(n)$$

2. when k is a field, the domain $k[x]$ is a euclidean ring with degree function the usual degree of a nonzero polynomial. In $k[x]$, we have

$$\partial(fg) = \deg(fg) = \deg(f) + \deg(g) = \partial(f) + \partial(g)$$

If a degree function is multiplicative, then ∂ is called a **norm**

3. The Gaussian integers $\mathbb{Z}[i]$ form a euclidean ring whose degree function
$$\partial(a+bi) = a^2 + b^2$$
is a norm. One reason to show that $\mathbb{Z}[i]$ is a euclidean ring is that it is a PID, and hence it has unique factorization of its elements of into products of irreducibles.
∂ is a multiplicative degree function for
$$\partial(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\,\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \partial(\alpha)\partial(\beta)$$
Let us show that ∂ satisfies the second desired property. Given $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, regard α/β as an element of $\mathbb{C}$. Rationalizing the denominator gives $\alpha/\beta = \alpha\overline{\beta}/\beta\overline{\beta} = \alpha\overline{\beta}/\partial\beta$, so that
$$a/\beta = x + yi$$
where $x, y \in \mathbb{Q}$. Write $x = a + u$ and $y = b + v$, where $a, b \in \mathbb{Z}$are integers closest to x and y, respectively; thus $|u|, |v| \leq 1/2$. It follows that
$$\alpha = \beta(a+bi) + \beta(u+vi)$$
Notice that $\beta(u+vi) \in \mathbb{Z}[i]$. Finally we have
$$\partial(\beta(u+vi)) = \partial(\beta)\partial(u+vi) < \partial(\beta)$$
And so $\mathbb{Z}[i]$ is a euclidean ring whose degree function is a norm
Note that quotients and remainders are not unique because of the choice

Theorem 3.75. *Every euclidean ring R is a PID*

Proof. Let I be an ideal in R. If $I \neq \{0\}$, by the least integer axiom, the set of all degrees of nonzero elements in I has a smallest element, say n; choose $d \in I$ with $\partial(d) = n$. Clearly $(d) \subseteq I$. For any $a \in I$, then there are $q, r \in R$ with $a = qd + r$, where either $r = 0$ or $\partial(r) < \partial(a)$. But $r = a - qd \in I$ and so d having the least degree implies that $r = 0$. Hence $a = qd \in (d)$. □

Corollary 3.76. *The ring of Gaussian integers $\mathbb{Z}[i]$ is a PID*

Definition 3.77. An element u in a domain R is a **universal side divisor** if u is not a unit and for every $x \in R$, either $u \mid x$ or there is a unit $z \in R$ with $u \mid (x + z)$

Proposition 3.78. *If R is a euclidean ring but not a field, then R has a universal side divisor*

Proof. Define

$$S = \{\partial(v) : v \neq 0 \text{ and } v \text{ is not a unit}\}$$

where ∂ is the degree function on R. Since R is not a field, S is a nonempty subset of the natural number. By the least integer axiom, S has a smallest element, say, $\partial(u)$. We claim that u is a universal side divisor. If $x \in R$, then there are q, r with $x = qu + r$. □

Proposition 3.79. *1. Let R be a euclidean ring R that is not a field. If the degree function ∂ is a norm, then α is a unit if and only if $\partial(\alpha) = 1$*

2. *Let R be a euclidean ring R that is not a field. If the degree function ∂ is a norm and if $\partial(a) = p$, where p is a prime, then α is not irreducible*
3. *The only units in the ring $\mathbb{Z}[i]$ of Gaussian integers are ± 1 and $\pm i$*

Proof. 1. Since $1^2 = 1$, we have $\partial(1)^2 = \partial(1)$, so that $\partial(1) = 0$ or $\partial(1) = 1$. If $\partial(1) = 0$, then $\partial(a) = \partial(1a) = 0$. But R is not a field, and so ∂ is not identically zero. We conclude that $\partial(1) = 1$

If $a \in R$ is a unit, then there is $\beta \in R$ with $\alpha\beta = 1$. Therefore $\partial(\alpha)\partial(\beta) = 1$ and hence $\partial(\alpha) = 1$

For the converse, we begin by showing that there is no element $\beta \in R$ with $\partial(\beta) = 0$. If such an element exists, the division algorithms gives $1 = q\beta + r$ and so $\partial(r) = 0$. That is β is a unit, then $\partial(\beta) = 1$, a contradiction

Assume now that $\partial(\alpha) = 1$. The division algorithm gives

$$\alpha = q\alpha^2 + r$$

As $\partial(\alpha^2) = \partial(\alpha)^2 = 1$, $r = 0$ or $\partial(r) = 0$, which would not occur. Hence $r = 0$ and $\alpha = q\alpha^2$. It follows that $1 = q\alpha$, and so α is a unit

2. If on the contrary, $\alpha = \beta\gamma$, where neither β or γ is a unit, then $p = \partial(\alpha) = \partial(\beta)\partial(\gamma)$.
3. If $\alpha = a + bi \in \mathbb{Z}[i]$ is a unit, then $1 = \partial(\alpha) = a^2 + b^2$.

□

Lemma 3.80. *If p is a prime and $p \equiv 1 \mod 4$, then there is an integer m with*

$$m^2 \equiv -1 \mod p$$

Proof. If $G = (\mathbb{I}_p)^\times$ is the multiplicative group of nonzero elements in $\mathbb{I}_p$, then $|G| = p - 1 \equiv 0 \mod 4$. By Proposition 2.71, G contains a subgroup

S of order 4. By Exercise 2.3.1 either S is cyclic or $a^2 = 1$ for all $a \in S$. Since $\mathbb{I}_p$ is a field, however, it cannot contain four roots of the quadratic $x^2 - 1$. Therefore, S is cyclic, say $S = \langle [m] \rangle$ where $[m]$ is the congruence class of m mod p. Since $[m]$ has order 4, we have $[m^4] = [1], [m^2] \neq 1$, and so $[m^2] = [-1]$ for $[-1]$ is the unique element in S of order 2. Therefore, $m^2 \equiv -1 \mod p$ □

Theorem 3.81 (Fermat's Two-Squares Theorem)**.** *An odd prime p is a sum of two squares,*

$$p = a^2 + b^2$$

where a and b are integers if and only if $p \equiv 1 \mod 4$

Proof. Assume that $p = a^2 + b^2$. Since p is odd, a and b have different parity; say, a is even and b is odd. Hence $a = 2m$ and $b = 2n + 1$ and

$$p = a^2 + b^2 = 4m^2 + 4n^2 + 4n + 1 \equiv 1 \mod 4$$

Conversely, assume that $p \equiv 1 \mod 4$. By the lemma, there is an integer m s.t.

$$p \mid (m^2 + 1)$$

In $\mathbb{Z}[i]$, there is a factorization $m^2 + 1 = (m + i)(m - i)$ and so

$$p \mid (m + i)(m - i) \text{ in } \mathbb{Z}[i]$$

If $p \mid (m \pm i)$ in $\mathbb{Z}[i]$, then there are integers u and v with $m \pm i = p(u + iv)$. Comparing the imaginary parts gives $pv = 1$, a contradiction. We conclude that p does not satisfy the analog of Euclid's lemma in Theorem 3.72; it follows from Exercise 3.5.1 that p is not irreducible. Hence there is a factorization

$$p = \alpha\beta \in \mathbb{Z}[i]$$

Therefore, taking norms gives an equation in $\mathbb{Z}$

$$\begin{aligned} p^2 &= \partial(p) = \partial(\alpha\beta) \\ &= \partial(\alpha)\partial(\beta) = (a^2 + b^2)(c^2 + d^2) \end{aligned}$$

By Proposition 3.79, the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$, so that any nonzero Gaussian integers that is not a unit has a norm > 1; therefore $a^2 + b^2 \neq 1$ and $c^2 + d^2 \neq 1$. Euclid's lemma now gives $p \mid a^2 + b^2$ or $p \mid c^2 + d^2$; then fundamental theorem of arithmetic gives $p = a^2 + b^2$. □

Lemma 3.82. *If $\alpha \in \mathbb{Z}[i]$ is irreducible, then there is a unique prime number p with $a \mid p$ in $\mathbb{Z}[i]$*

Proof. Since $\partial(\alpha) = \alpha\overline{\alpha}$, we have $\alpha \mid \partial(\alpha)$. Now $\partial(\alpha) = p_1 \dots p_n$. If $\alpha \mid q$ for some prime $q \neq p_i$, then $\alpha \mid (q, p_i) = 1$, forcing α to be unit. A contradiction □

Proposition 3.83. *Let $\alpha = a + bi \in \mathbb{Z}[i]$ be neither 0 nor a unit. Then α is irreducible if and only if*

1. *α is an associate of a prime p in $\mathbb{Z}$ of the form $p = 4m + 3$; or*
2. *α is an associate of $1 + i$ or its conjugate; or*
3. *$\partial(\alpha) = a^2 + b^2$ is a prime in $\mathbb{Z}$ of the form $4m + 1$*

Proof. By Lemma 3.82 there is a unique prime number p divides by α in $\mathbb{Z}[i]$. Since $\alpha \mid p$, we have $\partial(\alpha) \mid \partial(p) = p^2$ in $\mathbb{Z}$, so that $\partial(\alpha) = p$ or $\partial(\alpha) = p^2$.

1. $p \equiv 3 \mod 4$
   By Theorem 3.81 $p^2 = a^2 + b^2$. We have $\alpha\beta = p$ and $\partial(\alpha)\partial(\beta) = \partial(p)$. Therefore, $p^2\partial(\beta) = p^2$ and $\partial(\beta) = 1$. Thus β is a unit by Proposition 3.79 and p is irreducible.
2. $p \equiv 2 \mod 4$
   $a^2 + b^2 = 2$
3. $p \equiv 1 \mod 4$ If $\partial(\alpha) = p^2$, β is a unit as case 1. Now $\alpha\overline{\alpha} = p^2 = (\alpha\beta)^2$, so that $\overline{\alpha} = \alpha\beta^2$ but $\beta^2 = \pm 1$ by Proposition 3.79

□

Exercise 3.5.1. If R is a euclidean ring and $\pi \in R$ is irreducible, prove that $\pi \mid \alpha\beta$ implies $\pi \mid \alpha$ or $\pi \mid \beta$

Proof. R is PID and follow Theorem 3.72. □

3.6 Linear Algebra

Vector Spaces

Definition 3.84. If k is a field, then a **vector space over** k is an (additive) abelian group V equipped with a **scalar multiplication**; there is a function $k \times V \to V$, denoted by $(a, v) \mapsto av$ s.t. for all $a, b, 1 \in k$ and all $u, v \in V$

1. $a(u + v) = au + av$
2. $(a + b)v = av + bv$
3. $(abv) = a(bv)$
4. $1v = v$

The elements of V are called **vectors** and the elements of k are called **scalars**

Example 3.11. 1. Euclidean space $V = \mathbb{R}^n$ is a vector space over $\mathbb{R}$
2. If R is a commutative ring and k is a subring that is a field, then R is a vector space over k
   For example, if k is a field, then the polynomial ring $R = k[x]$ is a vector space over k.

Definition 3.85. If V is a vector space over a field k, then a **subspace** of V is a subset U of V s.t.
1. $0 \in U$
2. $u, u' \in U$ imply $u + u' \in U$
3. $u \in U$ and $a \in k$ imply $au \in U$

Definition 3.86. Let V be a vector space over a field k. A **k-linear combination** of a list $v_1, \ldots, v_n$ in V is a vector of v of the form

$$v = a_1 v_1 + \cdots + a_n v_n$$

where $a_i \in k$ for all i

Definition 3.87. If $X = v_1, \ldots, v_m$ is a list in a vector space V, then

$$\langle v_1, \ldots, v_m \rangle$$

the set of all the k-linear combinations of $v_1, \ldots, v_m$ is called the **subspace spanned by** X. We also say that $v_1, \ldots, v_m$ **spans** $\langle v_1, \ldots, v_m \rangle$

Lemma 3.88. *Let V be a vector space over a field k*
1. *Every intersection of subspaces of V is itself a subspace*
2. *If $X = v_1, \ldots, v_m$ is a list in V, then the intersection of all the subspaces of V containing X is $\langle v_1, \ldots, v_m \rangle$, and so $\langle v_1, \ldots, v_m \rangle$ is the **smallest subspace***

Example 3.12. Let $V = \mathbb{R}^2$, let $e_1 = (1, 0)$ and let $e_2 = (0, 1)$. then $V = \langle e_1, e_2 \rangle$

Definition 3.89. A vector space V is called **finite-dimensional** if it is spanned by a finite list; otherwise V is called **infinite-dimensional**

Notation. If $v_1, \ldots, v_m$ is a list, then $v_1, \ldots, \widehat{v_i}, \ldots, v_m$ is the shorter list with v_i deleted

Proposition 3.90. *If V is a vector space, then the following conditions on a list $X = v_1, \ldots, v_m$ spanning V are equivalent*

1. *X is not a shortest spanning list*
2. *some v_i is in the subspace spanned by the others; that is*

$$v_i \in \langle v_1, \ldots, \widehat{v_i}, \ldots, v_m \rangle$$

3. *there are scalars $a_1, \ldots, a_m$ not all zero with*

$$\sum_{l=1}^{m} a_l v_l = 0$$

Definition 3.91. A list $X = v_1, \ldots, v_m$ in a vector space V is **linearly dependent** if there are scalars $a_1, \ldots, a_m$ not all zero, with $\sum_{l=1}^{m} a_l v_l = 0$; otherwise X is called **linearly independent**

Corollary 3.92. *If $X = v_1, \ldots, v_m$ is a list spanning a vector space V, then X is a shortest spanning list if and only if X is linearly independent*

Definition 3.93. A **basis** of a vector space V is a linearly independent list that spans V

Proposition 3.94. *Let $X = v_1, \ldots, v_n$ be a list in a vector space V over a field k. Then X is a basis if and only if each vector in V has a unique expression as a k-linear combination of vectors in X*

Proof. If a vector $v = \sum a_i v_i = \sum b_i v_i$, then $\sum (a_i - b_i) = 0$ □

Definition 3.95. If $X = v_1, \ldots, v_n$ is a basis of a vector space V and if $v \in V$, then there are unique scalars $a_1, \ldots, a_n$ with $v = \sum_{i=1}^{n} a_i v_i$. The n-tuple $(a_1, \ldots, a_n)$ is called the **coordinate set** of a vector $v \in V$ relative to the basis X

Theorem 3.96. *Every finite-dimensional vector space V has a basis*

Proof. A finite spanning list X exists, since V is finite-dimensional. If it is linearly independent, it is a basis; if not, X can be shortened to a spanning list X' by Proposition 3.90 □

Lemma 3.97. *Let $u_1, \ldots, u_n$ be elements in a vector space V, and let $v_1, \ldots, v_m \in \langle u_1, \ldots, u_n \rangle$. If $m > n$, then $v_1, \ldots, v_m$ is a linearly dependent list*

Proof. Induction on $n \geq 1$
Base step. If $n = 1$
Inductive step. For $i = 1, \ldots, m$

$$v_i = a_{i1}u_1 + \cdots + a_{in}u_n$$

We may assume that some $a_{i1} \neq 0$ otherwise $v_1, \ldots, v_m \in \langle u_2, \ldots, u_n \rangle$, and the inductive hypothesis applies. Changing notation if necessary we may assume $a_{11} \neq 0$. For each $i \geq 2$, define

$$v_i' = v_i - a_{i1}a_{11}^{-1}v_1 \in \langle u_2, \ldots, u_n \rangle$$

Since $m - 1 > n - 1$ □

Corollary 3.98. *A homogeneous system of linear equations, over a field k, with more unknowns than equations has a nontrivial solution.*

Proof. An n-tuple $(\beta_1, \ldots, \beta_n)$ is a solution of a system

$$\begin{gathered} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n = 0 \\ \vdots \quad \vdots \quad \vdots \\ \alpha_{m1}x_1 + \cdots + \alpha_{mn}x_n = 0 \end{gathered}$$

if $\alpha_{i1}\beta_1 + \cdots + \alpha_{in}\beta_n = 0$ for all i. In other words, if $c_1, \ldots, c_n$ are the columns of the $m \times n$ coefficient matrix $A = [\alpha_{ij}]$, then

$$\beta_1 c_1 + \cdots + \beta_n c_n = 0$$

Note that $c_i \in k^m$. Now k^m can be spanned by m vectors. Since $n > m$, $c_1, \ldots, c_n$ is linearly dependent □

Theorem 3.99 (Invariance of Dimension)**.** *If $X = x_1, \ldots, x_n$ and $Y = y_1, \ldots, y_m$ are bases of a vector space V, then $m = n$*

Proof. Otherwise $n < m$ or $m < n$ □

Definition 3.100. If V is a finite-dimensional vector space over a field k, then its **dimension** denoted by $\dim_k(V)$ or $\dim(V)$, is the number of elements in a basis of V

Example 3.13. Let $X = \{x_1, \ldots, x_n\}$ be a finite set. Define

$$k^X = \{\text{functions } f : X \to k\}$$

Now k^X is a vector space if we define addition

$$f + f' : x \mapsto f(x) + f'(x)$$

and scalar multiplication for $a \in k$

$$af : x \mapsto af(x)$$

It's easy to check that the set of n functions of the form f_x, where $x \in X$ defined by

$$f_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 \end{cases}$$

form a basis.

An n-tuple $(a_1, \ldots, a_n)$ is really a function $f : \{1, \ldots, n\} \to k$ with $f(i) = a_i$

Lemma 3.101. *If $X = v_1, \ldots, v_n$ is a linearly dependent list of vectors in a vector space V, then there exists v_r with $r \geq 1$ with $v_r \in \langle v_1, \ldots, v_{r-1} \rangle$*

Lemma 3.102 (Exchange Lemma)**.** *If $X = x_1, \ldots, x_m$ is a basis of a vector space V and $y_1, \ldots, y_n$ is a linearly independent subset of V, then $n \leq m$*

Proof. We begin by showing that one of the x's in X can be replaced by y_n so that the new list still spans V. Now $y_n \in \langle X \rangle$, so that the list

$$y_n, x_1, \ldots, x_m$$

is linearly dependent. By Lemma 3.101 there is some i with $x_i = ay_n + \sum_{j<i} a_j x_j$. Throwing out x_i and replacing it by y_n gives a spanning list

$$X' = y_n, x_1, \ldots, \widehat{x_i}, \ldots, x_m$$

Now repeat this argument for the spanning list $y_{n-1}, y_n, x_1, \ldots, \widehat{x_i}, \ldots, x_m$. It follows that the disposable vector must be one of the remaining x's, say x_l. After throwing out x_l, we have a new spanning list X''. If $n > m$, then this procedure ends with a spanning list consisting of m y's and no x'. Thus a proper sublist of $Y = y_1, \ldots, y_n$ spans V, a contradiction □

Theorem 3.103 (Invariance of Dimension)**.** *If $X = x_1, \ldots, x_n$ and $Y = y_1, \ldots, y_m$ are bases of a vector space V, then $m = n$*

Proof. By Lemma 3.102, $n \leq m$ and $m \leq n$ □

Definition 3.104. A **longest** (or a **maximal**) linearly independent list $u_1, \ldots, u_m$ is a linearly independent list for which there is no vector $v \in V$ s.t. $u_1, \ldots, u_m, v$ is linearly independent

Lemma 3.105. *If V is a finite-dimensional vector space, then a longest linearly independent list $v_1, \ldots, v_n$ is a basis of V*

Proposition 3.106. *Let $Z = u_1, \ldots, u_m$ be a linearly independent list in an n-dimensional vector space V. Then Z can be extended to a basis*

Corollary 3.107. *If $\dim(V) = n$, then any list of $n+1$ or more vectors is linearly dependent*

Corollary 3.108. *Let V be a vector space with $\dim(V) = n$*
1. *A list of n vectors that spans V must be linearly independent*
2. *Any linearly independent list of n vectors must span V*

Corollary 3.109. *Let U be a subspace of a vector space V of dimension n*
1. *U is finite-dimensional and $\dim(U) \leq \dim(V)$*
2. *If $\dim(U) = \dim(V)$, then $U = V$*

Exercise 3.6.1. If V is a finite-dimensional vector space and U is a subspace, prove that

$$\dim(U) + \dim(V/U) = \dim(V)$$

Proof. If $v_1 + U, \ldots, v_r + U$ is a basis of V/U, then $v_1, \ldots, v_r$ are linearly independent. □

Linear Tranformations

Definition 3.110. If V and W are vector spaces over a field k, then a function $T : V \to W$ is a **linear transformation** if for all vectors $u, v \in V$, and all scalars $a \in k$
1. $T(u+v) = T(u) + T(v)$
2. $T(av) = aT(v)$

We say that a linear transformation T is **nonsingular** (or is an **isomorphism**) if T is a bijection.

Example 3.14. 1. If θ is an angle, then the rotation about the origin by θ is a linear transformation $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$

2. If V and W are vector spaces over a field k, write $\mathrm{Hom}_k(V, W)$ for the set of all linear transformations $V \to W$. It's a vector space

Definition 3.111. If V is a vector space over a field k, then the **general linear group**, denoted by $\mathrm{GL}(V)$, is the set of all nonsingular linear transformations $V \to V$

A composite ST of linear transformation S and T is again a linear transformation

Theorem 3.112. *Let $v_1, \ldots, v_n$ be a basis of a vector space V over a field k. If W is a vector space over k and $u_1, \ldots, u_n$ is a list in W, then there exists a unique linear transformation $T : V \to W$ with $T(v_i) = u_i$ for all i*

Proof. Each $v \in V$ has a unique expression of the form $v = \sum_i a_i v_i$ and so $T : V \to W$ given by $T(v) = \sum a_i u_i$ is a well-defined function

To prove the uniqueness of T, assume that $S : V \to W$ is a linear transformation with

$$S(v_i) = u_i = T(v_i)$$

Then

$$\begin{aligned} S(v) &= S(\sum a_i v_i) = \sum S(a_i v_i) \\ &= \sum a_i S(v_i) = \sum a_i T(v_i) = T(v) \end{aligned}$$

□

Corollary 3.113. *If two linear transformations $S, T : V \to W$ agree on a basis, then $S = T$*

Proposition 3.114. *If $T : k^n \to k^m$ is a linear transformation, then there exists an $m \times n$ matrix A s.t.*

$$T(y) = Ay$$

for all $y \in k^n$ (here y is an $n \times 1$ column matrix)

Proof. If $e_1, \ldots, e_n$ is the standard basis of k^n and $e'_1, \ldots, e'_m$ is the standard basis of k^m, define $A = [a_{ij}]$ to be the matrix whose jth column is the coordinate set of $T(e_j)$. If $S : k^n \to k^m$ is defined by $S(y) = Ay$, then $S = T$ since they agree on a basis: $T(e_j) = \sum_i a_{ij} e'_i = Ae_j$ □

Definition 3.115. Let $X = v_1, \ldots, v_n$ be a basis of V and let $Y = w_1, \ldots, w_m$ be a basis of W. If $T : V \to W$ is a linear transformation, then the **matrix of** T is the $m \times n$ matrix $A = [a_{ij}]$, whose jth column $a_{1j}, a_{2j}, \ldots, a_{mj}$ is the coordinate set of $T(v_j)$ determined by w's: $T(v_j) = \sum_{i=1}^{m} a_{ij} w_j$. The matrix A does depend on the choice of bases X and Y: we will write

$$A = {}_Y[T]_X$$

In case $V = W$, we often let the basis $X = v_1, \ldots, v_n$ and $w_1, \ldots, w_m$ coincide. If $1_V : V \to V$, given by $v \mapsto v$ is the identity linear transformation, then ${}_X[1_V]_X$ is the $n \times n$ **identity matrix** I_n, defined by

$$I = [\delta_{ij}]$$

where δ_{ij} is the Kronecker delta. A matrix is **nonsingular** if it has inverse.

Example 3.15. Let $T : V \to W$ be a linear transformation, and let $X = v_1, \ldots, v_n$ and $Y = w_1, \ldots, w_n$ be bases of V and W ,respectively. The matrix for T is set up from the equation

$$T(v_j) = a_{1j} w_1 + \cdots + a_{mj} w_m$$

Example 3.16.

1. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be rotation by 90°. The matrix of T related to the standard basis $X = (1, 0), (0, 1)$ is

$$ {}_X[T]_X = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

   However if $Y = (0, 1)(1, 0)$, then

$$ {}_Y[T]_Y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

2. Let k be a field, let $T : V \to V$ be a linear transformation on a two-dimensional vector space, and assume that there is some vector $v \in V$ with $T(v)$ not a scalar multiple of v. The assumption on v says that the list $X = v, T(v)$ is linearly independent, and hence it's a basis of V. Write $v_1 = v, v_2 = Tv$.
   We compute ${}_X[T]_X$

$$T(v_1) = v_2 \quad \text{and} \quad T(v_2) = av_1 + bv_2$$

   for some $a, b \in k$. We conclude that

$$ {}_X[T]_X = \begin{bmatrix} 0 & a \\ 1 & b \end{bmatrix}$$

Proposition 3.116. *Let V and W be a vector spaces over a field k, and let $X = v_1, \ldots, v_n$ and $Y = w_1, \ldots, w_m$ be bases of V and W, respectively. If $\mathrm{Hom}_k(V, W)$ denotes the set of all linear transformations $T : V \to W$ and $\mathrm{Mat}_{m\times n}\, k$ denotes the set of all $m \times n$ matrices with entries in k, then the function $T \mapsto {}_Y[T]_X$ is a bijection $\mathrm{Hom}_k(V, W) \to \mathrm{Mat}_{m\times n}(k)$*

Proof. Given a matrix A, its columns define vectors in W; in more detail, if the jth column of A is $a_{1j}, \ldots, a_{mj}$, define $z_j = \sum_{i=1}^{m} a_{ij} w_i$. By Theorem 3.112, there exists a linear transformation $T : V \to W$ with $T(v_j) = z_j$ and ${}_Y[T]_X = A$. □

Proposition 3.117. *Let $T : V \to W$ and $S : W \to U$ be linear transformations. Choose bases $X = x_1, \ldots, x_n$ of V, $Y = y_1, \ldots, y_m$ of W, and $Z = z_1, \ldots, z_l$ of U, then*

$$ {}_Z[S \circ T]_X = ({}_Z[S]_Y)({}_Y[T]_X) $$

Proof. Let ${}_Y[T]_X = [a_{ij}]$, so that $T(x_j) = \sum_p a_{pj} y_p$, and let ${}_Z[S]_Y = [b_{qp}]$, so that $S(y_p) = \sum_q b_{qp} z_q$. Then

$$ \begin{aligned} ST(x_j) = S(T(x_j)) &= S(\sum_p a_{pj} y_p) \\ &= \sum_p a_{pj} S(y_p) = \sum_p \sum_q a_{pj} b_{qp} z_q = \sum_q c_{qj} z_q \end{aligned} $$

where $c_{qj} = \sum_p b_{qp} a_{pj}$. Therefore

$$ {}_Z[ST]_X = [c_{qj}] = {}_Z[S]_Y\, {}_Y[T]_X $$

□

Corollary 3.118. *Matrix multiplication is associative*

Proof. Let A be an $m \times n$ matrix, let B be an $n \times p$ matrix, and let C be a $p \times q$ matrix. By Theorem 3.112, there are linear transformations

$$ k^q \xrightarrow{T} k^p \xrightarrow{S} k^n \xrightarrow{R} k^m $$

with $C = [T], B = [S], A = [R]$

Then

$$ [R \circ (S \circ T)] = [R][S \circ T] = [R]([S][T]) = A(BC) $$

On the other hand

$$ [(R \circ S) \circ T] = [R \circ S][T] = ([R][S])[T] = (AB)C $$

□

Corollary 3.119. *Let $T : V \to W$ be a linear transformation of vector space V over a field k, and let X and Y be bases of V and W, respectively. If T is nonsingular, then the matrix of T^{-1} is the inverse of the matrix of T*

$$_X[T^{-1}]_Y = (_Y[T]_X)^{-1}$$

Proof. $I = {}_Y[1_W]_Y = {}_Y[T]_X{}_X[T^{-1}]_Y$ and $I = {}_X[1_V]_X = {}_X[T^{-1}]_Y{}_Y[T]_X$ □

Corollary 3.120. *Let $T : V \to V$ be a linear transformation on a vector space V over a field k. If X and Y are bases of V, then there is a nonsingular matrix P with entries in k so that*

$$_Y[T]_Y = P(_X[T]_X)P^{-1}$$

Conversely, if $B = PAP^{-1}$, where B, A, P are $n \times n$ matrices with entries in k and P is nonsingular, then there is a linear transformation $T : k^n \to k^n$ and bases X and Y of k^n s.t. $B =_Y [T]_Y$, $A =_X [T]_X$

Proof. The first statement follows from Proposition 3.117 and associativity

$$_Y[T]_Y =_Y [1_V T 1_V]_Y = (_Y[1_V]_X)(_X[T]_X)(_X[1_V]_Y)$$

Set $P =_Y [1_V]_X$

For the converse, let $E = e_1, \ldots, e_n$ be the standard basis of k^n, and define $T : k^n \to k^n$ be $T(e_j) = Ae_j$. If follows that $A =_E [T]_E$. Now define a basis $Y = y_1, \ldots, y_n$ by $y_j = P^{-1}e_j$. Y is a basis because P^{-1} is nonsingular. It suffices to prove that $B =_Y [T]_Y$; that is $T(y_j) = \sum_i b_{ij} y_i$, where $B = [b_{ij}]$

$$\begin{aligned} T(y_j) = Ay_y = AP^{-1}e_j &= P^{-1}Be_j \\ &= P^{-1}\sum_i b_{ij}e_i = \sum_i b_{ij}P^{-1}e_i \\ &= \sum_i b_{ij}y_i \end{aligned}$$

□

Definition 3.121. Two $n \times n$ matrices B and A with entries in field k are **similar** if there is a nonsingular matrix P with entries in k with $B = PAP^{-1}$

Corollary 3.120 says the two matrices arise from the same linear transformation on a vector space V if and only if they are similar

Definition 3.122. If $T : V \to W$ is a linear transformation, then the **kernel** (or the **null space**) of T is

$$\ker T = \{v \in V : T(v) = 0\}$$

and the **image** of T is

$$\operatorname{im} T = \{w \in W : w = T(v) \text{ for some } v \in V\}$$

Proposition 3.123. *Let $T : V \to W$ be a linear transformation*

1. $\ker T$ *is a subspace of V and* $\operatorname{im} T$ *is a subspace of W*
2. *T is injective if and only if* $\ker T = \{0\}$

Lemma 3.124. *Let $T : V \to W$ be a linear transformation*

1. *If T is nonsingular, then for every basis $X = v_1, \ldots, v_n$ of V, we have $T(X) = T(v_1), \ldots, T(v_n)$ a basis of W*
2. *Conversely, if there exists some basis $X = v_1, \ldots, v_n$ of V for which $T(X)$ is a basis of W, then T is nonsingular*

Proof.

1. If $\sum c_i T(v_i) = 0$, then $T(\sum c_i v_i) = 0$ and so $\sum c_i v_i \in \ker T = \{0\}$. Hence each $c_i = 0$ because X is linearly independent. If $w \in W$, then the surjectivity of T provides $v \in V$ with $w = T(v)$. But $v = \sum a_i v_i$, and so $w = T(v) = T(\sum a_i v_i) = \sum a_i T(v_i)$. Therefore $T(X)$ is a basis of W
2. Let $w \in W$. Since $T(X)$ is a basis of W, we have $w = \sum c_i T(v_i) = T(\sum c_i v_i)$. Add so T is surjective. If $\sum c_i v_i \in \ker T$, then $\sum c_i T(v_i) = 0$ and so linear independence gives all $c_i = 0$; hence $\ker T = \{0\}$. Therefore T is nonsingular

□

Theorem 3.125. *If V is an n-dimensional vector space over a field k, then V is isomorphic to k^n*

Proof. Choose a basis $v_1, \ldots, v_n$ of V. If $e_1, \ldots, e_n$ is the standard basis of k^n, then Theorem 3.112 says that there is a linear transformation $T : V \to k^n$ with $T(v_i) = e_i$; by Lemma 3.124 T is nonsingular □

Corollary 3.126. *Two finite-dimensional vector space V and W over a field k are isomorphic if and only if* $\dim(V) = \dim(W)$

Proposition 3.127. *Let V be a finite-dimensional vector space with* $\dim(V) = n$*, and let $T : V \to V$ be a linear transformation. The following statements are equivalent*

1. *T is an isomorphism*
2. *T is surjective*
3. *T is injective*

Proof. $2 \to 3$. Let $v_1, \ldots, v_n$ be the basis of V. Since T is surjective, there are vectors $u_1, \ldots, u_n$ with $Tu_i = v_i$. We claim that $u_1, \ldots, u_n$ are linearly independent. To show that T is injective, it suffices to show that $\ker T = \{0\}$

$3 \to 1$. Let $v_1, \ldots, v_n$ be a basis of V. If $c_1, \ldots, c_n$ are scalars not all 0, then $\sum c_i v_i \neq 0$. Since T is injective, it follows that $\sum c_i T(v_i) \neq 0$ and so $Tv_1, \ldots, Tv_n$ are linearly independent. Therefore Lemma 3.124 shows that T is an isomorphism □

Corollary 3.128. *If A and B are $n \times n$ matrices with $AB = I$, then $BA = I$. Therefore A is nonsingular with inverse B*

Proof. There are linear transformations $T, S : k^n \to k^n$ with $[T] = A, [S] = B$, and $AB = I$ gives

$$[TS] = [T][S] = [1_{k^n}]$$

Since $T \mapsto [T]$ is a bijection, by Proposition 3.116, it follows that $TS = 1_{k^n}$. Hence T is a surjection and S is an injection by Proposition 1.12 But Proposition 3.127 says taht T, S are both isomorphism, so that $S = T^{-1}$ and $TS = 1_{k^n} = ST$ □

Definition 3.129. The set of all nonsingular $n \times n$ matrices with entries in k is denoted by $\mathrm{GL}(n, k)$

It's easy to prove that $\mathrm{GL}(n, k)$ is a group

Proposition 3.130. *Let V be an n-dimensional vector space over a field k, and let $X = v_1, \ldots, v_n$ be a basis of V. Then $\mu : GL(V) \to GL(n, k)$ defined by $T \mapsto [T] = {}_X[T]_X$ is an isomorphism*

Proof. By Proposition 3.116 the function $\mu' : T \mapsto [T]$ is a bijection

$$\mathrm{Hom}_k(V, V) \to \mathrm{Mat}_n(k)$$

If $T \in \mathrm{GL}(V)$, then $[T]$ is a nonsingular matrix by Corollary 3.119; that is, if μ is the restriction of μ', then $\mu : \mathrm{GL}(V) \to \mathrm{GL}(n, k)$ is an injective homomorphism.

If $A \in \mathrm{GL}(n, k)$, then $A = [T]$ for some $T : V \to V$. It suffices to show that T is an isomorphism; that is, $T \in \mathrm{GL}(V)$. Since $[T]$ is a nonsingular

matrix, there is a matrix B with $[T]B = I$. Now $B = [S]$ for some $S : V \to V$ and

$$[TS] = [T][S] = I = [1_V]$$

□

Definition 3.131. A linear transformation $T : V \to V$ is a **scalar transformation** if there is $c \in k$ with $T(v) = cv$ for all $v \in V$; that is $T = c1_V$. A **scalar matrix** is a matrix of the form cI

Corollary 3.132. *1. The center of the group $GL(V)$ consists of all the nonsingular scalar transformations*
2. The center of the group $GL(n, k)$ consists of all the nonsingular scalar matrices

3.7 Quotient Rings and Finite Fields

Theorem 3.133. *If I is an ideal in a commutative ring R, then the additive abelian group R/I can be made into a commutative ring in such a way that the natural map $\pi : R \to R/I$ is a surjective ring homomorphism*

Proof. Define multiplication on the additive abelian group R/I by

$$(a + I)(b + I) = ab + I$$

□

Definition 3.134. The commutative ring R/I constructed in Theorem 3.133 is called the **quotient ring** of R modulo I

Corollary 3.135. *If I is an ideal in a commutative ring R, then there are a commutative ring A and a ring homomorphism $\pi : R \to A$ with $I = \ker \pi$*

Proof. Natural map $\pi : R \to R/I$ □

Theorem 3.136 (First Isomorphism Theorem)**.** *If $f : R \to A$ is a homomorphism of rings, then* $\ker f$ *is an ideal in R,* $\operatorname{im} f$ *is a subring of A, and*

$$R/\ker f \cong \operatorname{im} f$$

Definition 3.137. If k is a field, the intersection of all the subfields of k is called the **prime field** of k

Every subfield of $\mathbb{C}$ contains $\mathbb{Q}$ and so the prime field of $\mathbb{C}$ and of $\mathbb{R}$ is $\mathbb{Q}$.

Notation. From now on, we will denote $\mathbb{I}_p$ by $\mathbb{F}_p$ when we are regarding it as a field.

Proposition 3.138. *If k is a field, then its prime field is isomorphic to $\mathbb{Q}$ or to $\mathbb{F}_p$ for some prime p*

Proof. Consider the ring homomorphism $\chi : \mathbb{Z} \to k$ defined by $\chi(n) = n\epsilon$, where we denote the **one** in k by ϵ. Since every ideal in $\mathbb{Z}$ is principal, there is an integer m with $\ker \chi = (m)$. If $m = 0$, then χ is an injection, and so there is an isomorphism copy of $\mathbb{Z}$ that is a subring of k. By Exercise 3.4.3 , there is a field $Q \cong \text{Frac}(\mathbb{Z}) = \mathbb{Q}$. with $\text{im}\,\chi \subseteq Q \subseteq k$. Now Q is the prime ideal of k, for it is the subfield generated by by ϵ. . If $m \neq 0$, the first isomorphism theorem gives $\mathbb{I}_m = \mathbb{Z}/(m) \cong \text{im}\,\chi \subseteq k$. Since k is a field, $\text{im}\,\chi$ is a domain, and so Proposition 3.7 gives m prime. If we now write p instead of m, then $\text{im}\,\chi = \{0, \epsilon, 2\epsilon, \ldots, (p-1)\epsilon\}$ is a subfield of k isomorphic to $\mathbb{F}_p$ □

Definition 3.139. A field k has **characteristic 0** if its prime field is isomorphic to $\mathbb{Q}$; a field k has **characteristic** p if its prime field is isomorphic to $\mathbb{F}_p$ for some prime p

The fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0

Proposition 3.140. *If k is a field of characteristic $p > 0$, then $pa = 0$ for all $a \in k$*

Proof. $p \cdot 1 = 0$ □

Proposition 3.141. *If k is a field of characteristic $p > 0$ then $pa = 0$ for all $a \in k$*

Proposition 3.142. *If k is a finite field, then $|k| = p^n$ for some prime p and some $n \geq 1$*

Proof. The prime field P of k cannot be the infinite field $\mathbb{Q}$, and so $P \cong \mathbb{F}_p$ for some p. Now k is a vector space over P, and so it is a vector space over $\mathbb{F}_p$. Clearly, k is finite-dimensional, and if $\dim_{\mathbb{F}_p}(k) = n$, then $|k| = p^n$ □

Proposition 3.143. *If k is a field and $I = (p(x))$, where $p(x)$ is a nonzero polynomial in $k[x]$, then the following are equivalent: $p(x)$ is irreducible; $k[x]/I$ is a field; $k[x]/I$ is a domain*

Proof. Assume $p(x)$ is irreducible. Note that $I = (p(x))$ is a proper ideal so that the *one* in $k[x]/I$, namely, $1 + I$ is not zero. If $f(x) + I \in k[x]/I$ is nonzero, then $f(x) \notin I$. Since $p(x)$ is irreducible, by Lemma 3.49, p and f are relatively prime. By Theorem 3.44, there are polynomials s and t s.t. $1 = sp + tf$. Thus $tf - 1 \in I$ and so $1 + I = tf + I = (t + I)(f + I)$. Therefore every nonzero element of $k[x]/I$ has an inverse and so $k[x]/I$ is a field.

If $k[x]/I$ is a domain. If $p(x)$ is not an irreducible polynomial. Then $p(x) = g(x)f(x)$ with $\deg(p) > \deg(g)$, $\deg(p) > \deg(f)$. It follows that $f + I$ and $g + I$ is nonzero but $(f + I)(g + I) = p + I$ is zero, contradicting to the fact that $k[x]/I$ is a domain. □

Proposition 3.144. *Let k be a field, let $p(x) \in k[x]$ be a monic irreducible polynomial of degree d, let $K = k[x]/I$, where $I = (p(x))$, and let $\beta = x + I \in K$*

1. *K is a field and $k' = \{a + I; a \in k\}$ is a subfield of K isomorphic to k*
2. *β is a root of $p(x)$ in K*
3. *if $g(x) \in k[x]$ and β is a root of $g(x)$, then $p(x) \mid g(x)$ in $k[x]$*
4. *$p(x)$ is the unique monic irreducible polynomial in $k[x]$ having β as a root*
5. *The list $1, \beta, \beta^2, \ldots, \beta^{d-1}$ is a basis of K as a vector space over k, and so $\dim_k(K) = d$*

Proof. 2. Note that β is a root in K, suppose $p(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + x^d$, hence

$$\begin{aligned} p(\beta) &= (a_0 + I) + (a_1 + I)\beta + \cdots + (a_{d-1} + I)\beta^{d-1} + (1 + I)\beta^d \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_{d-1} + I)(x + I)^{d-1} + (1 + I)(x + I)^d \\ &= a_0 + a_1x + \cdots + x^d + I = p(x) + I = I \end{aligned}$$

3. If $p(x) \nmid g(x)$, then $p(x)$ and $g(x)$ are relatively prime since $p(x)$ is irreducible. Hence $1 = p(x)s(x) + g(x)t(x)$. Since $k[x] \subseteq K[x]$, we may regard this equation in $K[x]$. Hence $1 = 0$, a contradiction
5. Every element of K has the form $f(x) + I$, where $f(x) \in k[x]$. By the division algorithm, there are $f(x) = g(x)p(x) + r(x)$ with either $r(x) = 0$ or $\deg(r) < d$. We know that $r(\beta) = r + I$, hence $1, \beta, \ldots, \beta^{d-1}$ spans K
   To prove uniqueness, suppose

$$b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1} = c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1}$$

   Define $g(x) = \sum_{i=0}^{d-1}(c_i - b_i)x^i$; if $g(x) = 0$ we are done. Otherwise, then $\deg(g)$ is defined and $\deg(g) < d$. On the other hand, β is a root of $g(x)$ and hence $p(x) \mid g(x)$, a contradiction

□

Definition 3.145. If K is a field containing k as a subfield, then K is called a (field) **extension** of k, and we write "K/k is a field extension"

An extension field K of a field k is a **finite extension** of k if K is a finite-dimensional vector space over k. The dimension of K, denoted by $[K : k]$, is called the **degree** of K/k

Example 3.17. The polynomial $x^2 + 1 \in \mathbb{R}[x]$ is irreducible, and so $K = \mathbb{R}[x]/(x^2 + 1)$ is a field extension $K/\mathbb{R}$ of degree 2. If β is a root of $x^2 + 1$, then $\beta^2 = -1$; moreover, every element of K has a unique expression of the form $a + b\beta$, where $a, b \in \mathbb{R}$. Clearly this is another construction of $\mathbb{C}$.

Consider the evaluation map $\varphi : \mathbb{R}[x] \to \mathbb{C}$ given by $\varphi : f(x) \mapsto f(i)$. First φ is surjective, for $a + ib = \varphi(a + bx) \in \operatorname{im}\varphi$. Second, $\ker\varphi = \{f(x \in \mathbb{R}[x] : f(i) = 0)\}$. We know that $x^2 + 1 \in \ker\varphi$, so that $(x^2 + 1) \subseteq \ker\varphi$. For the reverse inclusion, take $g(x) \in \ker\varphi$. Now i is a root of $g(x)$, and so $\gcd(g, x^2 + 1) \neq 1$ in $\mathbb{C}[x]$; therefore $\gcd(g, x^2 + 1) \neq 1$ in $\mathbb{R}[x]$. Irreducibility of $x^2 + 1$ in $\mathbb{R}[x]$ gives $x^2 + 1 \mid g(x)$ and so $g(x) \in (x^2 + 1)$. Therefore $\ker\varphi = (x^2 + 1)$. The first isomorphism theorem now gives $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$

Definition 3.146. Let K/k be a field extension. An element $\alpha \in K$ is **algebraic** over k if there is some nonzero polynomial $f(x) \in k[x]$ having α as root; otherwise α is **transcendental** over k. An extension K/k is **algebraic** if every $\alpha \in K$ is algebraic over k

Proposition 3.147. *If K/k is a finite field extension, then K/k is an algebraic extension.*

Proof. $[K : k] = n < \infty$. Hence the list of $1, \alpha, \ldots, \alpha^n$ is dependent. Thus there are $c_0, \ldots, c_n \in k$, not all 0, with $\sum c_i\alpha^i = 0$. Thus the polynomial $f(x) = \sum c_i x^i$ is not the zero polynomial, and α is a root of $f(x)$. □

Definition 3.148. If K/k is an extension and $\alpha \in K$, then $k(\alpha)$ is the intersection of all those subfields of K that contain k and α; we call $k(\alpha)$ the subfield of K obtained by **adjoining** α to k

More generally, if A is a (possibly infinite) subset of K, define $k(A)$ to be the intersection of all subfields of K contain $k \cup A$

Theorem 3.149. *1. If K/k is an extension and $\alpha \in K$ is algebraic over k, then there is a unique monic irreducible polynomial $p(x) \in k[x]$ having α as a*

root. Moreover, if $I = (p(x))$*, then* $k[x]/I \cong k(\alpha)$*; indeed, there exists an isomorphism*

$$\varphi : k[x]/I \to k(\alpha)$$

with $\varphi(x + I) = \alpha$ *and* $\varphi(c + I) = c$ *for all* $c \in k$

2. *If* $\alpha' \in K$ *is another root of* $p(x)$*, then there is an isomorphism*

$$\theta : k(\alpha) \to k(\alpha')$$

with $\theta(\alpha) = \alpha'$ *and* $\theta(c) = c$ *for all* $c \in k$

Proof. 1. Consider the evaluation, the ring homomorphism $\varphi : k[x] \to K$ defined by

$$\varphi : f(x) \mapsto f(\alpha)$$

Now $\ker \varphi$ is the ideal in $k[x]$. Since k[x] is an Euclidean ring and hence a PID, we have $\ker \varphi = (p(x))$ for some monic polynomial $p(x) \in k[x]$. But $k[x]/(p(x)) \cong \operatorname{im} \varphi$, which is a domain, and so $p(x)$ is irreducible by Proposition 3.143. The same proposition says that $k[x]/p(x)$ is a field, and so $\operatorname{im} \varphi$ is a subfield of K containing K and α.Since every subfield of K that contains k and α must contain $\operatorname{im} \varphi$, we have $\operatorname{im} \varphi = k(\alpha)$.

2. $k[x]/I \cong k(\alpha)$ and $k[x]/I \cong k(\alpha')$

□

Definition 3.150. If K/k is a field extension and $\alpha \in K$ is algebraic over k, then the unique monic irreducible polynomial $p(x) \in k[x]$ having α as a root is called the **minimal polynomial** of α over k, and it is denoted by

$$\operatorname{irr}(\alpha, k) = p(x)$$

Theorem 3.151. *Let* $k \subseteq E \subseteq K$ *be fields with* E *a finite extension of* k *and* K *a finite extension of* E*. Then* K *is a finite extension of* k*, and*

$$[K : k] = [K : E][E : k]$$

Proof. If $A = a_1, \ldots, a_n$ is a basis of E over k and if $B = b_1, \ldots, b_m$ is a basis of K over E, then it suffices to prove that a list X of all $a_i b_j$ is a basis of K over k □

Example 3.18. Let $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$, then the root are

$$\sqrt{2} + \sqrt{3}, \quad \sqrt{2} - \sqrt{3}, \quad -\sqrt{2} - \sqrt{3}, \quad -\sqrt{2} + \sqrt{3}$$

We claim that $f(x)$ is irreducible in $\mathbb{Q}[x]$. If $g(x)$ is a quadratic factor of $f(x)$ in $\mathbb{Q}[x]$, then

$$g(x) = (x - a\sqrt{2} - b\sqrt{3})(x - c\sqrt{2} - d\sqrt{3})$$

where $a, b, c, d \in \{1, -1\}$. Multiplying

$$g(x) = x^2 - ((a+c)\sqrt{2} + (b+d)\sqrt{3})x + 2ac + 3bd + (ad + bc)\sqrt{6} \notin \mathbb{Q}[x]$$

Therefore $f(x)$ is irreducible in $\mathbb{Q}[x]$. If $\beta = \sqrt{2} + \sqrt{3}$, then $f(x) = \text{irr}(\beta, \mathbb{Q})$

Consider the field $E = \mathbb{Q}(\beta)$. There is a tower of fields $\mathbb{Q} \subseteq E \subseteq F$, where $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and so

$$[F : \mathbb{Q}] = [F : E][E : \mathbb{Q}]$$

Since $f(x)$ is a monic irreducible polynomial, $[E : \mathbb{Q}] = 4$. On the other hand

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

Now $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ because $\sqrt{2}$ is root of $x^2 - 2$. We claim that $[F : \mathbb{Q}(\sqrt{2})] \leq 2$. The field F arises by adjoining $\sqrt{3}$ to $\mathbb{Q}(\sqrt{2})$; either $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, in which case the degree is 1, or $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$, in which the degree is 2. It follows that $[F : \mathbb{Q}] \leq 4$ and so $[F : E] = 1$; that is, $F = E$

Theorem 3.152 (Kronecker)**.** *If k is a field and $f(x) \in k[x]$, then there exists a field K containing k as a subfield and with $f(x)$ a product of linear polynomials in $K[x]$*

Proof. Induction on $\deg(f)$. If $\deg(f) = 1$, then $f(x)$ is linear and we can choose $K = k$. If $\deg(f) > 1$, write $f(x) = p(x)g(x)$ where $p(x)$ is irreducible. Now Proposition 3.144 provides a field F containing k and root z of $p(x)$. Hence in $F[x]$, we have $p(x) = (x - z)h(x)$ and $f(x) = (x - z)h(x)g(x)$. By induction, there is a field K containing F so that $h(x)g(x)$, and hence $f(x)$ is a product of linear factors in $K[x]$ □

Definition 3.153. Let k be a subfield of a field K, and let $f(x) \in k[x]$. We say that $f(x)$ **splits over** K if

$$f(x) = a(x - z_1) \cdots (x - z_n)$$

where $z_1, \ldots, z_n \in K$ and $a \in k$ is nonzero

If $f(x) \in k[x]$ is a polynomial, then a field extension E/k is called a **splitting field** of $f(x)$ **over** k if $f(x)$ splits over E, but $f(x)$ does not split over any proper subfield of E

$f(x) = x^2 + 1 \in \mathbb{Q}[x]$. $f(x)$ splits over $\mathbb{C}$. $\mathbb{Q}(i)$ is a splitting field of $f(x)$ over $\mathbb{Q}$. $\mathbb{R}(i) = \mathbb{C}$ is a splitting field of $f(x)$ over $\mathbb{R}$

Corollary 3.154. *Let k be a field, and let $f(x) \in k[x]$. Then a splitting field of $f(x)$ over k exists.*

Proof. By Kronecker theorem □

Example 3.19. Let $f(x) = x^n - 1 \in k[x]$ for some field k ,and let E/k be a splitting field. In Theorem 3.41, we saw that the group Γ_n of all nth roots of unity in E is a cyclic group: $\Gamma_n = \langle \omega \rangle$, where ω is a primitive nth root of unity.

Proposition 3.155. *Let p be a prime, and let k be a field. If $f(x) = x^p - c \in k[x]$ and α is a pth root of c (in some splitting field), then either $f(x)$ is irreducible in $k[x]$ or c has a pth root in k. In either case, if k contains the pth roots of unity, then $k(\alpha)$ is a splitting field of $f(x)$*

Proof. By Kronecker's theorem, there exists a field extension K/k that contains all the roots of $f(x)$; that is, K contains all the pth roots of c. If $\alpha^p = c$, then every such root has the form $\omega\alpha$, where ω is a pth root of unity.

If $f(x)$ is not irreducible in $k[x]$. Then there is a factorization $f(x) = g(x)h(x)$. Now the constant term b of $g(x)$ is, up to sign, the product of some of the roots of $f(x)$:

$$\pm b = \alpha^d \omega$$

where ω, which is a product of d pth roots of unity, is itself a pth root of unity. It follows that

$$(\pm b)^p = \alpha^{dp} = c^d$$

But p being prime and $d < p$ forces $(d, p) = 1$. hence $1 = sd + tp$, therefore

$$c = c^{sd+tp} = c^{sd} c^{tp} = (\pm b)^{ps} c^{tp} = [(\pm b)^s c^t]^p$$

therefore c has a pth roots of unity. □

Theorem 3.156 (Galois)**.** *If p is a prime and n is a positive integer, then there is a field having exactly p^n elements.*

Proof. Write $q = p^n$, and consider the polynomial

$$g(x) = x^q - x \in \mathbb{F}_p[x]$$

By Kronecker's theorem, there is a field K containing $\mathbb{F}_p$ s.t. $g(x)$ is a product of linear factors in $K[x]$. Define

$$E = \{\alpha \in K : g(\alpha) = 0\}$$

Since the derivative $g'(x) = qx^{q-1} - 1 = p^n x^{q-1} - 1 = -1$ (Exercise 3.2.3), it follows that the $\gcd(g, g')$ is 1. By Exercise 3.3.1, all the roots of $g(x)$ are distinct

We claim that E is a subfield of K, and this will complete the proof. If $a, b \in E$ then $a^q = a$ and $b^q = b$. Therefore $(ab)^q = ab$ and $ab \in E$. By Exercise 3.4.2, $(a-b)^q = a^q - b^q = a - b$, so that $a - b \in E$ □

Corollary 3.157. *For every prime p and every integer $n \geq 1$, there exists an irreducible polynomial $g(x) \in \mathbb{F}_p[x]$ of degree n. In fact, if α is a primitive element of $\mathbb{F}_{p^n}$, then its minimal polynomial $g(x) = \operatorname{irr}(\alpha, \mathbb{F}_p)$*

Proof. Let $E/\mathbb{F}_p$ be an extension field with p^n elements, and let $\alpha \in E$ be a primitive element. Clearly, $\mathbb{F}_p(\alpha) = E$. By Theorem 3.149, $g(x) = \operatorname{irr}(\alpha, \mathbb{F}_p) \in \mathbb{F}_p[x]$ is an irreducible polynomial having α as a root. If $\deg(g) = d$, then Proposition 3.144 gives $[\mathbb{F}_p[x]/(g(x)) : \mathbb{F}_p] = d$; but $\mathbb{F}_p[x]/(g(x)) \cong \mathbb{F}_p(\alpha) = E$ by Theorem 3.149, so that $[E : \mathbb{F}_p] = n$. Therefore $n = d$, and so $g(x)$ is an irreducible polynomial of degree of n □

This corollary can also be proved by counting. If $m = p_1^{e_1} \dots p_n^{e_n}$, define the **Möbius function** by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1 \\ 0 & \text{if any } e_i > 1 \\ (-1)^n & \text{if } 1 = e_1 = e_2 = \cdots = e_n \end{cases}$$

If N_n is the number of irreducible polynomials in $\mathbb{F}_p[x]$ of degree n, then

$$N_n = \frac{1}{n} \sum_{d|n} \mu(d)\, p^{n/d}$$

Example 3.20. 1. Consider a field with four elements:

$$\mathbb{F}_4 = \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in \mathbb{F}_2 \right\}$$

On the other hand, we may construct a field of order 4 as the quotient $F = \mathbb{F}_2[x]/(q(x))$, where $q(x) \in \mathbb{F}_2[x]$ is the irreducible polynomial

$x^2 + x + 1$. By Proposition 3.144, F is a field consisting of all $a + b\beta$, where $\beta = x + (q(x))$ is a root of $q(x)$ and $a, b \in \mathbb{F}_2$. Since $\beta^2 + \beta + 1 = 0$, we have $\beta^2 = -\beta - 1 = \beta + 1$; moreover, $\beta^3 = \beta\beta^2 = \beta(\beta + 1) = \beta^2 + \beta = 1$. There is a ring isomorphism $\varphi : \mathbb{F}_4 \to F$ with $\varphi(\left[\begin{smallmatrix} a & b \\ b & a+b \end{smallmatrix}\right]) = a + b\beta$

2. There are three monic irreducible quadratics in $\mathbb{F}_3[x]$, namely,

$$p(x) = x^2 + 1, \quad q(x) = x^2 + x - 1, \quad r(x) = x^2 - x - 1$$

each give rise to a field with $9 = 3^2$ elements. Let us look at the first two in more detail. Proposition 3.144 says that $E = \mathbb{F}_3[x]/(p(x))$ is given by

$$E = \{a + b\alpha : \text{where } \alpha^2 + 1 = 0\}$$

Similarly, if $F = \mathbb{F}_3[x]/(q(x))$, then

$$F = \{a + b\beta : \text{where } \beta^2 + \beta - 1 = 0\}$$

There two fields are isomorphic. The map $\varphi : E \to F$, defined by $\varphi(a + b\alpha) = a + b(1 - \beta)$

Lemma 3.158. *Let $\varphi : k \to k'$ be an isomorphism of fields, and let $\varphi^* : k[x] \to k'[x]$ be the ring isomorphism: $\varphi^* : g(x) = a_0 + a_1x + \cdots + a_nx^n \mapsto g^*(x) = \varphi(a_0) + \cdots + \varphi(a_n)x^n$. Let $f(x) \in k[x]$ and $f^*(x) = \varphi^*(x) \in k'[x]$. If E is a splitting field of $f(x)$ over k and E' is a splitting field of $f^*(x)$ over k', then there is an isomorphism $\Phi : E \to E'$ extending φ:*

$$\begin{array}{ccc} E & \overset{\Phi}{\dashrightarrow} & E' \\ \big| & & \big| \\ k & \xrightarrow{\varphi} & k' \end{array}$$

Proof. Induction on $d = [E : k]$. If $d = 1$, then $f(x)$ is a product of linear polynomials in $k[x]$. $\Phi = \varphi$

Choose a root z of $f(x)$ in E that is not in k, and let $p(x) = \operatorname{irr}(z, k)$. Now $\deg(p) > 1$ and $[k(z) : k] = \deg(p)$. Let z' be a root of $p^*(x)$ in E', and let $p^*(x) = \operatorname{irr}(z', k')$ be the corresponding monic irreducible polynomial in $k'[x]$.

By a generalization of Proposition 3.149, there is an isomorphism $\widetilde{\varphi} : k(z) \to k'(z')$ extending φ with $\widetilde{\varphi}z \mapsto z$. We may regard $f(x)$ as a polynomial with coefficients in $k(z)$, for $k \subseteq k(z)$ implies $k[x] \subseteq k(z)[x]$. We claim that E is a splitting field of $f(x)$ over $k(z)$; that is

$$E = k(z)(z_1, \ldots, z_n)$$

where $z_1, \ldots, z_n$ are the roots of $f(x)/(x-z)$. Similarly, E' is a splitting field of $f^*(x)$ over $k'(z')$. But $[E : k(z)] < [E : k]$, so that the inductive hypothesis gives an isomorphism $\Phi : E \to E'$ that extends $\widetilde{\varphi}$ □

Theorem 3.159. *If k is a field and $f(x) \in k[x]$, then any two splitting fields of $f(x)$ over k are isomorphic via an isomorphism that fixes k pointwise*

Corollary 3.160 (Moore)**.** *Any two finite fields having exactly p^n elements are isomorphic*

Proof. If E is a field with $q = p^n$ elements, then Lagrange's Theorem applied to the multiplicative group $E^\times$ shows that $a^{q-1} = 1$ for every $a \in E^\times$. It follows that every element of E is a root of $f(x) = x^q - x \in \mathbb{F}_p[x]$, and so E is a splitting field of $f(x)$ over $\mathbb{F}_p$ □

Finite fields are often called **Galois fields**. We speak of the field with q elements, where $q = p^n$ is a power of a prime p, and we denote it by

$$\mathbb{F}_q$$

Exercise 3.7.1. For every commutative ring R, prove that $R[x]/(x) \cong R$

4 Fields

4.1 Insolvability of the Quintic

By Kronecker's theorem, for each monic $f(x) \in k[x]$, where k is a field, there is an extension field K/k and roots $z_1, \ldots, z_n \in K$ with

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - z_1)\ldots(x - z_n)$$

Hence we have

$$\begin{cases} a_{n-1} = -\sum_i z_i \\ a_{n-2} = \sum_{i<j} z_i z_j \\ a_{n-3} = -\sum_{i<j<k} z_i z_j z_k \\ \vdots \\ a_0 = (-1)^n z_1 \ldots z_n \end{cases}$$

Definition 4.1. The **elementary symmetric functions** of n variables are the polynomials, for $j = 1, \ldots, n$

$$e_j(x_1, \ldots, x_n) = \sum_{i_1 < \cdots < i_j} x_{i_1} \ldots x_{i_j}$$

We have

$$e_j(z_1, \ldots, z_n) = (-1)^j a_{n-j}$$

Definition 4.2. Let E be a field containing a subfield k. An **automorphism** of E is an isomorphism $\sigma : E \to E$; we say that σ **fixes** k if $\sigma(a) = a$ for every $a \in k$

Proposition 4.3. *Let k be a subfield of a field K, let*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in k[x]$$

and let $E = k(z_1, \ldots, z_n) \subseteq K$ be a splitting field. If $\sigma : E \to E$ is an automorphism fixing k, then σ permutes the set of root $\{z_1, \ldots, z_n\}$ of $f(x)$

Proof. If r is a root of $f(x)$, then

$$0 = f(r) = r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0$$

Applying σ to this equation gives

$$\begin{aligned} 0 &= \sigma(r)^n + \sigma(a_{n-1})\sigma(r)^{n-1} + \cdots + \sigma(a_0) \\ &= \sigma(r)^n + a_{n-1}\sigma(r)^{n-1} + \cdots + a_0 \\ &= f(\sigma(r)) \end{aligned}$$

Therefore $\sigma(r)$ is a root of $f(x)$ □

Definition 4.4. Let k be a subfield of a field E. The **Galois group** of E over k, denoted by $\mathrm{Gal}(E/k)$, is the set of all those automorphisms of E that fix k. If $f(x) \in k[x]$, and if $E = k(z_1, \ldots, z_n)$ is a splitting field, then the **Galois group** of $f(x)$ over k is defined to be $\mathrm{Gal}(E/k)$

Lemma 4.5. *Let $E = k(z_1, \ldots, z_n)$. If $\sigma : E \to E$ is an automorphism fixing k, that is, if $\sigma \in \mathrm{Gal}(E/k)$, and if $\sigma(z_i) = z_i$ for all i, then σ is the identity 1_E*

Proof. Induction on $n \geq 1$. If $n = 1$, then each $u \in E$ has the form $u = f(z_1)/g(z_1)$, where $f(x), g(x) \in k[x]$ and $g(z_1) \neq 0$. Hence σ fixes all $u \in E$. For the inductive steop, write $K = k(z_1, \ldots, z_{n-1})$ and note that $E = K(z_n)$ □

Theorem 4.6. *If $f(x) \in k[x]$ has degree n, then its Galois group $\mathrm{Gal}(E/k)$ is isomorphic to a subgroup of S_n*

Proof. Let $X = \{z_1, \ldots, z_n\}$. If $\sigma \in \mathrm{Gal}(E/k)$, then Proposition 4.3 shows that its restriction $\sigma|X$ is a permutation of X. Define $\varphi : \mathrm{Gal}(E/k) \to S_X$ by $\varphi : \sigma \mapsto \sigma|X$. This is a homomorphism.

$\mathrm{im}\,\varphi \leq S_X \cong S_n$. Since φ fixes k, $\ker\varphi = \{1\}$. Therefore φ is injective. □

If $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, then complex conjugate σ is an automorphism of its splitting field $\mathbb{Q}(i)$ which fixes $\mathbb{Q}$. Since $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ is a subgroup of the symmetric group S_2, which has order 2, it follows that $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{I}_2$

Lemma 4.7. *If k is a field of characteristic 0, then every irreducible polynomial $p(x) \in k[x]$ has no repeated roots*

Proof. Note Exercise 3.3.1. Either $p'(x) = 0$ or $\deg(p') < \deg(p)$. Since $p(x)$ is irreducible, it not a constant and so it has some nonzero monomial $a_i x^i$ where $i \geq 1$. Therefore $i a_i x^{i-1}$ is a nonzero monomial in $p'(x)$, because k has characteristic 0, and so $p'(x) \neq 0$. Finally, since $p(x)$ is irreducible, its only divisors are constant and associates; as $p'(x)$ has smaller degree, $\gcd(p', p) = 1$ □

Definition 4.8. Let E/k be an algebraic extension. An *irreducible* polynomial $p(x)$ is **separable** if it has no repeated roots. An arbitrary polynomial $f(x)$ is **separable** if each of its irreducible factor has no repeated roots.

An element $\alpha \in E$ is called **separable** if either α is transcendental over k or if α is algebraic over k and its minimal polynomial $\mathrm{irr}(\alpha, k)$ has no repeated roots

A field extension E/k is called a **separable extension** if each of its elements is separable

Lemma 4.7 shows that every extension of a field of characteristic 0 is a separable extension. If E is a finite field with p^n elements, then Lagrange's theorem (for the multiplicative group $E^\times$) shows that every element of E is a root of $x^{p^n} - x$. We saw in the proof of Theorem 3.156 that $x^{p^n} - x$ has no repeated roots. It follows that if $k \subseteq E$, then E/k is a separable extension, for if $\alpha \in E$, then $\mathrm{irr}(\alpha, k)$ is a divisor of $x^{p^n} - x$

Example 4.1. Example of an inseparable extension. Let $k = \mathbb{F}_p(t) = \mathrm{Frac}(\mathbb{F}_p[t])$, and let $E = k(\alpha)$, where α is a root of $f(x) = x^p - t$. In $E[x]$ we have

$$f(x) = x^p - t = x^p - \alpha^p = (x - \alpha)^p$$

If we show that $\alpha \notin k$, then $f(x)$ is irreducible, by Proposition 3.155, and so $f(x) = \text{irr}(\alpha, k)$ is an inseparable polynomial. Therefore E/k is an inseparable extension

If $\alpha \in k$, then $\alpha = g(t)/h(t)$. Hence $g = \alpha h$ and $g^p = \alpha^p h^p = t h^p$, so that

$$\deg(g^p) = \deg(t h^p) = 1 + \deg(h^p)$$

But $p \mid \deg(g^p)$ and $p \mid \deg(h^p)$

Theorem 4.9. *1. Let E/k be a splitting field of a separable polynomial $f(x) \in k[x]$, let $\varphi : k \to k'$ be a field isomorphism, and let E'/k' be a splitting field of $f^*(x) \in k'[x]$ (where $f^*(x)$ is obtained from $f(x)$ by applying φ to its coefficients)*

$$\begin{array}{ccc} E & \overset{\Phi}{\dashrightarrow} & E' \\ | & & | \\ k & \xrightarrow{\varphi} & k' \end{array}$$

Then there are exactly $[E : k]$ isomorphisms $\Phi : E \to E'$ that extend φ

2. If E/k is a splitting field of a separable $f(x) \in k[x]$, then

$$\left|\text{Gal}(E/k)\right| = [E : k]$$

Proof. 1. Induction on $[E : k]$. If $[E : k] = 1$, then $E = k$ and there is only one extension. If $[E : k] > 1$, let $f(x) = p(x)g(x)$, where $p(x)$ is an irreducible factor of largest degree, say d. We may assume $d > 1$, otherwise $f(x)$ splits over k and $[E : k] = 1$. Choose a root α of $p(x)$. If $\widetilde{\varphi} : k(\alpha) \to E'$ is any extension of φ, then $\varphi(\alpha)$ is a root α' of $p^*(x)$, by Proposition 4.3. Since $f^*(x)$ is separable, $p^*(x)$ has exactly d roots $\alpha' \in E'$; by Lemma 4.5 and Theorem 3.149, there are exactly d isomorphisms $\widetilde{\varphi} : k(\alpha) \to k'(\alpha')$ extending φ, for each α'. Now E is also a splitting field of $f(x)$ over $k(\alpha)$, because adjoining all the roots of $f(x)$ to $k(\alpha)$; similarly, E^* is a splitting field of $f^*(x)$ over $k'(\alpha)$. Now $[E : k(\alpha)] < [E : k]$ because $[E : k(\alpha)] = [E : k]/d$ ($1, \alpha, \ldots, \alpha^{d-1}$ is an basis by Proposition 3.144), so that induction shows that each of the d isomorphisms $\widehat{\varphi}$ has exactly $[E : k]/d$ extensions $\Phi : E \to E^*$. Thus we have constructed $[E : k]$ isomorphisms extending φ. But there are no others, because every τ extending φ has $\tau|k(\alpha) = \widehat{\varphi}$ for some $\widehat{\varphi} : k(\alpha) \to k'(\alpha^*)$

2. take $k = k'$, $E = E^*$, $\varphi = 1_k$

□

Corollary 4.10. *Let E/k be a splitting field of a separable polynomial $f(x) \in k[x]$ of degree n. If $f(x)$ is irreducible, then $n \mid \left|\mathrm{Gal}(E/k)\right|$*

Proof. By Theorem 4.9, $\left|\mathrm{Gal}(E/k)\right| = [E : k]$. Let $\alpha \in E$ be a root of $f(x)$. Since $f(x)$ is irreducible, $[k(\alpha) : k] = n$, and

$$[E : k] = [E : k(\alpha)][k(\alpha) : k] = n[E : k(\alpha)]$$

□

Proposition 4.11. *The polynomial $f(x) = x^4 + 1$ is irreducible in $\mathbb{Q}[x]$, yet it factors in $\mathbb{F}_p[x]$ for every prime p*

Proof. To see that $f(x)$ is irreducible, it suffices to show that $f(x-1)$ is irreducible by Lemma 6.33. But $f(x-1) = x^4 - 4x^3 + 6x^2 - 4x + 2$ is irreducible, by Eisenstein's Criterion.

We now show for all prime p, that $x^4 + 1$ factors in $\mathbb{F}_p[x]$. If $p = 2$, then $x^4 + 1 = (x+1)^4$ and so we may assume that p is an odd prime. It is easy to check that every square n^2 is congruent to $0, 1$ or $4 \mod 8$; since p is odd, we must have $p^2 \equiv 1 \mod 8$. Therefore, $\left|(\mathbb{F}_{p^2})^\times\right| = p^2 - 1$ is divisible by 8. But $(\mathbb{F}_{p^2})^\times$ is a cyclic group, by Theorem 3.41, and so it has a (cyclic) subgroup of order 8, by Lemma 2.79. It follows that $(\mathbb{F}_{p^2})$ contains all the 8th roots of unity; in particular, $\mathbb{F}_{p^2}$ contains all the roots of $x^4 + 1$. Hence, the splitting field E_p of $x^4 + 1$ over $\mathbb{F}_p$ is $\mathbb{F}_{p^2}$, and so $[E_p : \mathbb{F}_p] = 2$ $(qp + r)$. Since $x^4 + 1$ is irreducible in $\mathbb{F}_p[x]$, then $4 \mid [E_p : \mathbb{F}_p]$, by Corollary . Therefore, $x^4 + 1$ factors in $\mathbb{F}_p[x]$ for every prime p. □

Example 4.2.

1. Let $f(x) = x^3 - 1 \in \mathbb{Q}[x]$. Now $f(x) = (x-1)(x^2+x+1)$. Suppose roots of $x^2 + x + 1$ is ω and $\overline{\omega}$. The splitting field of $f(x)$ is $\mathbb{Q}(\omega)$, for $\omega^2 = \overline{\omega}$, and so $[\mathbb{Q}(\omega), \mathbb{Q}] = 2$. Therefore $\left|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})\right| = 2$. It's nontrivial element is complex conjugation.
2. Let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Now $f(x)$ is irreducible with roots $\pm\sqrt{2}$, so that $E = \mathbb{Q}(\sqrt{2})$ is a splitting field. $\left|\mathrm{Gal}(E/\mathbb{Q})\right| = 2$. Now every element of E has a unique expression of the form $a + b\sqrt{2}$.
3. Let $g(x) = x^3 - 2 \in \mathbb{Q}[x]$. The roots of $g(x)$ are $\beta, \omega\beta, \omega^2\beta$, where $\beta = \sqrt[3]{2}$ and ω is a primitive cube root of unity. The splitting field of $g(x)$ is $E = \mathbb{Q}(\beta, \omega)$. Now that

   $$[E : \mathbb{Q}] = [E : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = 3[E : \mathbb{Q}(\beta)]$$

   for $g(x)$ is irreducible over $\mathbb{Q}$. Now $E \neq \mathbb{Q}(\beta)$ for every element in $\mathbb{Q}(\beta)$ is real. Therefore $[E : \mathbb{Q}] = \left|\mathrm{Gal}(E/\mathbb{Q})\right| > 3$. On the other hand,

we know that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to S_3, and so we must have $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$

4. We examined $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ which is irreducible; in fact, $f(x) = \mathrm{irr}(\beta, \mathbb{Q})$, where $\beta = \sqrt{2} + \sqrt{3}$. If $E = \mathbb{Q}(\beta)$, then $[E : \mathbb{Q}] = 4$; moreover E is a splitting field of $f(x)$. It follows that $|G| = \left|\mathrm{Gal}(E/\mathbb{Q})\right| = 4$; hence either $G \cong \mathbb{I}_4$ or $G \cong \mathbf{V}$. Actually $G \cong \mathbf{V}$

Proposition 4.12. *If m is a positive integer, k is a field, and E is a splitting field of $x^m - 1$ over k, then* $\mathrm{Gal}(E/k)$ *is abelian; in fact,* $\mathrm{Gal}(E/k)$ *is isomorphic to a subgroup of the group of units $U(\mathbb{I}_m) = \{[i] \in \mathbb{I}_m : (i, m = 1\}\}q$*

Proof. By Example 3.19, $E = k(\omega)$, where ω is a primitive mth root of unity. The group Γ_m of all roots of $x^m - 1$ in E is cyclic and if $\sigma \in \mathrm{Gal}(E/k)$, then its restriction to (Γ_m) is an automorphism of Γ_m. Hence $\sigma(\omega) = \omega^i$ must also be a generator of Γ_m; that is, $(i, m) = 1$, by Theorem 2.33. i is uniquely determined mod m, so that the function $\theta : \mathrm{Gal}(k(\omega)/k) \to U(\mathbb{I}_m)$ is well-defined. θ is homomorphism.

Therefore, Lemma 4.5 shows that θ is injective □

Theorem 4.13. *If p is prime, then*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{I}_n$$

and a generator is the ***Frobenius automorphism*** $\mathrm{Fr} : u \mapsto u^p$

Proof. Let $q = p^n$ and $G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Since $\mathbb{F}_q$ has characteristic p, we have $(a + b)^p = a^p + b^p$, and so the Frobenius Fr is a homomorphism of fields. As any homomorphism of fields, Fr is injection; as $\mathbb{F}_q$ is finite, Fr must be an automorphism, by the Pigeonhole principle; that is, $\mathrm{Fr} \in G$ (Fr fixes $\mathbb{F}_p$, by Fermat's Theorem)

If $\pi \in \mathbb{F}_q$ is a primitive element, then $d(x) = \mathrm{irr}(\pi, \mathbb{F}_p)$ has degree n, by Corollary 3.157. It suffices to prove that the order j of Fr is not less than n. But if $\mathrm{Fr}^j = 1_{\mathbb{F}_q}$ for $j < n$, then $u^{p^j} = u$ for all of the $q = p^n$ elements $u \in \mathbb{F}_q$, giving too many roots of the polynomial $x^{p^j} - x$ □

Proposition 4.14. *Let k be a field, let $f(x) \in k[x]$, and let E/k be a splitting field of $f(x)$. If $f(x)$ has no repeated roots, then $f(x)$ is irreducible if and only if* $\mathrm{Gal}(E/k)$ *acts transitively on the roots of $f(x)$.*

Proof. Assume that $f(x)$ is irreducible, and let $\alpha, \beta \in E$ be roots of $f(x)$. By Theorem 3.149, there is an isomorphism $\varphi : k(\alpha) \to k(\beta)$ with $\varphi(\alpha) = \beta$ which fixes k. Lemma 3.158 shows that φ extends to an automorphism Φ

of E that fixes k; that is, $\Phi \in \mathrm{Gal}(E/k)$. Now $\Phi(\alpha) = \varphi(\alpha) = \beta$, and so $\mathrm{Gal}(E/k)$ acts transitively on the roots.

Assume that $\mathrm{Gal}(E/k)$ acts transitively on the roots of $f(x)$. Let $f(x) = p_1(x) \dots p_t(x)$ be a factorization into irreducibles in $k[x]$, where $t \geq 2$. Choose a root $\alpha \in E$ of $p_1(x)$ and a root $\beta \in E$ of $p_2(x)$. By hypothesis, there is $\sigma \in \mathrm{Gal}(E/k)$ with $\sigma(\alpha) = \beta$. Now σ permutes the roots of $p_1(x)$, contradicting β not being a root of $p_1(x)$ □

The analogy

Polygon Ω ..... polynomial $f(x) \in k[x]$
Regular polygon ..... irreducible polynomial
Vertices of Ω ..... roots of $f(x)$
Plain ..... splitting field E of $f(x)$
Motion ..... automorphism fixing k
Symmetry group $\Sigma(\Omega)$ ..... Galois group $\mathrm{Gal}(E/k)$

Classical Formulas and Solvability by Radicals

Definition 4.15. A **pure extension** of **type** m is an extension field $k(u)/k$, where $u^m \in k$ for some $m \geq 1$. An extension field K/k is a **radical extension** if there is a tower of intermediate fields

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = K$$

in which each K_{i+1}/K_i is a pure extension

Every pure extension is a radical extension. If $u^m = a \in k$, then $k(u)$ arises from k by adjoining an mth root of a. If $k \subseteq \mathbb{C}$, there are m different mth roots of a, namely, $u, \omega u, \dots, \omega^{m-1}u$, where $\omega = e^{2\pi i/m}$ is a primitive mth root.

Definition 4.16. Let $f(x) \in k[x]$ have a splitting field E. We say that $f(x)$ is **solvable by radicals** if there is a radical extension

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

where $E \subseteq K_t$

Example 4.3. 1. For every field k and every $n \geq 1$, we show that $f(x) = x^n - 1 \in k[x]$ is solvable by radicals. A splitting field of $x^n - 1$ is $E = k(\omega)$

2. Let p be a prime and let k contain all pth roots of unity. If $k(u)/k$is a pure extension of type p, then we claim that $k(u)$ is a splitting field of $f(x) = x^p - u^p$. If k has characteristic p, then $x^p - u^p = (x-u)^p$, and $f(x)$ splits over $k(u)$; otherwise, k contains a primitive pth root of unity, ω, and $f(x) = \prod_i (x - \omega^i u)$. Note that $f(x)$ is separable if characteristic $k \neq p$

1. Quadratics If $f(x) = x^b + bx + c$, then the quadratic formula gives its roots as
$$\frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$$
Let $k = \mathbb{Q}(b, c)$. Define $K_1 = k(u)$, where $u = \sqrt{b^2 - c}$. Then K_1 is a radical extension of k, for $u^2 \in k$. Moreover, the quadratic formula implies that K_1 is the splitting field of $f(x)$, and so $f(x)$ is solvable by radicals
2. Cubics Let $f(X) = X^3 + bX^2 + cX + d$, and let $k = \mathbb{Q}(b, c, d)$. Change of variable $X = x - b/3$ yields a new polynomial: $\widetilde{f}(x) = x^3 + qx + r \in k[x]$ having the same splitting field E; it follows that $\widetilde{f}(x)$ is solvable by radicals if and only if $f(x)$ is. The cubic formula gives the roots of $\widetilde{f}(x)$ as
$$g + h, \quad , \omega g + \omega^2 h, \quad w^2 g + \omega h$$
where $g^3 = \frac{1}{2}(-r + \sqrt{R})$, $h = -q/3g$, $R = r^2 + \frac{4}{27}q^3$, and ω is a primitive cube root of unity.
Define $K_1 = k(\sqrt{R})$, $K_2 = K_1(\alpha)$, where $\alpha^3 = \frac{1}{2}(-r + \sqrt{R})$. K_2 contains the root $\alpha + \beta$ of $\widetilde{f}(x)$, where $\beta = -q/3\alpha$. Finally define $K_3 = K_2(\omega)$x

Translation into Group Theory

if $k \subseteq k(u)$ is of type m, then factor $m = p_1 \dots p_q$, where the p's are primes, and replace $k \subseteq k(u)$ by

$$k \subseteq k(u^{m/p_1}) \subseteq k(u^{m/p_1 p_2}) \subseteq \cdots \subseteq k(u)$$

Definition 4.17. An extension field E/k is called **normal** if it is the splitting field of a polynomial in $k[x]$

Theorem 4.18. *Let $k \subseteq B \subseteq E$ be a tower of fields. If B/k and E/k are normal extensions, then $\sigma(B) = B$ for all $\sigma \in \mathrm{Gal}(E/k)$, $\mathrm{Gal}(E/B) \triangleleft \mathrm{Gal}(E/k)$ and*

$$\mathrm{Gal}(E/k)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k)$$

Proof. Since B/k is a normal extension, it is a splitting field of some $f(x)$ in $k[x]$; that is, $B = k(z_1, \ldots, z_t) \subseteq E$, where $z_1, \ldots, z_t$ are the roots of $f(x)$. If $\sigma \in \mathrm{Gal}(E/k)$, the restriction of σ to B permutes the roots and hence $\sigma(B) = B$.

Define $\rho : \mathrm{Gal}(E/k) \to \mathrm{Gal}(B/k)$ by $\sigma \mapsto \sigma|B$. ρ is a homomorphism and $\ker \rho = \mathrm{Gal}(E/B)$; thus, $\mathrm{Gal}(E/B) \lhd \mathrm{Gal}(E/k)$. But ρ is surjective: if $\tau \in \mathrm{Gal}(B/k)$, then Lemma 3.158 applies to show that there is $\sigma \in \mathrm{Gal}(E/k)$ extending τ □

Lemma 4.19. *1. If $B = k(u_1, \ldots, u_t)/k$ is a finite extension field, then there is a normal extension E/k containing B; that is, E is a splitting field of some $f(x) \in k[x]$. If each u_i is separable over k, then $f(x)$ is a separable polynomial and, if $G = \mathrm{Gal}(E/k)$, then*

$$E = k(\sigma(u_1), \ldots, \sigma(u_t) : \sigma \in G)$$

2. If B/k is a radical extension, then the normal extension E/k is a radical extension

Proof. 1. By Theorem 3.149, there are irreducible polynomials $p_i(x) = \mathrm{irr}(u_i, k) \in k[x]$. Define E to be a splitting field of $f(x) = p_1(x) \ldots p_t(x)$ over k. Since $u_i \in E$ for all i, we have $B = k(u_1, \ldots, u_t) \subseteq E$. If each u_i is separable over k, then each $p_i(x)$ is a separable polynomial, and hence $f(x)$ is a separable polynomial.
For each pair of roots u and u' of any $p_i(x)$, Theorem 3.149 gives an isomorphism $\gamma : k(u) \to k(u')$. By Lemma 3.158, each such γ extends to an automorphism $\sigma \in G = \mathrm{Gal}(E/k)$. Thus $f(x)$ splits over $k(\sigma(u_1), \ldots, \sigma(u_t) : \sigma \in G)$. But E/k is a splitting field of $f(x)$ over k and $k(\sigma(u_1), \ldots, \sigma(u_t) : \sigma \in G) \subseteq E$; hence,

$$E = k(\sigma(u_1), \ldots, \sigma(u_t) : \sigma \in G)$$

because a splitting field is the smallest field over which $f(x)$ splits

2. Assume now that $B/k$is a radical extension; say, $B = k(v_1, \ldots, v_s)$, where
$$k \subseteq k(v_1) \subseteq k(v_1, v_2) \subseteq \cdots \subseteq k(v_1, \ldots, v_s) = B$$
and each $k(v_1, \ldots, v_{i+1})/k(v_1, \ldots, v_i)$ is a pure extension; of course, $\sigma(B) = k(\sigma(v_1), \ldots, \sigma(v_s))$ is a radical extension of k for every $\sigma \in G$. Define
$$B_1 = k(\sigma(v_1) : \sigma \in G)$$

Now if $G = \{1, \sigma, \tau, \dots\}$, then the tower

$$k \subseteq k(v_1) \subseteq k(v_1, \sigma(v_1)) \subseteq k(v_1, \sigma(v_1), \tau(v_1)) \subseteq \cdots \subseteq B_1$$

displays B_1 as a radical extension of k. If $v_1^m \in k$, $\tau(v_1)^m = \tau(v_1^m)$ lies in $\tau(k) = k$. Define

$$B_{i+1} = B_i(\sigma(v_{i+1}) : \sigma \in G)$$

Assume, by induction, that B_i/k is a radical extension and that $\sigma(B_i) \subseteq B_i$ for all $\sigma \in G$. Now B_{i+1}/B_i is a radical extension

□

Lemma 4.20. *Let*

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t$$

be a tower with each K_i/K_{i-1} a pure extension of prime type p_i. If K_t/k is a normal extension and k contains all the p_ith roots of unity, for $i = 1, \dots, t$, then there is a sequence of subgroups

$$\mathrm{Gal}(K_t/k) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_t = \{1\}$$

with each $G_{i+1} \triangleleft G_i$, and G_i/G_{i+1} cyclic of prime order p_{i+1} or $\{1\}$

Proof. Define $G_i = \mathrm{Gal}(K_t/K_i)$. Now $K_1 = k(u)$, where $u^{p_1} \in k$; since k contains all the p_1th roots of unity, K_1/k is a splitting field of the polynomial $f(x) = x^{p_1} - u^{p_1}$. Theorem 4.18 now applies: $G_1 = \mathrm{Gal}(K_t/K_1)$ is a normal subgroup of $G_0 = \mathrm{Gal}(K_t/k)$ and $G_0/G_1 \cong \mathrm{Gal}(K_1/k)$. Now Example 4.3 says that if characteristic $k \neq p_1$, then $f(x)$ is separable. By Theorem 4.9, $G_0/G_1 \cong \mathbb{I}_{p_1}$ (K_1 is the splitting field of $f(x)$). If characteristic $k = p_1$, then $G_0/G_1 \cong \mathrm{Gal}(K_1/k) = \{1\}$ □

Definition 4.21. A **normal series** of a group G is a sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_t = \{1\}$$

with each G_{i+1} a normal subgroup of G_i; the **factor groups** of this series are the quotient groups

$$G_0/G_1, G_1/G_2, \dots, G_{t-1}/G_t$$

The **length** of this series is the number of nontrivial factor groups.

A finite group G is called **solvable** if it has a normal series each of whose factor groups has prime order.

In this language, Lemma 4.20 says that $\mathrm{Gal}(K_t/k)$ is a solvable group if K_t is a radical extension of k and k contains appropriate roots of unity.

Example 4.4. 1. S_4 is a solvable group. Consider the chain of subgroups

$$S_4 \supseteq A_4 \supseteq \mathbf{V} \supseteq W \supseteq \{1\}$$

W is any subgroup of $\mathbf{V}$ of order 2.

2. A nonabelian simple group G, for example $G = A_5$ is not solvable, for its only proper normal subgroup is $\{1\}$, and $G/\{1\} \cong G$ is not cyclic of prime order

Lemma 4.22. *Let k be a field, let $f(x) \in k[x]$ be solvable by radicals, and let $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$ be a tower with K_i/K_{i-1} a pure extension of prime type p_i for all i. If K_t contains a splitting field E of $f(x)$ and k contains all the p_ith roots of unity, then the Galois group $\mathrm{Gal}(E/k)$ is a quotient of a solvable group*

Proof. By Lemma 4.19 , we may assume that K_t is a normal extension of k. By Lemma 4.20, $\mathrm{Gal}(K_t/k)$ is a solvable group. Since E and K_t are splitting fields over k, Theorem 4.18 show that $\mathrm{Gal}(K_t/E) \triangleleft \mathrm{Gal}(K_t/k)$ and $\mathrm{Gal}(K_t/k)/\mathrm{Gal}(K_t/E) \cong \mathrm{Gal}(E/k)$ □

Proposition 4.23. *Every quotient of a solvable group G is itself a solvable group*

Proof. Let $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_t = \{1\}$. If $N \triangleleft G$. There is a sequence

$$G = G_0N \supseteq G_1N \supseteq \cdots \supseteq G_tN = N \supseteq \{1\}$$

To see that this is a normal series, we claim that

$$(g_in)G_{i+1}N(g_in)^{-1} \subseteq g_iG_{i+1}Ng_i^{-1} = g_iG_{i+1}g_i^{-1}N \subseteq G_{i+1}N$$

The first inclusion holds because $n(G_{i+1}N)n^{-1} \subseteq NG_{i+1}N \subseteq (G_{i+1}N)(G_{i+1}N) = G_{i+1}N$.

The Second Isomorphism Theorem gives

$$\frac{G_i}{G_i \cap (G_{i+1}N)} \cong \frac{G_i(G_{i+1}N)}{G_{i+1}N} = \frac{G_iN}{G_{i+1}N}$$

Since $G_{i+1} \triangleleft G_i \cap G_{i+1}N$, the Third Isomorphism Theorem gives a surjection $G_i/G_{i+1} \to G_i/[G_i \cap G_{i+1}N]$, and so the composite is a surjection $G_i/G_{i+1} \to G_iN/G_{i+1}N$. As G_i/G_{i+1} is cyclic of prime order, its image is either cyclic of prime order or trivial. Therefore, G/N is a solvable group □

Proposition 4.24. *Every subgroup H of a solvable group G is solvable*

Proof.

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_t = \{1\}$$

Consider the sequence of subgroups

$$H = H \cap G_0 \supseteq H \cap G_1 \supseteq \cdots \supseteq H \cap G_t = \{1\}$$

This is a normal series. The Second Isomorphism Theorem gives

$$\begin{aligned}(H \cap G_i)/(H \cap G_{i+1}) &= (H \cap G_i)/[(H \cap G_i) \cap G_{i+1}] \\ &\cong G_{i+1}(H \cap G_i)/G_{i+1}\end{aligned}$$

But the last quotient is a subgroup of G_i/G_{i+1}. Since the only subgroups of a cyclic group of prime order C and $\{1\}$, it follows that the nontrivial factor groups $(H \cap G_i)/(H \cap G_{i+1})$ are cyclic of prime order. Therefore, H is a solvable group □

Example 4.5. If $n \geq 5$, then the symmetric group S_n is not solvable. Otherwise, each of its subgroups would also be solvable. But $A_5 \supseteq S_5 \supseteq S_n$, and the simple group A_5 is not solvable, by Example 4.4

Proposition 4.25. *If $H \triangleleft G$ and both H and G/H are solvable groups, then G is solvable*

Proof. Since G/H is solvable, there is normal series

$$G/H \supseteq K_1^* \supseteq \cdots \supseteq K_m^* = \{1\}$$

having factor groups of prime order. By the Correspondence Theorem for Groups, there are subgroups $K_i \leq G$

$$G \supseteq K_1 \supseteq \cdots \supseteq K_m = H$$

with $K_i/H = K_i^*$ and $K_{i+1} \triangleleft K_i$. By the Third Isomorphism Theorem

$$K_i^*/K_{i+1}^* \cong K_i/K_{i+1}$$

for all i, and so K_i/K_{i+1} is cyclic of prime order for all i

Since H is solvable, there is a normal series

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_q = \{1\}$$

Splice these two series together

$$G \supseteq K_1 \supseteq \cdots \supseteq K_m = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_q = \{1\}$$

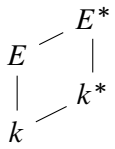
□

Corollary 4.26. *If H and K are solvable groups, then $H \times K$ is solvable*

Proof. $(H \times K)/H \cong K$ □

Theorem 4.27 (Galois)**.** *Let $f(x) \in k[x]$, where k is a field, and let E be a splitting field of $f(x)$ over k. If $f(x)$ is solvable by radicals, then its Galois group* $\mathrm{Gal}(E/k)$ *is a solvable group*

Proof. Let $p_1, \ldots, p_t$ be the types of the pure extensions occurring in the radical extension arising from $f(x)$ being solvable by radicals. Define m to be the product of all these p_i, define E^* to be a splitting field of $x^m - 1$ over E, and define $k^* = k(\Omega)$, where Ω is the set of all mth roots of unity in E^*. Now E^*/k^* is a normal extension, for it is a splitting field of $f(x)$ over k^*, and so $\mathrm{Gal}(E^*/k^*)$ is solvable, by Lemma 4.22 and Proposition 4.23. Consider the tower $k \subseteq k^* \subseteq E^*$



Since k^*/k is normal, Theorem 4.18 gives $\mathrm{Gal}(E^*/k^*) \triangleleft \mathrm{Gal}(E^*/k)$ and

$$\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/k^*) \cong \mathrm{Gal}(k^*/k)$$

NowGal(E^*/k^*) is solvable, while $\mathrm{Gal}(k^*/k)$ is abelian, hence solvable, by Proposition 4.12. Finally, we may use Theorem 4.18 once again, for the tower $k \subseteq E \subseteq E^*$ satisfies the hypothesis that both E and E^* are normal. It follows that $\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/E) \cong \mathrm{Gal}(E/k)$, and so G/k, being a quotient of a solvable group, is solvable □

Theorem 4.28 (Abel-Ruffini)**.** *If $n \geq 5$, the general polynomial*

$$f(x) = (x - y_1)(x - y_2) \cdots (x - y_n)$$

over a field k is not solvable by radicals

Proof. If $E = k(y_1, \ldots, y_n)$ and $F = k(a_0, \ldots, a_{n-1})$ where a_i are the coefficients of $f(x)$, then E is the splitting field of $f(x)$ over F.

We claim that $\mathrm{Gal}(E/F) \cong S_n$. Now if $\sigma \in S_n$, then there is an automorphism $\widetilde{\sigma}$ of $k[y_1, \ldots, y_n]$, defined by $\widetilde{\sigma} : f(y_1, \ldots, y_n) \mapsto f(y_{\sigma 1}, \ldots, y_{\sigma n})$. Thus $\widetilde{\sigma}$ extends to an automorphism σ^* of $E = \mathrm{Frac}(k[y_1, \ldots, y_n])$ and σ^* fixes F; hence $\sigma^* \in \mathrm{Gal}(E/F)$. Since $\sigma \mapsto \sigma^*$ is an injection, $|S_n| \leq \left|\mathrm{Gal}(E/F)\right|$. On the other hand, Theorem 4.6 giving the reverse inequality. Therefore $\mathrm{Gal}(E/F) \cong S_n$. But S_n is not a solvable group if $n \geq 5$, by Example 4.5 □

5 Groups II

5.1 Finite Abelian Groups

Direct Sums

External direct sum, denoted by $S_1 \times \cdots \times S_n$ is the n-tuples $s_1, \ldots, s_n$, where $s_i \in S_i$ for all i, and its binary operation is

$$(s_1, \ldots, s_n) + (s_1', \ldots, s_n') = (s_1 + s_1', \ldots, s_n + s_n')$$

However the most useful version, isomorphic to $S_1 \times \cdots \times S_n$ is called their **internal direct sum**

Definition 5.1. If S and T are subgroups of an abelian group G, then G is the **direct sum**, denoted by

$$G = S \oplus T$$

if $S + T = G$ and $S \cap T = \{0\}$

Proposition 5.2. *The following statements are equivalent for an abelian group G and subgroups S and T of G*

1. $G = S \oplus G$
2. *Every $g \in G$ has a unique expression of the form*

$$g = s + t$$

   where $s \in S$ and $t \in T$
3. *There are homomorphisms $p : G \to S$ and $q : G \to T$, called **projections**, and $i : S \to G$ and $j : T \to G$ called **injections**, s.t.*

$$pi = 1_S, \quad qj = 1_T, \quad pj = 0, \quad qi = 0, \quad ip + jq = 1_G$$

Corollary 5.3. *Let S and T be subgroups of an abelian group G. If $G = S \oplus T$, then $S \oplus T \cong S \times T$*

Conversely, given abelian group S and T, define subgroups $S' \cong S$ and $T' \cong T$ of $S \times T$ by

$$S' = \{(s, 0) : s \in S\} \quad \textit{and} \quad T' = \{(0, t) : t \in T\}$$

then $S \times T = S' \oplus T'$

Definition 5.4. If $S_1, \ldots, S_n, \ldots$ are subgroups of an abelian group G, define the **finite direct sum** $S_1 \oplus \cdots \oplus S_n$ using induction on $n \geq 2$:

$$S_1 \oplus \cdots \oplus S_{n+1} = [S_1 \oplus \cdots \oplus S_n] \oplus S_{n+1}$$

We also denote the direct sum by

$$\sum_{i=1}^{n} S_i = S_1 \oplus \cdots \oplus S_n$$

Example 5.1. Let V be a two-dimensional vector space over a field k, which we view as an additive abelian group, and let x, y be a basis. It's easy to check that the intersection of any two of the subspaces $\langle x \rangle$, $\langle y \rangle$ and $\langle x + y \rangle$ is $\{0\}$. On the other hand, we do not have $V = [\langle x \rangle \oplus \langle y \rangle] \oplus \langle x + y \rangle$ because $[\langle x \rangle \oplus \langle y \rangle] \cap \langle x + y \rangle \neq \{0\}$

In the context of abelian groups, we shall write $S \subseteq G$ to denote S being a subgroup of G.

Proposition 5.5. *Let $G = S_1 + \cdots + S_n$, where the S_i are subgroups. Then the following conditions are equivalent*

1. $G = S_1 \oplus \cdots \oplus S_n$
2. *Every $a \in G$ has a unique expression of the form $a = s_1 + \cdots + s_n$, where $s_i \in S_i$*
3. *For each i*
$$S_i \cap (S_1 + \cdots + \widehat{S_i} + \cdots + S_n) = \{0\}$$
where $\widehat{S_i}$ means that the term S_i is omitted from the sum

Corollary 5.6. *Let $G = \langle y_1, \ldots, y_n \rangle$. If for all $m_i \in \mathbb{Z}$, we have $\sum_i m_i y_i = 0$ implies $m_i y_i = 0$; then*

$$G = \langle y_1 \rangle \oplus \cdots \oplus \langle y_n \rangle$$

Example 5.2. Let V be an n-dimensional vector space over a filed k, which we view as an additive abelian group. If $v_1, \ldots, v_n$ is a basis, then

$$V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle$$

where $\langle v_i \rangle = \{r v_i : r \in k\}$

Proposition 5.7. *If $G_1, \ldots, G_n$ are abelian groups and $H_i \subseteq G_i$ are subgroups, then*

$$(G_1 \oplus \cdots \oplus G_n)/(H_1 \oplus \cdots \oplus H_n) \cong (G_1/H_1) \times \cdots \times (G_n/H_n)$$

If G is an abelian group and m is an integer, let us write

$$mG = \{ma : a \in G\}$$

Proposition 5.8. *If G is an abelian group and p is a prime, then G/pG is a vector space over $\mathbb{F}_p$*

Proof. If $[r] \in \mathbb{F}_p$ and $a \in G$, define scalar multiplication

$$[r](a + pG) = ra + pG$$

□

Definition 5.9. Let $F = \langle x_1, \ldots, x_n \rangle$ be an abelian group. If

$$F = \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$$

where each $\langle x_z \rangle \cong \mathbb{Z}$, then F is called a (finitely generated) **free abelian group** with **basis** $x_1, \ldots, x_n$

Proposition 5.10. *If $\mathbb{Z}^m$ denotes the direct sum of m copies of $\mathbb{Z}$, then $\mathbb{Z}^m \cong \mathbb{Z}^n$ if and only if $m = n$*

Proof. For any abelian group G, if $G = G_1 \oplus \cdots \oplus G_n$, then $2G = 2G_1 \oplus \cdots \oplus 2G_n$. It follows from Proposition 5.7 that

$$G/2G \cong (G_1/2G_1) \oplus \cdots \oplus (G_n/2G_n)$$

so that $|G/2G| = 2^n$. Since $G/2G \cong H/2H$ □

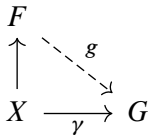
Corollary 5.11. *If F is a (finitely generated) free abelian group, then any two bases of F have the same number of elements*

Proof. If $x_1, \ldots, x_n$ is a basis of F, then $F \cong \mathbb{Z}^n$ □

Definition 5.12. If F is a free abelian group with basis $x_1, \ldots, x_n$, then n is called the **rank** of F, and we write $\text{rank}(F) = n$

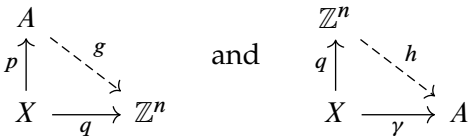
The rank of free abelian group plays the same role as the dimension of a vector space.

Theorem 5.13. *Let F be a free abelian group with basis $X = \{x_1, \ldots, x_n\}$. If G is any abelian group and if $\gamma : X \to G$ is any function, then there exists a unique homomorphism $g : F \to G$ with $g(x_i) = \gamma(x_i)$*



Proposition 5.14. *Let A be an abelian group containing a subset $X = \{x_1, \ldots, x_n\}$, and let A have the property in 5.13. Then $A \cong \mathbb{Z}^n$*

Proof. Consider



□

Basis Theorem

Definition 5.15. If p is a prime, then an abelian group G is **p-primary** if for each $a \in G$, there is $n \geq 1$ with $p^n a = 0$

If G is any abelian group, then its **p-primary component** is

$$G_p = \{a \in G : p^n a = 0 \text{ for some } n \geq 1\}$$

Theorem 5.16 (Primary Decomposition)**.** *1. Every finite abelian group G is a direct sum of its p-primary components*

$$G = G_{p_1} \oplus \cdots \oplus G_{p_n}$$

2. Two finite abelian groups G and G' are isomorphic if and only if $G_p \cong G'_p$ for every prime P

Proof. Let $x \in G$ be nonzero, and let its order be d.

$$d = p_1^{e_1} \ldots p_n^{e_n}$$

Define $r_i = d/p_i^{e_i}$. It follows that $r_i x \in G_{p_i}$. But the gcd of $r_1, \ldots, r_n$ is 1, hence $1 = \sum_i s_i r_i$. Therefore

$$x = \sum_i s_i r_i x \in G_{p_1} + \cdots + G_{p_n}$$

Write $H_i = G_{p_1} + \cdots + \widehat{G_{p_i}} + \cdots + G_{p_n}$. By Proposition 5.5, it suffices to prove that $G_{p_i} \cap H_i = \{0\}$. If $x \in G_{p_i} \cap H_i$, $p_i^l x = 0$, $x = \sum_{j \neq i} y_j$ where

$p_j^{g_j} y_j = 0$. Hence $ux = 0$ where $u = \prod_{j \neq i} p_j^{g_j}$. But p_i^l and u are relatively prime, so $1 = sp_i^l + tu$. Therefore

$$x = (sp_i^l + tu)x = 0$$

□

Definition 5.17. Let p be a prime and let G be a p-primary abelian group. A subgroup $S \subseteq G$ is a **pure subgroup** if for all $n \geq 0$

$$S \cap p^n G = p^n S$$

If $s = p^n g$, then there is a $s' \in S$ s.t. $s = p^n s'$

Example 5.3.
1. Every direct summand S of G is a pure subgroup. Let $G = S \oplus T$ and $s \in S$, and $s \in S$. If $s = p^n(u + v)$ for $u \in S$ and $v \in T$, then $p^n v = s - p^n v \in S \cap T = \{0\}$ and $s = p^n u$
2. If $G = \langle a \rangle$ is a cyclic group of order p^2, where p is a prime, then $S = \langle pa \rangle$ is not a pure subgroup of G, for $s = pa \in S$, but there is no element $s' \in S$ with $s = ps'$

Lemma 5.18. *If p is a prime and G is a finite p-primary abelian group, then G has a nonzero pure cyclic subgroup. If y is an element of largest order in G, then $\langle y \rangle$ is a pure cyclic subgroup*

Proof. Since G is finite, there exists $y \in G$ of largest order, say, p^l. We claim that $S = \langle y \rangle$ is a pure subgroup of G.

If $s \in S$, then $s = mp^t y$, where $t \geq 0$ and $p \nmid m$. Suppose that

$$s = p^n a$$

for some $a \in G$; an element $s' \in G$ with $s = mp^t y = p^n s'$ must be found. We may assume that $n < l$; otherwise $s = p^n a = 0$, and we may choose $s' = 0$.

We claim that $t \geq n$. If $t < n$, then

$$p^l a = p^{l-n} p^n a = l^{l-n} s = p^{l-n} mp^t y = mp^{l-n+t} y$$

But $p \nmid m$ and $l - n + t < l$ and so $p^l a \neq 0$, a contradiction. Thus $t \geq n$, and we can define $s' = mp^{t-n} y$. Now $s' \in S$ and

$$p^n s' = mp^t y = s$$

so that S is a pure subgroup □

Definition 5.19. If p is a prime and G is a finite p-primary abelian group, then

$$d(G) = \dim(G/pG)$$

Observe that d is additive over direct sum,

$$d(G \oplus H) = d(G) + d(H)$$

for Proposition 5.7 gives

$$(G \oplus H)/p(G \oplus H) = (G \oplus H)(pG \oplus pH) \cong (G/pG) \oplus (H/pH)$$

Lemma 5.20. *If G is a finite p-primary abelian group, then $d(G) = 1$ if and only if G is a nonzero cyclic group*

Proof. If G is a nonzero cyclic group, then so is any nonzero quotient of G; in particular, G/pG is cyclic. Now $G/pG \neq \{0\}$, by Exercise 5.1.1, and so $\dim(G/pG) = 1$

Conversely, if $d(G) = 1$, then $G/pG \cong \mathbb{I}_p$; hence G/pG is cyclic, say, $G/pG = \langle z + pG \rangle$. Assume $\langle z \rangle$ is a proper subgroup of G. The Correspondence Theorem says that pG is a maximal subgroup of G. We claim that pG is the only maximal subgroup of G. If $L \subseteq G$ is any maximal subgroup, then $G/L \cong \mathbb{I}_p$ for G/L is a simple abelian group and has order p. It follows that if $a \in G$, then $p(a + L) = 0$ in G/L, and so $pa \in L$; that is, $pG \subseteq L$. But here pG is a maximal subgroup, so that $pG = L$. Every proper subgroup of G is contained in pG. In particular, $\langle z \rangle \subseteq pG$, so that the generator $z + pG$ of G/pG is zero, a contradiction □

Lemma 5.21. *Let G be a finite p-primary abelian group*

1. *If $S \subseteq G$, then $d(G/S) \leq d(G)$*
2. *If S is a pure subgroup of G, then $d(G) = d(S) + d(G/S)$*

Proof. 1. By the Correspondence Theorem, $p(G/S) = (pG + S)/S$, so that

$$(G/S)/p(G/S) = (G/S)/[(pG + S)/S] \cong G/(pG + S)$$

by the Third Isomorphism Theorem. Since $pG \subseteq pG + S$, there is a surjective homomorphism (of vector spaces over $\mathbb{F}_p$)

$$G/pG \to G/(pG + S)$$

. Hence

$$\dim(G)(G/pG) \geq \dim(G/(pG + S)) = d(G/S)$$

2. We now analyze $(pG + S)/pG$, the kernel of $G/pG \to G/(pG + S)$. By the Second Isomorphism Theorem

$$(pG + S)/pG \cong S/(S \cap pG)$$

Since S a pure subgroup, $S \cap pG = pS$; therefore

$$(pG + S)/pG \cong S/pS$$

and so $\dim[(pG + S)/pG] = d(S)$. But if W is a subspace of a finite-dimensional vector space V, then $\dim(V) = \dim(W) + \dim(V/W)$, by Exercise 3.6.1. Hence for $V = G/pG$, $W = (pG + S)/pG$, we have $d(G) = d(S) = d(G/S)$

□

Theorem 5.22 (Basis Theorem)**.** *Every finite abelian group G is a direct sum of primary cyclic groups*

Proof. By the Primary Decomposition, Theorem 5.16, we may assume that G is p-primary for some prime p. □

Exercise 5.1.1. Let G be a p-primary abelian group. If $G = pG$, prove that either $G = \{0\}$ or G is infinite.

Proof. $G = p^k G$ for any $k \geq 0$. If G is finite, then there exists $y \in G$ with largest order l and $p^l G = \{0\} = G$ □

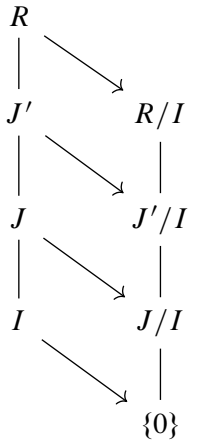
6 Commutative Rings II

6.1 Prime Ideals and Maximal Ideals

Proposition 6.1 (Correspondence Theorem for Rings)**.** *If I is a proper ideal in a commutative ring R, then there is an inclusion-preserving bijection φ from the set of all intermediate ideals J containing I, that is, $I \subseteq J \subseteq R$, to the set of all the ideals in R/I, given by*

$$\varphi : J \mapsto \pi(J) = J/I$$

where π is the natural map



Proof. If we forget its multiplication, the commutative ring R is merely an additive group and its ideal is a (normal) subgroup. Theorem 2.70 gives an inclusion-preserving bijection

$$\Phi : \{\text{all subgroups of } R \text{ containing } I\} \to \{\text{all subgroups of } R/I\}$$

where $\Phi(J) = \pi(J) = J/I$

If J is an ideal, then $\Phi(J)$ is also an ideal. □

In practice, the correspondence theorem is invoked, tacitly, by saying that every ideal in the quotient ring R/I has the form J/I for some ideal J with $I \subseteq J \subseteq R$

Example 6.1. Let $I = (m)$ be a nonzero ideal in $\mathbb{Z}$. If J is an ideal in $\mathbb{Z}$ containing I, then $J = (a)$ for some $a \in \mathbb{Z}$ because $\mathbb{Z}$ is a PID and $(m) \subseteq (a)$ iff $a \mid m$. The correspondence theorem shows that every ideal in $\mathbb{I}_m$ has the form $([a])$ for some divisor a of m

Definition 6.2. An ideal I in a commutative ring R is called a **prime ideal** if it is a proper ideal and $ab \in I$ implies $a \in I$ or $b \in I$

Example 6.2. We claim that the prime ideals in $\mathbb{Z}$ are precisely the ideals (p), where either p is 0 or a prime.

Proposition 6.3. *An ideal I in a commutative ring R is a prime ideal if and only if R/I is a domain*

Proposition 6.4. *If K is a field, then a nonzero polynomial $p(x) \in k[x]$ is irreducible if and only if $(p(x))$ is a prime ideal*

Proof. Suppose that $p(x)$ is irreducible. First $(p(x))$ is a proper ideal. Otherwise $1 \in (p(x))$, so there is a polynomial $f(x)$ with $1 = p(x)f(x)$. But $p(x)$ has degree at least 1

Second, if $ab \in (p)$, then $p \mid ab$, and Euclid's lemma in $k[x]$ gives $p \mid a$ or $p \mid b$ □

Definition 6.5. An ideal I in a commutative ring R is a **maximal ideal** if it is a proper ideal and there is no ideal J with $I \nsubseteq J \nsubseteq R$

Proposition 6.6. *A proper ideal I in a nonzero commutative ring R is a maximal ideal if and only if R/I is a field*

Proof. The correspondence theorem shows that I is maximal if and only if R/I has no ideals other than $\{0\}$ and R/I □

Corollary 6.7. *Every maximal ideal I in a commutative ring R is a prime ideal*

Example 6.3. The converse of Corollary 6.7 is false. Consider the principal ideal (x) in $\mathbb{Z}[x]$. By Exercise 3.7.1

$$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$$

since $\mathbb{Z}$ is a domain, x is a prime ideal. Since $\mathbb{Z}$ is not a field, (x) is not a maximal ideal. Let

$$J = \{f(x) \in \mathbb{Z}[x] : f(x) \text{ has even constant term}\}$$

Since $\mathbb{Z}[x]/J \cong \mathbb{F}_2$ is a field, it follows that J is a maximal ideal containing (x)

Example 6.4. Let k be a field, and let $a = (a_1, \ldots, a_n) \in k^n$. Define the **evaluation map**

$$e_a : k[x_1, \ldots, x_n] \to k$$

by

$$e_a : f(x_1, \ldots, x_n) \mapsto f(a)$$

e_a is a surjective ring homomorphism, and so $\ker e_a$ is a maximal ideal

Theorem 6.8. *If R is a PID, then every nonzero prime ideal I is a maximal ideal*

Proof. Assume that there is a proper ideal J with $I \subseteq J$. Since R is a PID, $I = (a)$ and $I = (b)$ for some $a, b \in R$. Now $a \in J$ implies that $a = rb$ for some $r \in R$ and so $rb \in I$. Since I is prime, either $r \in I$ or $b \in I$. If $r \in I$, then $r = ta$ for some $t \in I$, and $a = tab = atb$. Since R is a domain, $1 = tb$. Hence $J = R$ □

Corollary 6.9. *If k is a field and $p(x) \in k[x]$ is irreducible, then the quotient ring $k[x]/(p(x))$ is a field*

Proof. Since $p(x)$ is irreducible, $(p(x))$ is a prime ideal. Since $k[x]$ is a PID, $(p(x))$ is maximal □

Proposition 6.10. *Let P be a prime ideal in a commutative ring R. If I and J are ideals with $IJ \subseteq P$, then $I \subseteq P$ or $J \subseteq P$*

Proof. Suppose, on the contrary, that $I \nsubseteq P$ and $J \nsubseteq P$; thus there are $a \in I$ and $b \in J$ with $a, b \notin P$. But $ab \in IJ \subseteq P$, contradicting P being prime □

Proposition 6.11. *Let B be a subset of a commutative ring R which is closed under addition and multiplication*

1. *Let $J_1, \ldots, J_n$ be ideals in R, at least $n-2$ which are prime. If $B \subseteq J_1 \cup \cdots \cup J_n$, then B is contained in some J_i*
2. *Let I be an ideal in R with $I \subsetneq B$. If there are prime ideals $P_1, \ldots, P_n$ s.t. $B - I \subseteq P_1 \cup \cdots \cup P_n$, then $B \subseteq P_i$ for some i*

Proof. 1. Induction on $n \geq 2$. If $B \nsubseteq J_2$, then there is $b_1 \in B$ with $b_1 \notin J_2$, and hence $b_1 \in J_1$. If $B \nsubseteq J_1$, there is $b_2 \in B$ with $b_2 \notin J_1$ and $b_2 \in J_2$. However if $y = b_1 + b_2$, then $y \notin J_1$ and $y \notin J_2$, contradicting $B \subseteq J_1 \cup J_2$
For the inductive step, assume that $B \subseteq J_1 \cup \cdots \cup J_{n+1}$, where at least $n - 1 = (n+1) - 2$ of the J_i are prime ideals. Let

$$D_i = J_1 \cup \cdots \cup \widehat{J_i} \cup \cdots \cup J_{n+1}$$

the inductive hypothesis allows us to assume that $B \nsubseteq D_i$ for all i. Hence for all i, there exists $b_i \in B$ with $b_i \notin D_i$; since $B \subseteq D_i \cup J_i$, we must have $b_i \in J_i$. Now $n \geq 3$, so that at least one of the J_i is a prime ideal. Assume J_1 is prime. Consider the elements

$$y = b_1 + b_2 b_3 \ldots b_{n+1}$$

$y \notin J_i$ for any i

2. $B \subseteq I \cup P_1 \cup \cdots \cup P_n$

□

6.2 Unique Factorization Domains

Definition 6.12. Elements a and b in a commutative ring R are **associates** if there exists a unit $u \in R$ with $b = ua$

Proposition 6.13. *Let R be a domain and let $a, b \in R$*
1. *$a \mid b$ and $b \mid a$ if and only if a and b are associates*
2. *The principal ideals (a) and (b) are equal if and only if a and b are associates*

Corollary 6.14. *If R is a PID and $p \in R$ is irreducible, then (p) is a prime ideal*

Proof. (p) is maximal □

Definition 6.15. A domain R is a **unique factorization domain** (**UFD**) if
1. every $r \in R$, neither 0 nor a unit, is a product of irreducibles
2. if $up_1 \dots p_m = vq_1 \dots q_n$, where u and v are units and p_i, q_i are irreducible, then $m = n$ and there is a permutation

$\sigma \in S_n$ with p_i and $q_{\sigma(i)}$ associates for all i

Proposition 6.16. *Let R be a domain in which every $r \in R$, neither 0 nor a unit, is a product of irreducibles. Then R is a UFD if and only if (p) is a prime ideal in R for every irreducible element $p \in R$*

Proof. Assume that R is a UFD. If $a, b \in R$ and $ab \in (p)$, then there is $r \in R$ with

$$ab = rp$$

Factor each of a, b, r into irreducibles; by unique factorization, the left side of the equation must involve an associate of p

Assume that

$$up_1 \dots p_m = vq_1 \dots q_n$$

where p_i and q_j are irreducibles and u, v are units. We prove, by induction on $\max\{m, n\} \geq 1$. If $\max m, n = 1$, then $up_1 = v, u = vq_1$ or $up_1 = vq_1$. The first two cannot happen, and so the base step is true. For the inductive steop, the given equation shows that $p_1 \mid q_1 \dots q_n$. By hypothesis, (p_1) is a prime ideal, and so there is some q_j with $p_1 \mid q_j$, so that p_1 and q_j are associates. Canceling p_1 from both side. □

Lemma 6.17. *1. If R is a commutative ring and*

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$$

is an ascending chain of ideals of R, then $J = \bigcup_{n \geq 1} I_n$ is an ideal in R

2. *If R is a PID, then it has no infinite strictly ascending chain of ideals*

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots$$

3. *Let R be a PID. If $r \in R$ is neither 0 nor a unit, then r is a product of irreducibles*

Proof. 1. If $a \in J$, then $a \in I_n$ for some n; if $r \in R$, then $ra \in I_n$; hence $ra \in J$. If $a, b \in J$, then $a \in I_m$ and $a \in I_n \ldots$

2. J is principal ideal domain and $J = (d)$, then

$$J = (d) \subseteq I_n \subsetneq I_{n+1} \subseteq J$$

3. A divisor r of an element $a \in R$ is called a **proper divisor** of a. Call a nonzero nonunit $a \in R$ **good** if it is a product of irreducibles. If a is bad, then $a = rs$, where both r and s are proper divisors. But the product of good elements is good, and so at least one of the factors, say r, is bad. It follows , by induction, that there exists a sequence $a_1 = a, a_2 = r, a_3, \ldots, a_n, \ldots$ of bad elements and yields a strictly ascending chain

$$(a_1) \subsetneq (a_2) \subsetneq \ldots$$

□

Theorem 6.18. *If R is a PID, then R is a UFD.*

Proposition 6.19. *If R is a UFD, then a gcd of any finite set of elements $a_1, \ldots, a_n$ in R exists*

Proof.

$$a = up_1^{e_1} \ldots p_t^{e_t}$$
$$b = vp_1^{f_1} \ldots p_t^{f_t}$$

where $e_i, f_i \geq 0$ □

Definition 6.20. Elements $a_1, \ldots, a_n$ in a UFD R is called **relatively prime** if their gcd is a unit

Definition 6.21. A polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, where R is a UFD, is called **primitive** if its coefficients are relatively prime

Example 6.5. For a UFD R, every irreducible $p(x) \in R[x]$ of positive degree is primitive.

Lemma 6.22 (Gauss's Lemma)**.** *If R is a UFD and $f(x), g(x) \in R[x]$ are both primitive, then their product $f(x)g(x)$ is also primitive*

Proof. If $\pi : R \to R/(p)$ is the natural map $\pi : a \mapsto a+(p)$, then Proposition 3.63 shows that the function $\widetilde{\pi} : R[x] \to (R/(p))[x]$ is a ring homomorphism. If a polynomial $h(x) \in R[x]$ is not primitive, there is some irreducible p s.t. all the coefficients of $\widetilde{\pi}(h)$ are 0 in $R/(p)$; that is, $\widetilde{\pi}(h) = 0$ in $R/(p)[x]$. Thus, if the product $f(x)g(x)$ is not primitive, there is some irreducible p with $0 = \widetilde{\pi}(fg) = \widetilde{\pi}(f)\widetilde{\pi}(g)$. Since (p) is a prime ideal, $R/(p)$ is a domain, and hence $(R/(p))[x]$ is also a domain. But neither $\widetilde{\pi}(f)$ nor $\widetilde{\pi}(g)$ are 0 in $(R/(p))[x]$, a contradiction □

Lemma 6.23. *Let R be a UFD, let $Q = \mathrm{Frac}(R)$, and let $f(x) \in Q[x]$ be nonzero*

1. *There is a factorization*

$$f(x) = c(f)f^*(x)$$

   where $c(f) \in Q$ and $f^*(x) \in R[x]$ is primitive. This factorization is unique in the sense that if $f(x) = qg^*(x)$, where $q \in Q$ and $g^*(x) \in R[x]$ is primitive, then there is a unit $w \in R$ with $q = wc(f)$ and $g^*(x) = w^{-1}f^*(x)$
2. *If $f(x), g(x) \in R[x]$, then $c(fg)$ and $c(f)c(g)$ are associates in R and $(fg)^*$ and f^*g^* are associates in $R[x]$*
3. *Let $f(x) \in Q[x]$ have a factorization $f(x) = qg^*(x)$, where $q \in Q$ and $g^*(x) \in R[x]$ is primitive. Then $f(x) \in R[x]$ if and only if $q \in R$*
4. *Let $g^*(x), f(x) \in R[x]$. If $g^*(x)$ is primitive and $g^*(x) \mid bf(x)$, where $b \in R$ and $b \neq 0$, then $g^*(x) \mid f(x)$*

Proof. 1. Clearing denominators, there is $b \in R$ with $bf(x) \in R[x]$. If d is the gcd of the coefficients of $bf(x)$, then $(b/d)f(x) \in R[x]$ is a primitive polynomial. If we define $c(f) = d/b$ and $f^*(x) = (b/d)f(x)$ Suppose $c(f)f^*(x) = qg^*(x)$. Exercise 6.2.1 allows use to write $q/c(f)$ in lowest terms: $q/c(f) = u/v$. The equation $vf^*(x) = ug^*(x)$ holds in $R[x]$. Since v, u are relatively prime and $g^*(x)$ is primitive, v is a unit

4. Since $bf = hg^*$, we have $bc(f)f^* = c(h)h^*g^* = c(h)(hg)^*$. By uniqueness, f^* and $(hg)^*$ are associates

□

Definition 6.24. Let R be a UFD with $Q = \mathrm{Frac}(R)$. If $f(x) \in Q[x]$, there is a factorization $f(x) = c(f)f^*(x)$, where $c(f) \in Q$ and $f^*(x) \in R[x]$ is primitive. We call $c(f)$ the **content** of $f(x)$ and $f^*(x)$ the **associated primitive polynomial**

Theorem 6.25 (Gauss)**.** *If R is a UFD, then $R[x]$ is also a UFD*

Proof. We show first, by induction on $\deg(f)$, that every $f(x) \in R[x]$, neither 0 nor a unit, is a product of irreducibles. If $\deg(f) > 0$, then $f(x) = c(f)f^*(x)$ where $c(f) \in R$ and $f^*(x)$ is primitive. If $f^*(x)$ is irreducible, we are done. Otherwise $f^*(x) = g(x)h(x)$, where neither g nor h is a unit. And so each is is a product of irreducibles, by the inductive hypothesis

Now Proposition 6.16 applies: $R[x]$ is a UFD if $(p(x))$ is a prime ideal for every irreducible $p(x) \in R[x]$. Let's assume $p \mid fg$ and $p \nmid f$

Case (i). Suppose that $\deg(p) = 0$. Write

$$f(x) = c(f)f^*(x), \quad g(x) = c(g)g^*(x)$$

Now $p \mid fg$, so that

$$p \mid c(f)c(g)f^*(x)g^*(x)$$

Since $f^*(x)g^*(x)$ is primitive, Lemma 6.23 says that $c(f)c(g)$ is an associate of $c(fg)$. However, if $p \mid fg$, then p divides each coefficient of fg; that is, p is a common divisor of all coefficients of fg, and hence in R, which is a UFD, p divides the associates $c(fg)$ and $c(f)c(g)$. But Proposition 6.16 says that (p) is a prime ideal, and so $p \mid c(f)$ or $p \mid c(g)$. Therefore $p \mid c(g)$

Case (ii). Suppose that $\deg(p) > 0$. Let

$$(p, f) = \{s(x)p(x) + t(x)f(x) : s(x), t(x) \in R[x]\}$$

Choose $m(x) \in (p, f)$ of minimal degree. If $Q = \mathrm{Frac}(R)$ is the fraction field of R, then the division algorithm in $Q[x]$ gives polynomials $q'(x), r'(x) \in Q[x]$ with

$$f(x) = m(x)q'(x) + r'(x)$$

where either $r'(x) = 0$ or $\deg(r') < \deg(m)$. Clearing denominators, there are polynomials $q(x), r(x) \in R[x]$ and a constant $b \in R$ with

$$bf(x) = q(x)m(x) + r(x)$$

Since $m \in (p, f)$, there are polynomials $s(x), t(x) \in R[x]$ with $m = sp + tx$; hence $r = bf - qm \in (b, f)$. Since m has minimal degree, we must have $r = 0$; that is, $bf(x) = q(x)m(x)$, and so $bf(x) = c(m)m*(x)q(x)$. So that $m^*(x) \mid f(x)$ by Lemma 6.23. A similar argument, replacing $f(x)$ by $p(x)$, gives $m^*(x) \mid p(x)$. If $m^*(x)$ were an associate of $p(x)$, then $p(x) \mid f(x)$, contrary to hypothesis. Hence $m^*(x)$ is a unit; that is, $m(x) = c(m) \in R$,

and so p, f contains the nonzero constant $c(m)$. Now $c(m) = sp + tf$, and so

$$c(m)g(x) = s(x)p(x)g(x) + t(x)f(x)g(x)$$

Since $p \mid fg$, we have $p(x) \mid c(m)g(x)$. But $p(x)$ is primitive, $p(x) \mid g(x)$ □

Corollary 6.26. *If k is a field, then $k[x_1, \ldots, x_n]$ is a UFD*

Corollary 6.27 (Gauss)**.** *Let R be a UFD, let $Q = \mathrm{Frac}(R)$, and let $f(x) \in R[x]$. If*

$$f(x) = G(x)H(x) \in Q[x]$$

then there is a factorization

$$f(x) = g(x)h(x) \in R[x]$$

where $deg(g) = deg(G)$ and $deg(h) = deg(H)$; in fact, $G(x)$ is a constant multiple of $g(x)$ and $H(x)$ is a constant multiple of $h(x)$. Therefore, if $f(x)$ does not factor into polynomials of smaller degree in $R[x]$, then $f(x)$ is irreducible in $Q[x]$

Example 6.6. We claim that $f(x, y) = x^2 + y^2 - 1 \in k[x, y]$ is irreducible, where k is a field. Write $Q = k(y) = \mathrm{Frac}(k[y])$, and view $f(x, y) \in Q[x]$. Now the quadratic $g(x) = x^2 + (y^2 - 1)$ is irreducible in $Q[x]$ iff it has no roots in $Q = k(y)$, and this is so by Exercise 3.4.1

It follows from Proposition 6.16 that (x^2+y^2-1) is a prime ideal because it is generated by an irreducible polynomial

Proposition 6.28. *Let k be a field, and view $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ as a polynomial in $R[x_n]$, where $R = k[x_1, \ldots, x_{n-1}]$*

$$f(x_n) = a_0(x_1, \ldots, x_{n-1}) + \cdots + a_m(x_1, \ldots, x_{n-1})x_n^m$$

If $f(x_n)$ is primitive and cannot be factored into two polynomials of lower degree in $R[x_n]$, then $f(x_1, \ldots, x_n)$ is irreducible in $k[x_1, \ldots, x_n]$

Proof. Suppose that $f(x_n) = g(x_n)h(x_n)$ in $R[x_n]$; by hypothesis, the degrees of g and h in x_n cannot both be less than $\deg(f)$; say, $\deg(g) = 0$. It follows, because f is primitive, that g is a unit in $k[x_1, \ldots, x_{n-1}]$. Therefore, $f(x_1, \ldots, x_n)$ is irreducible in $R[x_n]$ □

Corollary 6.29. *If k is a field and $g(x_1, \ldots, x_n), h(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ are relatively prime, then $f(x_1, \ldots, x_n, y) = yg(x_1, \ldots, x_n) + h(x_1, \ldots, x_n)$ is irreducible in $k[x_1, \ldots, x_n, y]$*

Proof. Let $R = k[x_1, \ldots, x_n]$. Note that f is primitive in $R[y]$, because $(g, h) = 1$ forces any divisor of its coefficients g, h to be a unit. Since f is linear in y, it is not the product of two polynomials in $R[y]$ of smaller degree, and hence Proposition 6.28 shows that f is irreducible in $R[y] = k[x_1, \ldots, x_n, y]$ □

Example 6.7. The polynomials x and $y^2 + z^2 - 1$ are relatively prime in $\mathbb{R}[x, y, z]$, so that $f(x, y, z) = x^2 + y^2 + z^2 - 1$ is irreducible

Corollary 6.30. *If α is an algebraic integer, then* $\operatorname{irr}(\alpha, \mathbb{Q})$ *lies in* $\mathbb{Z}[x]$

Definition 6.31. If α is an algebraic integer, then its **minimal polynomial** is the monic polynomial in $\mathbb{Z}[x]$ of least degree having α as a root.

Remark. We define the (algebraic) **conjugates** of α to be the roots of $\operatorname{irr}(\alpha, \mathbb{Q})$, and we define the **norm** of α to be the absolute value of the product of the conjugates α

Theorem 6.32. *Let $f(x) = a_0 + a_1 x + \cdots + x^n \in \mathbb{Z}[x]$ be monic, and let p be a prime. If $f(x)$ is irreducible* $\bmod p$*, that is, if*

$$\widetilde{f}(x) = [a_0] + [a_1]x + \cdots + x^n \in \mathbb{F}_p[x]$$

is irreducible, then $f(x)$ is irreducible in $\mathbb{Q}[x]$

Proof. By Proposition 3.63, the natural map $\varphi : \mathbb{Z} \to \mathbb{F}_p$ defines a homomorphism $\widetilde{\varphi} : \mathbb{Z}[x] \to \mathbb{F}_p$. If $g(x) \in \mathbb{Z}[x]$, define its image $\widetilde{\varphi}(g(x)) \in \mathbb{F}_p[x]$ by $\widetilde{g}(x)$. Prove $f(x)$ is irreducible in $\mathbb{Z}[x]$. Then by Gauss's theorem, $f(x)$ is irreducible in $\mathbb{Q}[x]$ □

Exercise 6.2.1. Let R be a UFD and let $Q = \operatorname{Frac} R$ be its fraction field. Prove that each nonzero $a/b \in Q$ has an expression in lowest terms; that is, a and b are relatively prime.

Proof. there gcd exists □

Exercise 6.2.2. Let R be a UFD

1. If $a, b, c \in R$ and a and b are relatively prime, prove that $a \mid bc$ implies $a \mid c$
2. If $a, c_1, \ldots, c_n \in R$ and $c_i \mid a$ for all i, prove that $c \mid a$, where $c = \operatorname{lcm}\{c_1, \ldots, c_n\}$

Example 6.8. 1. We show that $f(x) = x^4 - 5x^3 + 2x + 3$ is an irreducible polynomial in $\mathbb{Q}[x]$
The only candidates for rational roots are $1, -1, 3, -3$ and none of these is a root.
Since $\widetilde{f}(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ is irreducible by Example 3.4, it follows that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
2. Let $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$
$\widetilde{\Phi}_5(x)$ is irreducible in $\mathbb{F}_2[x]$, and so $\Phi_5(x)$ is irreducible in $\mathbb{Q}[x]$

Lemma 6.33. *Let $g(x) \in \mathbb{Z}[x]$. If there is $c \in \mathbb{Z}$ with $g(x+c)$ irreducible in $\mathbb{Z}[x]$, then $g(x)$ is irreducible in $\mathbb{Q}[x]$*

Proof. $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]$, given by $f(x) \mapsto f(x+c)$ is an isomorphism. If $g(x) = s(x)t(x)$, then $g(x+c) = \varphi(g(x)) = \varphi(s)\varphi(t)$. Therefore $g(x)$ is irreducible in $\mathbb{Q}$. □

Theorem 6.34 (Eisenstein Criterion)**.** *Let R be a UFD with $Q = \mathrm{Frac}(R)$, and let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. If there is an irreducible element $p \in R$ with $p \mid a_i$ for all $i < n$ but with $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible in $Q[x]$*

Proof. Let $\widetilde{\varphi} : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ and let $\bar{f}(x)$ denote $\widetilde{\varphi}(f(x))$. If $f(x)$ is not irreducible in $\mathbb{Q}[x]$, then Gauss's Theorem gives polynomials $g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$, where $g(x) = b_0 + \cdots + b_m x^m$, $h(x) = c_0 + \cdots + c_k x^k$. Thus $\bar{f} = \bar{g}\bar{h}$.

Since $p \nmid a_n$, we have $\bar{f}(x) \neq 0$; in fact, $\bar{f}(x) = ux^n$ for some unit $u \in \mathbb{F}_p$, because all its coefficients aside from its leading coefficient are 0. By unique factorization in $\mathbb{F}_p[x]$, we must have $\bar{g}(x) = vx^m$ and $\bar{h}(x) = wx^k$ (for units $v, w \in \mathbb{F}_p$); equivalently, $p \mid b_0$ and $p \mid c_0$. But $a_0 = b_0 c_0$, and so $p^2 \mid a_0$, a contradiction. □

6.3 Noetherian Rings

Definition 6.35. A commutative ring R satisfies the **ACC**, the **ascending chain condition**, if every ascending chain of ideals

$$I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

stops.

Definition 6.36. If X is a subset of a commutative ring R, then the **ideal generated by** X is the set of all finite linear combinations

$$I = (X) = \{\sum_{\text{finite}} r_i x_i : r_i \in R, x_i \in X\}$$

We say that I is **finitely generated**, often abbreviated to f.g., if $X = \{a_1, \ldots, a_n\}$. We write

$$I = (a_1, \ldots, a_n)$$

and we call I the **ideal generated by** $a_1, \ldots, a_n$

A set of generators $a_1, \ldots, a_n$ of an ideal I is sometimes called a **basis** of I

Proposition 6.37. *The following conditions are equivalent for a commutative ring R*

1. *R has the ACC*
2. *R satisfies the **maximum condition**: Every nonempty family $\mathcal{F}$ of ideals of R has a maximal element*
3. *Every ideal in R is finitely generated*

Proof. (2) $\to$ (3). Let I be an ideal in R, and define $\mathcal{F}$ to be the family of all the finitely generated ideals in I; of course, $\mathcal{F} \neq \emptyset$. By hypothesis, there exists a maximal element $M \in \mathcal{F}$. If $M \subsetneq I$, then there is $a \in I$ with $a \notin M$. The ideal

$$J = \{m + ra : m \in M, r \in R\} \subseteq I$$

is finitely generated, and so $J \in \mathcal{F}$ □

Definition 6.38. A commutative ring R is called **noetherian** if every ideal in R is finitely generated

Corollary 6.39. *If I is a proper ideal in a noetherian ring R, then there exists a maximal ideal M in R containing I.*

Corollary 6.40. *If R is a noetherian ring and I is an ideal in R, then R/I is also noetherian*

Proof. Correspondence theorem □

Theorem 6.41 (Hilbert Basis Theorem)**.** *If R is a commutative noetherian ring, then $R[x]$ is also noetherian*

Proof. Assume that I is an ideal in $R[x]$ that is not finitely generated, $I \neq \{0\}$. Define $f_0(x)$ to be a polynomial in I of minimal degree and define, inductively, $f_{n+1}(x)$ to be a polynomial of minimal degree in $I - (f_0, \ldots, f_n)$. It is clear that

$$\deg(f_0) \leq \deg(f_1) \leq \cdots$$

Let a_n denote the leading coefficient of $f_n(x)$. Since R is noetherian, Exercise 6.3.1 applies to give an integer m with $a_{m+1} \in (a_1, \ldots, a_m)$. Define

$$f^*(x) = f_{m+1}(x) - \sum_{i=0}^{m} x^{d_{m+1}-d_i} r_i f_i(x)$$

where $d_i = \deg(f_i)$. Now $f^*(x) \in I - (f_0, \ldots, f_m)$. It suffices to show that $\deg(f^*) < \deg(f_{m+1})$, for this contradicts $f_{m+1}(x)$ having minimal degree. □

Corollary 6.42. *1. If k is a field, then $k[x_1, \ldots, x_n]$ is noetherian*
2. The ring $\mathbb{Z}[x_1, \ldots, x_n]$ is noetherian
3. For any ideal I in $k[x_1, \ldots, x_n]$ where $k = \mathbb{Z}$ or k is a field, the quotient ring $k[x_1, \ldots, x_n]/I$ is noetherian

Exercise 6.3.1. Let R be a commutative ring. Prove that R is noetherian if and only if for every sequence $a_1, \ldots, a_n, \ldots$ of elements in R ,there is an integer $m \geq 1$ with a_{m+1} an R-linear combination of its predecessors

Proof. $(a_1), (a_1, a_2), (a_1, a_2, a_3), \ldots$ □

6.4 Application of Zorn's Lemma

Definition 6.43. If A is a set, let $\mathcal{P}(A)^{\#}$ denote the family of all its nonempty subsets. The **axiom of choice** states that if A is a nonempty set, then there exists a function $\beta : \mathcal{P}(A)^{\#} \to A$ with $\beta(S) \in S$ for every nonempty subset S of A. Such a function β is called a **choice function**

Definition 6.44. A partially ordered set X is **well-ordered** if every nonempty subset S of X contains a **smallest element**;

Well-ordering principle. *Every set X has some well-ordering of its elements*

Zorn's lemma. *If X is a nonempty partially ordered set in which every chain has an upper bound in X, then X has a maximal element*

Theorem 6.45. *The following statements are equivalent*
1. Zorn's lemma
2. The well-ordering principle
3. The axiom of choice

Proposition 6.46. *If C is a chain and $S = \{x_1, \ldots, x_n\} \subseteq C$, then there exists some x_i, for $1 \leq i \leq n$, with $x_j \preceq x_i$ for all $x_j \in S$*

Proof. Induction on $n \geq 1$ □

Theorem 6.47. *If R is a nonzero commutative ring, then R has a maximal ideal. Indeed, every proper ideal I in R is contained in a maximal ideal*

Proof. Let X be the family of all the proper ideals containing I and partially ordered by inclusion. □

Definition 6.48. Let V be a vector space over some field k, and let $Y \subseteq V$ be an infinite subset

1. Y is **linearly independent** if every finite subset of Y is linearly independent
2. Y **spans** V if each $v \in V$ is a linear combination of finitely many elements of Y. We write $V = \langle Y \rangle$
3. A **basis** of a vector space V is linearly independent subset that spans V

Theorem 6.49. *Every vector space V over a field F has a basis. Indeed, every linearly independent subset B of V is contained in a basis of V; that is, there is a subset B' so that $B \cup B'$ is a basis of V*

Proof. Let X be the family of all the linearly independent subsets of V that contain B. The family X is nonempty, for $B \in X$. Let $\mathcal{B} = \{B_j : j \in J\}$ be a chain of X. It follows from Proposition 6.46 that if $B_{j_1}, \ldots, B_{j_n}$ is any *finite* family of B_j's, then one contains all of the others.

Let $B^* = \bigcup_{j \in J} B_j$. Clearly, B^* contains B and $B_j \subseteq B^*$. Thus B^* is an upper bound of $\mathcal{B}$ if it belongs to X. If B^* is not linearly independent, then it has a finite subset $y_{i_1}, \ldots, y_{i_m}$ that is linearly dependent and $y_{i_k} \in B_{j_k}$ for some index j_k. Since there only finitely many y_{i_k}, there exists B_{j_0} that $y_{i_1}, \ldots, y_{i_m} \in B_{j_0}$. Hence Zorn's lemma applies to say that there is a maximal element in X

Let M be a maximal element in X. Since M is linear independent, it suffices to show that M spans V. If M does not span V, then there is $v_0 \in V$ with $v_0 \notin \langle M \rangle$. Consider the subset $M^* = M \cup \{v_0\}$ □

Corollary 6.50. *Every subspace W of a vector space V is a direct summand*

Proof. Let B be a basis of W. By the theorem, there is a subset B' with $B \cup B'$ is a basis of V. It is straightforward to check that $V = W \oplus \langle B' \rangle$ □

The ring of real numbers $\mathbb{R}$ is a vector space over $\mathbb{Q}$; a basis is usually called a **Hamel basis**, and it is useful in constructing analytic counterexamples. For example, we may use a Hamel basis to prove the existence of

a discontinuous function $f : \mathbb{R} \to \mathbb{R}$ that satisfies the functional equation $f(x + y) = f(x) + f(y)$.

As in the finite-dimensional case, if B is a basis of a vector space V, then any function $f : B \to V$ extends to a linear transformation $F : V \to V$. A Hamel basis has cardinal $c = |\mathbb{R}|$, and so there are $c^c = 2^c > c$ functions $f : \mathbb{R} \to \mathbb{R}$ satisfying the functional equation, for every linear transformation is additive. On the other hand, every continuous function on $\mathbb{R}$ is determined by its values on $\mathbb{Q}$, which is countable.

Let $x \in \mathbb{R}$, then there is a sequence of rational numbers $(q_n)_{n=1}^{\infty}$ that converges to x. Continuity of f means that

$$\lim_{n\to\infty} f(q_n) = f(\lim_{n\to\infty} q_n) = f(x)$$

This means that the values of f at rational numbers already determine f. In other words, the mapping $\Phi : C(\mathbb{R}, \mathbb{R}) \to \mathbb{R}^{\mathbb{Q}}$, defined by $\Phi(f) = f_{\mathbb{Q}}$, where $f|_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$ is the restriction of f to $\mathbb{Q}$ is an injection. Here $C(\mathbb{R}, \mathbb{R})$ denotes the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$.

Example 6.9. An **inner product** on a vector space V over a field k is a function

$$V \times V \to k$$

whose values are denoted by (v, w), s.t.

1. $(v + v', w) = (v, w) + (v', w)$ for all $v, v', w \in V$
2. $(\alpha v, w) = \alpha(v, w)$ for all $v, w \in V$ and $\alpha \in k$
3. $(v, w) = (w, v)$ for all $v, w \in V$

We say that the inner product is **definite** if $(v, v) \neq 0$ whenever $v \neq 0$

Regard $\mathbb{R}$ is a vector space over $\mathbb{Q}$, and let Y be a basis. Using 0 coefficients if necessary, for each $v, w \in \mathbb{R}$, there are $y_i \in Y$ and rational a_i and b_i with $v = \sum a_i y_i$ and $w = \sum b_i y_i$. Define

$$(v, w) = \sum a_i b_i$$

Lemma 6.51. *Let X and Y be sets, and let $f : X \to Y$ be a function. If $f^{-1}(y)$ is finite for every $y \in Y$, then $|X| \leq \aleph_0 |Y|$; hence if Y is infinite, then $|X| \leq |Y|$*

Lemma 6.52. *If X is an infinite set and $\mathrm{Fin}(X)$ is the family of all its finite subsets, then $|\mathrm{Fin}(X)| = |X|$*

Lemma 6.53. *If X and Y are sets with $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$*

Theorem 6.54. *Let k be a field and let V be a vector space over k*

1. *Any two bases of V have the same number of elements; this cardinal is called the* ***dimension*** *of V and is denoted by* $\dim(V)$
2. *Vector spaces V and V' over k are isomorphic if and only if* $\dim(V) = \dim(V')$

Proof. 1. Let B and B' be bases of V. We may assume B and B' are infinite.
Each $v \in V$ has a unique expression of the form $v = \sum_{b \in B} \alpha_b b$, where $\alpha_b \in k$ and almost all $\alpha_b = 0$(the rule only allows finite operation) . Define the **support** of v (w.r.t. B) by

$$\operatorname{supp}(v) = \{b \in B : \alpha_b \neq 0\}$$

thus $\operatorname{supp}(v)$ is a finite subset of B for every $v \in V$. Define $f : B' \to \operatorname{Fin}(B)$ by $f(b') = \operatorname{supp}(b)$. Note that if $\operatorname{supp}(b') = \{b_1, \ldots, b_n\}$, then $b' \in \langle b_1, \ldots, b_n \rangle = \langle \operatorname{supp}(b') \rangle$. Since $\langle \operatorname{supp}(b') \rangle$ has dimension n, it contains at most n elements of B', because B' is independent. Therefore $f^{-1}(T)$ is finite for every finite subset subset T of B. By Lemma 6.51, we have $\left|B'\right| \leq |\operatorname{Fin}(B)|$, and by Lemma 6.52, we have $\left|B'\right| \leq |B|$. Interchanging the roles of B and B' gives the reverse inequality, and so Lemma 6.53 gives $|B| = \left|B'\right|$.

□

Lemma 6.55. *Let R be a commutative ring and let $\mathcal{F}$ be the family of all those ideals in R that are not finitely generated. If $\mathcal{F} \neq \emptyset$, then $\mathcal{F}$ has a maximal element*

Theorem 6.56 (I. S. Cohen)**.** *A commutative ring R is noetherian if and only if every prime ideal in R is finitely generated*

Proof. Let $\mathcal{F}$ be the family of all ideals in R that are not finitely generated. If $\mathcal{F} \neq \emptyset$, then the lemma provides an ideal I that is not finitely generated and that is maximal.

Suppose $ab \in I$ but $a \notin I$ and $b \notin I$. $I \subsetneq I + Ra$ and $I_R a$ is finitely generated; we may assume that

$$I + Ra = (i_1 + r_1 a, \ldots, i_n + r_n a)$$

where $i_k \in I$ and $r_k \in R$. Consider $J = (I : a) = \{x \in R : xa \in I\}$. Now $I + Rb \subseteq J$ and hence J is finitely generated. We claim that $I = (i_1, \ldots, i_n, Ja)$. Clearly $(i_1, \ldots, i_n, Ja) \subseteq I$. If $z \in I \subseteq I + Ra$, there are $u_k \in R$ with $z = \sum_k u_k(i_k + r_k a)$. Then $(\sum_k u_k r_k)a = z - \sum_k u_k i_k \in I$, so that $\sum_k u_k r_k \in J$. Hence $z \in (i_1, \ldots, i_n, Ja)$. It follows that I is finitely generated. □

Proposition 6.57. *Let K/k be an extension*

1. *If $z \in K$, then z is algebraic over k iff $k(z)/k$ is finite*
2. *If $z_1, \ldots, z_n \in K$ are algebraic over k, then $k(z_1, \ldots, z_n)/k$ is a finite extension*
3. *If $y, z \in K$ are algebraic over k, then $y + z$, yz and y^{-1} (for $y \neq 0$) are also algebraic*
4. *Define*
$$K_{alg} = \{z \in K : z \text{ is algebraic over } k\}$$
Then K_{alg} is a subfield of K

Proof. 1. If $k(z)/k$ is finite, then Proposition 3.144 shows that z is algebraic over k

2. We prove this by induction on $n \geq 1$; the base step is part (1). For the inductive steop, there is a tower of fields
$$k \subseteq k(z_1) \subseteq \cdots \subseteq k(z_1, \ldots, z_n) \subseteq k(z_1, \ldots, z_{n+1})$$
Now $[k(z_{n+1}) : k]$ is finite by Theorem 3.149; say, $[k(z_{n+1}) : k] = d$, where d is the degree of the monic irreducible polynomial in $k[x]$ having z_{n+1} as a root. Since z_{n+1} satisfies a polynomial of degree d over k, it satisfies a polynomial of degree $d' \leq d$ over the large field $F = k(z_1, \ldots, z_n)$
3. $k(y + z) \subseteq k(y, z)$ and $k(yz) \subseteq k(y, z)$

□

Definition 6.58. Given the extension $\mathbb{C}/\mathbb{Q}$, define the **algebraic numbers** by
$$\mathbb{A} = (\mathbb{C}/\mathbb{Q})_{alg}$$

Example 6.10. We claim that $\mathbb{A}/\mathbb{Q}$ is an algebraic extension that is not finite. Suppose $[\mathbb{A} : \mathbb{Q}] = n$ for some integer n. There exist irreducible polynomial in $\mathbb{Q}[x]$ of degree $n + 1$; for example, $p(x) = x^{n+1} - 2$. If α is a root of $p(x)$, then $\alpha \in \mathbb{A}$ and so $\mathbb{Q}(\alpha) \subseteq \mathbb{A}$. Thus
$$n = [\mathbb{A} : \mathbb{Q}] = [\mathbb{A} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \geq n + 1$$

Lemma 6.59. *1. If $k \subseteq K \subseteq E$ is a tower of fields with E/K and K/k algebraic, then E/k is also algebraic*

2. *Let*
$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq K_{n+1} \subseteq \cdots$$
be an ascending tower of fields. If K_{n+1}/K_n is algebraic for all $n \geq 0$, then $K^* = \bigcup_{n \geq 0} K_n$ is a field algebraic over K_0

3. *Let $K = k(A)$. If each element $a \in A$ is algebraic over k, then K/k is an algebraic extension*

Definition 6.60. A field K is **algebraically closed** if every nonconstant $f(x) \in K[x]$ has a root in K. An **algebraic closure** of a field k is an algebraic extension $\overline{k}$ of k that is algebraically closed

$\overline{\mathbb{Q}} = \mathbb{A}$

Lemma 6.61. *Let k be a field, and let $k[T]$ be the polynomial ring in a set T of indeterminates. If $t_1, \ldots, t_n \in T$ are distinct, where $n \geq 2$, and $f_i(t_i) \in k[t_i] \subseteq k[T]$ are nonconstant polynomials, then the ideal $I = (f_1(t_1), \ldots, f_n(t_n))$ in $k[T]$ is a proper ideal*

Proof. If I not a proper ideal, then there exists $h_i(T) \in k[T]$ with

$$1 = h_1(T) f_1(t_1) + \cdots + h_n(T) f_n(t_n)$$

Consider the field extension $k(\alpha_1, \ldots, \alpha_n)$ whre α_i is a root of $f_i(t_i)$ for $i = 1, \ldots, n$. Denote the variables involved in the $h_i(T)$ other than $t_1, \ldots, t_n$, if any, by $t_{n+1}, \ldots, t_m$. Evaluating when $t_i = \alpha_i$ if $i \leq n$ and $t_i = 0$ if $i \geq n + 1$, then right side is 0 (evaluation is a homomorphism) □

Theorem 6.62. *Given a field k , there exists an algebraical closure $\overline{k}$ of k*

Proof. Let T be a set in bijective correspondence with the family of nonconstant polynomials in $k[x]$. Let $R = k[T]$ be the big polynomial ring, and let I be the ideal in R generated by all elements of the form $f(t_f)$, where $t_f \in T$

We claim that the ideal I is proper; if not, $1 \in I$, and there are distinct $t_1, \ldots, t_n \in T$ and polynomials $h_1(T), \ldots, h_n(T) \in k[T]$ with $1 = h_1(T) f_1(T) + \cdots + h_n(T) f_n(t_n)$, contradicting Lemma 6.61. Therefore there is a maximal ideal M in R containing I by Theorem 6.47. Define $K = R/M$. The proofs is now completed in a series of steps

1. K/k is a field extension
   Because M is maximal, $R = (a) + M$ for any $a \notin M$. So $1 = ra + m$ or equivalently $1 + M = (r + M)(a + M)$. So $K = R/M$ is a field. Let $i : k \to k[T]$ be the ring map taking $a \in k$ to the constant polynomial a, and let θ be the composite $k \xrightarrow{i} k[T] = R \xrightarrow{\text{nat}} R/M = K$. Now θ is injective by Corollary 3.68. We identify k with $\operatorname{im} \theta \subseteq K$

2. Every nonconstant $f(x) \in k[x]$ splits in $K[x]$
   By definition, there is $t_f \in T$ with $f(t_f) \in I \subseteq M$, and the coset $t_f + M \in R/M = K$ is a root of $f(x)$. It now follows by induction on degree that $f(x)$ splits over K
3. The extension K/k is algebraic
   By Lemma 6.59, it suffices to show that each $t_f + M$ is algebraic over k (for $K = k(\text{all } t_f + M)$ follows from 3.144)

Let $k_1 = K$ and construct k_{n+1} from k in the same way K is constructed from k. There is a tower of fields $k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_n \subseteq \ldots$ with each extension k_{n+1}/k_n algebraic and with every nonconstant polynomials in $k_n[x]$ having a root in k_{n+1}. By Lemma 6.59 $E = \bigcup_n k_n$is an algebraic extension of k. We claim that E is algebraiclly closed. □

Corollary 6.63. *If k is a countable field, then it has a countable algebraic closure. In particular, the algebraic closures of the prime fields $\mathbb{Q}$ and $\mathbb{F}_p$ are countable*

Proof. If k is countable, then the set T of all nonconstant polynomials is countable, say, $T = \{t_1, t_2, \ldots\}$, because $k[x]$ is countable. Hence $k[T] = \bigcup_{l \geq 1} k[t_1, \ldots, t_l]$ is countable, as its quotient k_1. It follows by induction on $g \geq 1$, that every k_n is countable □

Definition 6.64. If F/k and K/k are field extensions, then a **k-map** is a ring homomorphism $\varphi : F \to K$ that fixes k pointwise

Lemma 6.65. *If K/k is an algebraic extension, then every k-map $\varphi : K \to K$ is an automorphism of K*

Proof. By Corollary 3.68, the k-map φ is injective. Let $a \in K$ and there is an irreducible $p(x) \in k[x]$ having a as a root. φ permutes all roots of $p(x)$ □

Lemma 6.66. *Let k be a field and let $\overline{k}/k$ be an algebraic closure. If F/k is an algebraic extension, then there is an injective k-map $\psi : F \to \overline{k}$*

Proof. If E is an intermediate field, $k \subseteq E \subseteq F$, let us call an ordered pair (E, f) an **approximation** if $f : E \to \overline{k}$ is a k-map. In the following diagram, all arrows other than f are inclusions

$$\begin{array}{ccccc} \overline{k} & & & & \\ {\scriptstyle i}\uparrow & \nwarrow^{f} & & & \\ k & \longrightarrow & E & \longrightarrow & F \end{array}$$

Define $X = \{\text{approximations } (E, f) : k \subseteq E \subseteq F\}$. Note that $X \neq \emptyset$ because $(k, i) \in X$. Partially order X by

$$(E, f) \preceq (E', f') \text{ if } E \subseteq E' \text{ and } f|E' = f$$

Chain

$$\mathcal{S} = \{(E_j, f_j) : j \in J\}$$

has an upper bound $(\bigcup E_j, \bigcup f_j = \Phi)$. Φ is a k-map

By Zorn's Lemma, there exists a maximal element (E_0, f_0) in X. We claim that $E_0 = F$ and this will complete the proof (take $\psi = f_0$). If $E_0 \subsetneq F$, then there is $a \in F$ with $a \notin E_0$. Since F/k is algebraic, we have F/E_0 algebraic, and there is an irreducible $p(x) \in E_0[x]$ having a as a root. Since $\overline{k}/k$ is algebraic and $\overline{k}$ is algebraically closed, we have a factorization in $\overline{k}[x]$:

$$f_0^*(p(x)) = \prod_{i=1}^{n} (x - b_i)$$

where $f_0^* : E_0[x] \to \overline{k}[x]$ is the map $f_0^* : e_0 + \cdots + e_n x^n \mapsto f_0(e_0) + \cdots + f_0(e_n)x^n$. If all the b_i lie in $f_0(E_0) \subseteq \overline{k}$, then $f_0^{-1}(b_i) \in E_0 \subseteq F$ for all i, and there is a factorization of $p(x)$ in $F[x]$, namely, $p(x) = \prod_{i=1}^{n}[x - f_0^{-1}(b_i)]$. But $a \notin E_0$ implies $a \neq f_0^{-1}(b_i)$ for all i. Thus $x - a$ is another factor of $p(x)$ in $F[x]$, contrary to unique factorization. . We conclude that there is some $b_i \notin \text{im } f_0$. By Theorem 3.149, we may define $f_1 : E_0(a) \to \overline{k}$ by

$$c_0 + c_1 a + c_2 a^2 + \cdots \mapsto f_0(c_0) + f_0(c_1)b_i + \ldots$$

A straight forward check shows that f_1 is a k-map extending f_0. Hence $(E_0, f_0) \prec (E_0(a), f_1)$, contradicting the maximality of (E_0, f_0). □

Theorem 6.67. *Any two algebraic closure of a field k are isomorphic via a k-map*

Proof. Let K and L be two algebraic closure of a field k. By Lemma 6.66, there are k-maps $\psi : K \to L$ and $\theta : L \to K$. By Lemma 6.65, both composites $\theta\psi$ and $\psi\theta$ are automorphisms. It follows that ψ (and θ) is a k-isomorphisms □

Definition 6.68. If $\varphi \in k(x)$, then there are polynomials $g(x), h(x) \in k[x]$ with $(g, h) = 1$ and $\varphi = g(x)/h(x)$. Define the **degree** of φ by

$$\text{degree}(\varphi) = \max\{\deg(g), \deg(h)\}$$

A rational function $\varphi \in k(x)$ is called a **linear fractional transformation** if

$$\varphi = \frac{ax+b}{cx+d}$$

where $a, b, c, d \in k$ and $ad - bc \neq 0$. Let

$$\mathrm{LF}(k)$$

denote the group of all linear fractional transformations in $k(x)$ with binary operation composition: if $\varphi : x \mapsto (ax+b)/(cx+d)$ and $\psi : x \mapsto (rx+s)/(tx+u)$, then

$$\psi\varphi : x \mapsto \frac{r\varphi(x)+s}{t\varphi(x)+u} = \frac{(ra+sc)x+(rb+sd)}{(ta+ud)x+(tb+ud)}$$

Proposition 6.69. *If $\varphi \in k(x)$ is nonconstant, then φ is transcendental over k and $k(x)$ is a finite extension of $k(\varphi)$ with*

$$[k(x) : k(\varphi)] = \textit{degree}(\varphi)$$

Moreover, if $\varphi = g(x)/h(x)$ and $(g,h) = 1$, then

$$\mathrm{irr}(x, k(\varphi)) = g(y) - \varphi h(y)$$

where $\varphi h(y)$ denotes the product of φ and $h(y)$ in $k(\varphi)[y]$

Proof. Let $g(x) = \sum a_i x^i$ and $h(x) = \sum b_i x^i \in k[x]$. Define

$$\theta(y) = g(y) - \varphi h(y)$$

Now $\theta(y)$ is a polynomial in $k(\varphi)[y]$: $\theta(y) = \sum a_i y^i - \varphi \sum b_i y^i = \sum (a_i - \varphi b_i) y^i$. If $\theta(y)$ were the zero polynomial, then all its coefficients would be 0. But if b_i is a nonzero coefficient of $h(y)$, then $a_i - \varphi b_i = 0$ gives $\varphi = a_i/b_i$, contradicting φ not being a constant; that is, $\varphi \notin k$.

$$\deg(\theta(y)) = \deg(g(y) - \varphi h(y)) = \max\{\deg(g), \deg(h)\} = \mathrm{degree}(\varphi)$$

Now x is a root of $\theta(y)$, so that x is algebraic over $k(\varphi)$. Were φ algebraic over k, then $k(\varphi)/k$ would be finite, giving $[k(x) : k] = [k(x) : k(\varphi)][k(\varphi) : k]$ finite, a contradiction. Therefore φ is transcendental over k.

We claim that $\theta(y)$ is an irreducible polynomial in $k(\varphi)[y]$. If not, then $\theta(y)$ factors in $k[\varphi][y]$ by Gauss's Corollary 6.27. But $\theta(y) = g(y) - \varphi h(y)$ is linear in φ, and so Corollary 6.29 shows that $\theta(y)$ is irreducible. Finally, since $\deg(\theta) = \mathrm{degree}(\varphi)$, we have $[k(x) : k(\varphi)] = \mathrm{degree}(\varphi)$ □

Corollary 6.70. *Let $\varphi \in k(x)$, where $k(x)$ is the field of rational functions over a field k. Then $k(\varphi) = k(x)$ if and only if φ is a linear fractional transformations*

Proof. By Proposition 6.69, $k(\varphi) = k(x)$ if and only if degree$(\varphi) = 1$; that is, φ is a linear fractional transformation □

Define a map $\zeta : \mathrm{GL}(2,k) \to \mathrm{LF}(k)$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (ax+b)/(cx+d)$. In Exercise 6.4.2, $\ker \zeta = Z(2,k)$, the center of $\mathrm{GL}(2,k)$ consisting of all nonzero 2×2 scalar matrices. Hence if

$$\mathrm{PGL}(2,k) = \mathrm{GL}(2,k)/Z(2,k)$$

then $\mathrm{LF}(k) \cong \mathrm{PGL}(2,k)$

Corollary 6.71. *If $k(x)$ is the field of rational functions over a field k, then*

$$\mathrm{Gal}(k(x)/k) \cong \mathrm{LF}(k) \cong PGL(2,k)$$

Proof. Let $\sigma : k(x) \to k(x)$ be an automorphism of $k(x)$ fixing k. Since $k(\sigma(x)) = k(x)$, Corollary 6.70 says that $\sigma(x)$ is a linear fractional transformation. Define $\gamma : \mathrm{Gal}(k(x)/k) \to \mathrm{LF}(k)$ by $\gamma : \sigma \mapsto \sigma(x)$. Now γ is a homomorphism: $\gamma(\sigma\tau) = \gamma(\sigma)\gamma(\tau)$. Finally γ is an isomorphisms □

Theorem 6.72 (Lüroth's theorem)**.** *If $k(x)$ is a simple transcendental extension, then every intermediate field B with $k \subsetneq B \subseteq k(x)$ is also a simple transcendental extension of k: there is $\varphi \in B$ with $B = k(\varphi)$*

Definition 6.73. Let E/k be a field extension. A subset U of E is **algebraically dependent** over k if there exists a finite subset $u_1, \ldots, u_n \subseteq U$ and a nonzero polynomial $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ with $f(u_1, \ldots, u_n) = 0$. A field extension E/k is **purely transcendental** if either $E = k$ or E contains an algebraically independent B and $E = k(B)$

Let E/k be a field extension, let $u_1, \ldots, u_n \in E$ and let $\varphi : k[x_1, \ldots, x_n] \to E$ be the evaluation map $f(x_1, \ldots, x_n) \mapsto f(u_1, \ldots, u_n)$. Now $\{u_1, \ldots, u_n\}$is algebraically dependent if and only if $\ker \varphi \neq \{0\}$. If $\{u_1, \ldots, u_n\}$ is algebraically independent, then φ extends to an isomorphism $\widetilde{\varphi} : k(x_1, \ldots, x_n) \to k(u_1, \ldots, u_n) \subseteq E$, where $k(x_1, \ldots, x_n)$ is the field of rational functions

$$\begin{array}{ccc} k(x_1, \ldots, x_n) & \xrightarrow{\widetilde{\varphi}} & \mathrm{Frac}(E) = E \\ \uparrow & & \uparrow \\ k[x_1, \ldots, x_n] & \xrightarrow{\varphi} & E \end{array}$$

In particular, if $\{u_1, \ldots, u_n\}$ is algebraically independent and $E = k(u_1, \ldots, u_n)$, then $\widetilde{\varphi}$ is an isomorphism $k(x_1, \ldots, x_n) \to k(u_1, \ldots, u_n)$ with $x_i \mapsto u_i$. Therefore, a purely transcendental extension $k(u_1, \ldots, u_n)/k$ is isomorphic to the **function field in n variables**

Proposition 6.74. *Let E/k be a field extension. Then $U \subseteq E$ is algebraically dependent over k if and only if there is $v \in U$ with v algebraic over $k(U - \{v\})$*

Proof. If U is algebraically dependent over k, then there is a finite algebraically dependent subset $\{u_1, \ldots, u_n\} \subseteq U$; thus, we may assume that U is finite. We prove, by induction on $n \geq 1$, that some u_i is algebraic over $k(U - \{u_i\})$. If $n = 1$, it's obvious.

Let $U = \{u_1, \ldots, u_{n+1}\}$ be algebraically dependent. We may assume that $\{u_1, \ldots, u_n\}$ is algebraically independent. Since U is algebraically dependent, there is a nonzero $f(X, y) \in k[x_1, \ldots, x_n, y]$ with $f(u_1, \ldots, u_n, u_{n+1} = 0)$, where $X = \{x_1, \ldots, x_n\}$ and y is a new variable. We may write $f(X, y) = \sum_i g_i(X) y^i$, where $g_i(X) \in k[X]$.Since $f(X, y) \neq 0$, some $g_i(X) \neq 0$, and it follows from algebraic independence of $\{u_1, \ldots, u_n\}$ that $g_i(u_1, \ldots, u_n) \neq 0$. Therefore, $h(y) = \sum_i g(u_1, \ldots, u_n) y^i \in k(U)[y]$. But $0 = h(u_{n+1})$, so that u_{n+1} is algebraic over $k(u_1, \ldots, u_n)$

For the converse, assume that v is algebraic over $k(U - \{v\})$. We may assume that $U - \{v\}$ is finite, say, $U - \{v\} = \{u_1, \ldots, u_n\}$, where $n \geq 0$. We prove by induction on $n \geq 0$. For the inductive step, let $U - \{u_{n+1}\} = \{u_1, \ldots, u_n\}$ and assume it is algebraically independent. By hypothesis, there is a nonzero polynomial $f(y) = \sum_i c_i y^i \in k(u_1, \ldots, u_n)[y]$ with $f(u_{n+1}) = 0$. As $f(y) \neq 0$, we may assume that at least one of its coefficients is nonzero. For all i, the coefficient $c_i \in k(u_1, \ldots, u_n)$, so there are rational functions $c_i(x_1, \ldots, x_n)$ with $c_i(u_1, \ldots, u_n) = c_i$ [because $k(u_1, \ldots, u_n) \cong k(x_1, \ldots, x_n)$] □

Definition 6.75. A **dependency relation on a set** Ω is a relation $\preceq$ from Ω to 2^Ω, pronounced "is dependent on", satisfying the following **Dependency Axioms**:

1. if $S \subseteq \Omega$ and $u \in S$, then $u \preceq S$
2. if $u \preceq S$, then there exists a finite subset $S' \subseteq S$ with $u \preceq S'$
3. (**Transitivity**) if $u \preceq S$ and, for some $T \subseteq \Omega$, we have $s \preceq T$ for every $s \in S$, then $u \preceq T$
4. (**Exchange Axiom**) if $u \preceq S$ and $u \not\preceq S - \{v\}$, then $v \preceq (S - \{v\}) \cup \{u\}$

Example 6.11. If Ω is a vector space, define $u \preceq S$ to mean $u \in \langle S \rangle$, the subspace spanned by S. We claim that $\preceq$ is a dependency relation.

Lemma 6.76. *If E/k is a field extension, then $u \preceq S$, defined by u being algebraic over $k(S)$ is a dependency relation on E*

Proof. If $u \preceq S$, then u is algebraic over $k(S)$; that is, $u \in (E/k(S))_{\text{alg}} = \{e \in E : e \text{ is algebraic over } k(S)\}$. Suppose there is some $T \subseteq E$ with $s \preceq T$ for every $s \in S$; that is, $S \subseteq (E/k(T))_{\text{alg}}$. It follows from Lemma 6.59 that $(E/k(S))_{\text{alg}} \subseteq (E/k(T))_{\text{alg}}$; and so $u \preceq T$

The Exchange Axiom assumes that $u \preceq S$ and u is transcendental over $k(S - \{v\})$. Note that $v \in S$ and $u \notin S$. Let us apply Proposition 6.74 to the subsets $U' = \{u, v\}$ and $S' = S - \{v\}$ of E and the subfield $k' = k(S')$. With this notation, $k'(U' - \{u\}) = k'(v) = k(S', v) = k(S)$, so that u is algebraic over $k(S)$ can be restated as u algebraic over $k'(U' - \{u\})$. Thus Proposition 6.74 says that $U' = \{u, v\}$ is algebraically dependent over $k' = k(S)$: there is a nonzero polynomial $f(x, y) \in k(S')[x, y]$ with $f(u, v) = 0$. □

Definition 6.77. Let $\preceq$ be a dependency relation on a set Ω. Call a subset $S \subseteq \Omega$ **dependent** if there exists $s \in S$ with $s \preceq S - \{s\}$; call S **independent** if it is not dependent

Definition 6.78. Let $\preceq$ be a dependency relation on a set Ω. We say that a subset S **generates** Ω if $x \preceq S$ for all $x \in \Omega$. A **basis** of Ω is an independent subset that generates Ω

Lemma 6.79.
1. *Let $\preceq$ be a dependency relation on a set Ω. If $T \subseteq \Omega$ is independent and $z \not\preceq T$ for some $z \in \Omega$, then $T \cup \{z\} \supsetneq T$ is a strictly larger independent set.*
2. *Let E/k be a field extension. If $T \supseteq E$ is algebraically independent over k and $z \in E$ is transcendental over $k(T)$, then $T \cup \{z\}$ is algebraically independent*

Proof.
1. not hard
2. By Proposition 6.74, this is a special case of (1)

□

Definition 6.80. If E/k is a field extension, then a **transcendence basis** is a maximal algebraically independent subset of E over k

Theorem 6.81.
1. *If $\preceq$ is a dependency relation on a set Ω, then Ω has a basis. In fact, every independent subset B of Ω is part of basis*
2. *If E/k is a field extension, then E has a transcendence basis. In fact, every algebraically independent subset is part of a transcendence basis*

Proof. 1. Since the empty set $\emptyset$ is independent, the second statement implies the first

We use Zorn's Lemma to prove the existence of maximal independent subsets of Ω containing B. Let X be the family of all independent subsets of Ω containing B. X is nonempty. Suppose that $\mathcal{B} = (B_j)_{j\in J}$ is a chain in X. It is clear that $B^* = \bigcup_{j\in J} B_j$ is an upper bound of $\mathcal{B}$ if it lies in X. If B^* is dependent, then there is $y \in B^*$ with $y \preceq B^* - \{y\}$. By Dependency Axiom (2), there is a finite subset $\{x_1, \ldots, x_n\} \subseteq B^* - \{y\}$ with $y \preceq \{x_1, \ldots, x_n\} - \{y\}$. There is B' s.t. $\{x_1, \ldots, x_n, y\} \subseteq B'$ dependent

□

Theorem 6.82. *If B is a transcendence basis, then $k(B)/k$ is purely transcendental and $E/k(B)$ is algebraic*

Proof. By Theorem 6.81, it suffices to show that if B is a transcendence basis, then $E/k(B)$ is algebraic □

Theorem 6.83. *1. If Ω is a set with a dependency relation $\preceq$, then any two bases B and C have the same cardinality*

2. If B and C are transcendence basis of a field extension E/k , then $|B| = |C|$

Proof. If $B = \emptyset$, we claim that $C = \emptyset$. Otherwise there exists $y \in C$, and since C is independent, $y \not\preceq C - \{y\}$. But $y \preceq B = \emptyset$ and $\emptyset \subseteq C - \{y\}$, so that Dependency Axiom (3) $y \preceq C - \{y\}$, a contradiction.

Now assume B is finite; say, $B = \{x_1, \ldots, x_n\}$. We prove, by induction on $k \geq 0$, that there exists $\{y_1, \ldots, y_{k-1} \subseteq C\}$ with

$$B_k = \{y_1, \ldots, y_{k-1}, x_k, \ldots, x_n\}$$

a basis; that is , the elements $x_1, \ldots, x_{k-1}$ can be exchanged with elements $y_1, \ldots, y_{k-1} \in C$ so that B_k is a basis.

Assume $B_k = \{y_1, \ldots, y_{k-1}, x_k, \ldots, x_n\}$ is a basis, we want to show that B_{k+1} is basis. We claim that there is $y_k \in C$ with $y_k \not\preceq B_k - \{x_k\}$. Otherwise, $y \preceq B_k - \{x_k\}$ for all $y \preceq C$. But $x_k \preceq C$, and so Dependency Axiom (3) gives $x_k \preceq B_k - \{x_k\}$.

By Lemma 6.79, B_{k+1} is independent. To see that B_{k+1} is a basis, it suffices to show that it generates Ω. Now $y_k \preceq B_k$ and $y_k \not\preceq B_k - \{x_k\}$; the Exchange Axiom gives $x_k \preceq (B_k - \{x_k\} \cup \{y_k\}) = B_{k+1}$

If $|C| > n = |B|$. Then $B_n \subseteq C$. Thus a proper subset of C generates Ω, contradicting the independence of C □

Definition 6.84. The **transcendence degree** of $E/k$is defined by

$$\text{trdeg}(E/k) = |B|$$

where B is a transcendence basis of E/k

Example 6.12.
1. If E/k is a field extension, then $\text{trdeg}(E/k) = 0$ if and only if E/k is algebraic
2. If $E = k(x_1, \ldots, x_n)$ is the function field in n variables over a field k, then $\text{trdeg}(E/k) = n$, because $\{x_1, \ldots, x_n\}$ is a transcendence basis of E

Proposition 6.85. *There are nonisomorphic fields each of which is isomorphic to a subfield of the other*

Proof. Clearly $\mathbb{C}$ is isomorphic to a subfield of $\mathbb{C}(x)$. However we claim that $\mathbb{C}(x)$ is isomorphic to a subfield of $\mathbb{C}$. Let B be a transcendence basis of $\mathbb{C}$ over $\mathbb{Q}$, and discard one of its element, say, b. The algebraic closure F of $\mathbb{Q}(B - \{b\})$ is a proper subfield of $\mathbb{C}$ □

Exercise

Exercise 6.4.1. Prove that $\varphi \in k(x)$ has degree 1 if and only if φ is a linear fractional transformation

Exercise 6.4.2. For any field k, define a map $\zeta : \text{GL}(2, k) \to LF(k)$ by

$$\zeta : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (ax + b)/(cx + d)$$

1. Prove that ζ is a surjective group homomorphism
2. Prove that $\ker \zeta = Z(2, k)$, the subgroup of $\text{GL}(2, k)$ consisting of all nonzero scalar matrices

Exercise 6.4.3. Prove that the set $\mathbb{A}$ of all algebraic numbers is an algebraic closure of $\mathbb{Q}$

6.5 Varieties

Varieties and Ideals

Let k be a field and let k^n denoted the set of all n-tuples:

$$k^n = \{a = (a_1, \ldots, a_n) : a_i \in k \text{ for all } i\}$$

We use the abbreviation

$$X = (x_1, \ldots, x_n)$$

so that the polynomial ring $k[x_1, \ldots, x_n]$ in several variables may be denoted by $k[X]$ and a polynomial $f(x_1, \ldots, x_n)$ in $k[X]$ may be abbreviated by $f(X)$

Definition 6.86. If $f(X) \in k[X]$, its **polynomial function** $f^\flat : k^n \to k$ is defined by evaluation

$$f^\flat : (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$$

For the remainder of this section, we assume that all fields are infinite

Definition 6.87. If $f(X) \in k[X] = k[x_1, \ldots, x_n]$ and $f(a) = 0$, where $a \in k^n$, then a is called a **zero** of $f(X)$.

Proposition 6.88. *If k is an algebraically closed field and $f(X) \in k[X]$ is not a constant, then $f(X)$ has a zero*

Proof. Induction on $n \geq 1$, where $X = (x_1, \ldots, x_n)$. Write

$$f(X, y) = \sum_i g_i(X) y^i$$

For each $a \in k^n$, define $f_a(y) = \sum_i g_i(a) y^i$. If $f(X, y)$ has no zeros, then each $f_a(y) \in k[y]$ has no zeros, hence $f_a(y)$ is a nonzero constant. □

7 Rings

7.1 Modules

Example 7.1.

1. If k is any nonzero commutative ring, then $\mathrm{Mat}_n(k)$, all $n \times n$ matrices with entries in k, is a ring under matrix multiplication and matrix addition; it is commutative if and only if $n = 1$.
   Let k be any ring. If $A = [a_{ip}]$ is an $n \times l$ matrix and $B = [b_{pj}]$ is an $l \times m$ matrix, then their product AB is defined to be the $n \times m$ matrix whose ij entry has the usual formula: $(AB)_{ij} = \sum_p a_{ip} b_{pj}$. Thus $\mathrm{Mat}_n(k)$ is a ring, even if k is not commutative
2. If G is a group, we define the **group ring** $\mathbb{Z}G$ as follows. Its additive group is the free abelian group having a basis

8 Index

9 TODO Some statements need to be verified

6.66