Abstract Algebra

from the context of the courses
MTH 418H-419H: Honors Algebra

Kaedon Cleland-Host

May 3, 2022

Contents

Chapter 1

Group Theory

1.1 Groups

Definition 1.1.1. A **law of composition** is a map $S^2 \to S$.

Remark. We will use the notation ab for the elements of S obtained as $a, b \to ab$. This element is the product of a and b.

Definition 1.1.2. A **group** is a set G together with a law of composition that has the following three properties:

1. **Identity** There exists an element $1 \in G$ such that $1a = a1 = A$ for all $a \in G$.
2. **Associativity** $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. **Inverse** For any $a \in G$, there exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = 1$.

Definition 1.1.3. An **abelian group** is a group with a commutative law of composition. That is for any $a, b \in G$, $ab = ba$.

Definition 1.1.4. The **order** of a group G is the cardinality of the set.

Proposition 1.1.5. Cancellation Law For $a, b, c \in G$ if $ab = ac$ then $b = c$.

Proposition 1.1.6. Let S be a set with an associative law of composition and an identity. The subset of elements of S that are invertible forms a group.

1.2 Subgroups

Definition 1.2.1. A group H is a **Subgroup** of G iff H is subset of G, H has the same law of composition as G, and H is also a group. In other words H a group iff it is a subset of G with the following properties:

1. **Closure** $a, b \in H$ then $ab \in H$.
2. **Identity** $1 \in H$.
3. **Inverse** For all $a \in H$, $a^{-1} \in H$.

Definition 1.2.2. A subgroup S of G is a **proper subgroup** iff $S \neq G$ and $S \neq \{\mathbb{I}\}$.

Proposition 1.2.3. If H and K are subgroup of G, then $H \cap K$ is a subgroup.

Theorem 1.2.4. If S is a subgroup of $\mathbb{Z}^+$, then either

- $S = \{0\}$
- $S = \mathbb{Z}a$, where a is the smallest elements of S.

Definition 1.2.5. For two integers $a, b \in \mathbb{Z}$ we stat that a **divides** b iff $\frac{b}{a} \in \mathbb{Z}$ denoted $a|b$.

1.2.6 Greatest Common Divisor

Definition 1.2.7. The **greatest common divisor** of two integers $a, b \in \mathbb{Z}$ is the integer $d \in \mathbb{Z}$ such that

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} | n = ra + sb \forall r, s \in \mathbb{Z}\}$$

Proposition 1.2.8. Properties of the greatest common divisor Let $a, b \in \mathbb{Z}$, not both zero, and let d be the greatest common divisor. Then

1. There are integers $r, s \in \mathbb{Z}$ such that $d = ra + sb$.
2. $d|a$ and $d|b$.
3. If $e \in \mathbb{Z}$ such that $e|a$ and $e|b$ then $e|d$.

Definition 1.2.9. Two integers $a, b \in \mathbb{Z}$ are **relatively prime** iff $\gcd(a, b) = 1$.

Corollary 1.2.10. A pair $a, b \in \mathbb{Z}$ is relatively prime if an only if there are integers $r, s \in \mathbb{Z}$ such that $ra + sb = 1$.

Corollary 1.2.11. Let p be a prime integer. If p divides a product ab if integers, then at least one of $p|a$ or $p|b$ holds.

1.2.12 Least Common Multiple

Definition 1.2.13. The **least common multiple** of two integers $a, b \in \mathbb{Z}$ is the integer $m \in \mathbb{Z}$ such that

$$\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$$

Proposition 1.2.14. Properties of least common multiple Let a, b be non-zero integers and let m be there least common multiple. Then

1. $a|m$ and $b|m$.
2. If $n \in \mathbb{Z}$ such that $b|n$ and $a|n$, then $m|n$.

Corollary 1.2.15. For $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$ then $ab = dm$.

1.2.16 Cyclic Groups

Definition 1.2.17. Let G be a group and $x \in G$. The **cyclic subgroup** generated by x denoted $\langle x \rangle$ is

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, 1, x^1, x^2, \dots\}$$

Remark. For any subgroup S that contains x we have $S \subset \langle x \rangle$.

Definition 1.2.18. The **order of an element** $x \in G$ is the order of the group $\langle x \rangle$. This is the smallest positive integer n such that $x^n = 1$.

Proposition 1.2.19. Let $\langle x \rangle \subset G$ and consider the set $S = \{k \in \mathbb{Z} | x^k = 1\}$

1. The set S is a subgroup of $\mathbb{Z}^+$
2. $x^r = x^s$ $(r \geq s)$ if and only if $x^{r-s} = 1$.
3. If $S \neq \{0\}$, then $S = \mathbb{Z}n$ for some positive $n \in \mathbb{Z}$ and $\langle x \rangle = \{1, x^1, x^2, \dots, x^{n-1}\}$

Proposition 1.2.20. Let x be an element of finite order n in a group and let $k \in \mathbb{Z}$. Let $k = nq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

1. $x^k = x^r$
2. $x^k = 1$ if an only if $r = 0$.
3. The order of x^k is $n/\gcd(k, n)$.

1.3 Homomorphisms

Definition 1.3.1. A **homomorphism** $\varphi : G \to G'$ is a map from a group G to a group G' such that for any $a, b \in G$ we have

$$\varphi(ab) = \varphi(a)\varphi(b)$$

Proposition 1.3.2. Let $\varphi : G \to G'$ be a homomorphism

1. $\varphi(1) = 1$
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ for any $a \in G$

Definition 1.3.3. A homomorphism $\varphi : G \to G'$ is **injective** iff $\varphi(x) = \varphi(u) \Rightarrow x = y$

Definition 1.3.4. A homomorphism $\varphi : G \to G'$ is **surjective** iff for every $b \in G'$, there exists $a \in G$ such that $\varphi(a) = b$.

Definition 1.3.5. Let $\varphi : G \to G'$ be a homomorphism

1. The **kernal** of φ denoted $\ker(\varphi)$ is the set
$$\ker(\varphi) = \{a \in G | \varphi(a) = 1\}$$
2. The **image** of φ denoted $\operatorname{Im}(\varphi)$ is the set
$$\operatorname{im}(\varphi) = \{b \in G' | \exists a \in G, \varphi(a) = b\}$$

Corollary 1.3.6. A homomorphism $\varphi : G \to G'$ is injective if $\ker(\varphi) = \{1\}$

Corollary 1.3.7. A homomorphism $\varphi : G \to G'$ is surjective if $\operatorname{Im}(\varphi) = G'$

Proposition 1.3.8. Let $\varphi : G \to G'$ be a homomorphism the $\ker(\varphi)$ and $\operatorname{Im}(\varphi)$ are subgroups of G and G'

Definition 1.3.9. An **isomorphism** is a **bijective** homomorphism. A homomorphism is **bijective** iff it is both injective and surjective.

Proposition 1.3.10. If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is also an isomorphism.

Definition 1.3.11. Two groups G and G' are **isomorphic** iff there is an isomorphism $\varphi : G \to G'$.

Definition 1.3.12. An **automorphism** is an isomorphism $\varphi : G \to G$.

1.4 Cosets

Definition 1.4.1. Let H be a subgroup of G. The **left coset** of H induced by an element $a \in G$ is the set

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

The **right coset** of H induced by an element $a \in G$ is the set

$$Ha = \{ha|h \in H\}$$

Proposition 1.4.2. Let H be a subgroup of G. The left cosets partition G. The right cosets partition G.

Definition 1.4.3. For a subgroup H of G. The **index of** H **in** G denoted $[G : H]$ is the number of left cosets of H in G.

Lemma 1.4.4. All left cosets aH and all right cosets Ha of a subgroup H of a group G have the same order.

Lemma 1.4.5. Counting Formula. For a subgroup H of G we have

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

Theorem 1.4.6. Lagrange's Theorem. Let H be a subgroup of a finite group G. The order of H divides the order of G.

Corollary 1.4.7. The order of an element of a finite group divides the order of the group.

Corollary 1.4.8. If G is a group of prime order then for $a \in G$ where $a \neq \mathbb{I}$, we have $G = \langle a \rangle$.

Corollary 1.4.9. If $\varphi : G \to G'$ is a homomorphism of finite groups then

$$|G| = |\ker(\varphi)||\mathrm{Im}(\varphi)|$$

1.5 Normal Subgroups

Definition 1.5.1. A subgroup N of a group G is **normal** iff for every $a \in N$ and $g \in G$, $gag^{-1} \in N$.

Proposition 1.5.2. For any homomorphism $\varphi : G \to G'$ the $\ker(\varphi)$ is a normal subgroup of G.

Proposition 1.5.3. Let $H \subset G$ be a subgroup. Then the following are equivalent

1. H is a normal subgroup.
2. For all $g \in G$, $gHg^{-1} = H$
3. For all $G \in G$, $gH = Hg$
4. Every left coset of H in G is a right coset of H in G.

Corollary 1.5.4. If a group G has just one subgroup of order n, then that subgroup is normal.

1.6 Quotient Groups

Definition 1.6.1. Let $H \subset G$ be a subgroup. The **Quotient** is defined $G/H = \{\text{left cosets of } H\}$.

Proposition 1.6.2. If $H \subset G$ is a normal subgroup, then G/H is a group with law of composition $[aH][bH] = [abH]$.

Theorem 1.6.3. Correspondence Theorem Let $\varphi : G \to G'$ be a surjective homomorphism with kernal K. There is a bijective correspondence between subgroups of G' and subgroups of G that contain K.

$$\{\text{subgroups of } G \text{ that contain } K\} \leftrightarrow G/K$$

1.7 Product Groups

Definition 1.7.1. Let G and G' be groups, $G \times G'$ is the **product group** defined

$$G \times G' = \{(g, g')|g \in G, g' \in G'\}$$

with the law of composition

$$(a, a')(b, b') = (ab, a'b')$$

Proposition 1.7.2. Let G be a cyclic group of order mn where $\gcd(m, n) = 1$ then $G \equiv C_m \times C_n$.

Proposition 1.7.3. Let H, K be subgroups of a group G. Consider the multiplication map

$$f : H \times K \to G$$

given by $f(h, k) = hk$. Then

1. f is a homomorphism if an only if $kh = hk$ for all $h \in H$ and $k \in K$
2. f is injective if and only if $H \cap K = \{1\}$
3. if H is normal the image HK of f is a subgroup of G.

In particular, $G \cong H \times K$ under f if and only if $H \cap K = \{1\}$, $HK = G$ and K and H are both normal.

Proposition 1.7.4. The map $\pi : G \to G/N$ defined by $\pi(x) = [aN]$ such that $x \in aN$ is a surjective homomorphism with kernal N.

Theorem 1.7.5. First Isomorphism Theorem Let $\varphi : G \to G'$ be a surjective homomorphism and let N be its kernal.

$$G' \cong G/N$$

1.8 Group Actions

Definition 1.8.1. An **action** of a group G on a set S is a map

$$G \times S \to S$$

$$(g, s) \mapsto g * s$$

such that

1. $1 * s = s$ for all $s \in S$.
2. **Associativity**: $(gg') * s = g * (g * s)$ for all $g, g' \in G$ and $s \in S$.

Definition 1.8.2. Given an action of a group G on the set S, the **orbit** O_s of an element $s \in S$ is

$$O_s = \{gs \in S|g \in G\}$$

Definition 1.8.3. An action of G on S is **transitive** iff $S = O_s$ for some $s \in S$.

Definition 1.8.4. The **stabilizer** G_s of an element $s \in S$ is

$$G_s = \{g \in G|gs = s\}$$

Proposition 1.8.5. Let G be a subgroup of a group G.

1. The action of G on G/H is transitive.
2. The stabilizer $G_{[H]}$ of $[H]$ is the subgroup H.

Theorem 1.8.6. textbfOrbit Stabilizer Theorem Let G be a group action on a set S. For any $s \in S$, there is a bijection

$$\epsilon : G/G_s \leftrightarrow O_s$$

$$[aG_s] \mapsto as$$

such that $\epsilon(g[C]) = g\epsilon([C])$ for all $g \in G$ and $[C] \in G/G_s$

Corollary 1.8.7. Let G be a group acting on a finite set S. Then for any $s \in S$

$$|G| = |O_s||G_s|$$

1.9 Conjugation

Definition 1.9.1. The **conjugate** of $a \in G$ by $g \in G$ is gag^{-1}.

Definition 1.9.2. The **conjugation action** is the action of a group G defined by $G \times G \to G$ with $(g, x) \mapsto gxg^{-1}$.

Lemma 1.9.3. G is abelian $\Leftrightarrow$ conjugation map is the identity

Definition 1.9.4. The **centralizer** of x is the stabilizer of x under conjugation.

$$Z(x) = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$$

Definition 1.9.5. The conjugacy class of x is the orbit of x under conjugation.

$$C(x) = \{gxg^{-1} \in G | g \in G\}$$

Definition 1.9.6. The **center** of a group G is the subgroup

$$Z = \{z \in G | zg = gz \text{ for all } g \in G\}$$

Corollary 1.9.7. The center of a group is a normal subgroup.

Corollary 1.9.8. Every centralizer contains the center.

Proposition 1.9.9. The Class Equation The orbits of of conjugation partition the group.

$$|G| = \sum_{\text{conjugacy classes } C} |C|$$

1.10 p-Groups

Definition 1.10.1. A $p - group$ is a group of order p^n for some prime p.

Proposition 1.10.2. The center of a p-group is non-trivial.

Theorem 1.10.3. Fixed Point Theorem Let G be a p-group action on a finite set S If $|S|$ is not divisible by p, then there is a fixed point for the action of G on S.

Proposition 1.10.4. Every group of order p^2 is abelian.

Corollary 1.10.5. A group of order p^2 is either cyclic or a product of two cyclic groups

Definition 1.10.6. A subgroup $H \subset G$ of order p^e is called a **Sylow p-subgroup**.

Theorem 1.10.7. First Sylow Theorem A finite group whose order is divisible by a prime contains a Sylow p-subgroup.

Corollary 1.10.8. A group whose order is divisible by a prime p contains an element of order p.

Theorem 1.10.9. Second Sylow Theorem Let G be a finite group whose order is divisible by a prime p.

1. The Sylow p-subgroups of G are conjugate subgroups.
2. Every subgroup of G that is a p-group is contained in a Sylow p-subgroup.

Corollary 1.10.10. A group G has just one Sylow p-subgroup H if and only if H is normal.

Theorem 1.10.11. Third Sylow Theorem Let G be a finite group whose order $n = p^e m$, with p prime and p not dividing m. Let s be the number of Sylow p-subgroups of G. Then s divides m and $s \equiv 1 \mod p$.

Chapter 2

Field Theory

2.1 Rings and Fields

Definition 2.1.1. A **ring** R is a set with two laws of composition denoted $+$ and $\times$ that satisfy the following axioms:

- **Identity** $\exists$ elements denoted $0, 1 \in R$ such that $1 \times a = a$ and $0 + a = a$, $\forall\ a \in R$.
- **Additive Inverse** For all $a \in R$, there exists an element $-a \in R$ such that $-a + a = 0$.
- **Associativity** For all $a, b, c \in R$, $a \times (b \times c) = (a \times b) \times c$ and $a + (b + c) = (a + b) + c$.
- **Commutativity** For all $a, b \in R$, $a \times b = b \times a$ and $a + b = b + a$.
- **Distributivity** For all $a, b, c \in R$, $a \times (b + c) = (a \times b) + (a \times c)$.

Definition 2.1.2. A **field** F is a ring with at least two elements where every nonzero element has a multiplicative inverse.

- **Multiplicative Inverse** For all nonzero $a \in F$, there exists an element $a^{-1} \in R$ such that $a \times a^{-1} = 1$.

Definition 2.1.3. A **subring** H is a subset of a ring R with the following properties

- **Closure** For all $a, b \in H$, $a \times b, a + b \in H$.
- **Identity** $0, 1 \in H$.
- **Additive Inverse** For all $a \in H$, $-a \in H$.

Definition 2.1.4. A **subfield** H is a subring of a field F with at least two elements that contains multiplicative inverses of nonzero elements.

- **Multiplicative Inverse** For all $a \in H$, $a^{-1} \in H$.

Proposition 2.1.5. Let R be a ring. $0 = 1$ in R if and only if R is the zero ring.

2.2 Ring Homomorphisms

Definition 2.2.1. A **ring homomorphism** $\varphi : R \to R'$ is a map such that for all $a, b \in R$

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

Definition 2.2.2. A **ring isomorphism** is a bijective ring homomorphism.

Proposition 2.2.3. Let F be a field. If $f : F \to R$ is a ring homomorphism and R is nonzero, then f is injective.

Corollary 2.2.4. Any homomorphism between fields is injective.

2.3 Product Rings

Definition 2.3.1. Let R and R' be rings, $R \times R'$ is the **product ring** defined

$$R \times R' = \{(r, r') | r \in R, r' \in R'\}$$

with the laws of composition

$$(a, a') + (b, b') = (a + b, a' + b')$$
$$(a, a')(b, b') = (a \times b, a'b')$$

2.4 Quotient Rings

Definition 2.4.1. The **quotient ring** R/I where I is and ideal of the ring R is the ring of cosets of I with ring structure

$$(a+I)+(b+I)=(a+b+I)$$

$$(a+I)(b+I)=(ab+I)$$

Proposition 2.4.2. Let $f:R\to S$ be a ring homomorphism and R/I be a quotient ring, f defines a ring homomorphism $R/I\to S$ if an only if $I\subset\ker(f)$.

2.5 Characteristic

Definition 2.5.1. A field F has **characteristic** n iff $\sum^n 1=0$. Iff no such sum is possible a field has characteristic 0.

Proposition 2.5.2. The characteristic of a field must be prime.

Definition 2.5.3. For prime $p\in\mathbb{N}$, let $\mathbb{F}_p$ denote the field $\mathbb{Z}/(p)$.

Proposition 2.5.4. If a field F has characteristic $p>0$ then there exists a unique homomorphism $\mathbb{F}_p\to F$ and if $p=0$ then there exists a unique homomorphism $\mathbb{Q}\to F$.

2.6 Polynomial Rings

Definition 2.6.1. A **polynomial** with coefficients $a_i\in R$ in a ring R is a finite linear combination of powers of x^i

$$f(x)=a_nx^n+\cdots+a_1x+a_0$$

Definition 2.6.2. The **degree** of a polynomial f is the largest n such that $a_n\neq 0$.

Definition 2.6.3. A polynomial f is **monic** iff $a_n=1$ where $n=\deg f$.

Definition 2.6.4. For a ring R the **polynomial ring** denoted $R[x_1,\dots,x_r]$ is the ring of polynomials constructed from linear combinations of powers of the variables $x_1,\dots,x_r$.

Proposition 2.6.5. Let $x=(x_1,\dots,x_m)$ and $y=(y_1,\dots,y_n)$ be sets of variables. There is a unique isomorphism

$$R[x,y]\to R[x][y]$$

which is the identity on R and sends $x\mapsto x$, $y\mapsto y$.

2.7 Ideals

Definition 2.7.1. An **ideal** I of a ring R is an additive subgroup such that for all $s\in I$ and $r\in R$, $rs\in I$.

Definition 2.7.2. A **principle ideal** generated by an element $a\in R$ in a ring R is the ideal

$$(a)=aR=Ra=\{ra|r\in R\}$$

Proposition 2.7.3. The kernel of a ring homomorphism is an ideal.

Definition 2.7.4. An **ideal generated by** a set of elements $a_1,\dots,a_n\in R$ in a ring R is the ideal

$$(a_1,\dots,a_n)=\{r_1a_1+\cdots+r_na_n|r_1,\dots,r_n\in R\}$$

Definition 2.7.5. An ideal is **proper** iff it is neither $\{0\}$ nor R.

Proposition 2.7.6. A ring R is a field if and only if the only proper ideal is the zero ideal.

Definition 2.7.7. A **maximal ideal** M of a ring R is an ideal such that $M\neq R$ and there are not ideals I such that $M\subsetneq I\subsetneq R$.

Proposition 2.7.8. An ideal is maximal if and only if R/I is a field.

Theorem 2.7.9. If $I\times J=R$ where I, J are ideals.

$$R/(I\cap J)\cong R/I\times R/J$$

2.8 Integral Domains

Definition 2.8.1. A **domain** is a ring R such that $\forall a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$

Proposition 2.8.2. Any field is a domain.

Proposition 2.8.3. Any finite domain is a field.

Definition 2.8.4. An ideal I of a ring R is called **prime** iff R/P is a domain

Proposition 2.8.5. Any maximal ideal is prime.

Definition 2.8.6. A **principal ideal domain** is a domain R in which every ideal is principal.

Definition 2.8.7. A **euclidean domain** is a domain R a function $N : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that

1. $\forall x, y \in Rx \neq 0, \exists q, r \in R \text{s.t.} y = xq + r$
2. $\forall x, y \in Rx \neq 0, N(x) \leq N(xy)$

Theorem 2.8.8. Any euclidean domain is a principal ideal domain

Proposition 2.8.9. Let $p(x) \in F[x]$ and $\alpha \in F$ if $p(\alpha) = 0$ then $p(x) = (x - \alpha)q(x)$ for some $q(x) \in F[x]$

Definition 2.8.10. A **unique factorization domain** is a domain R such that any $x \in R$ can be factorized into irreducible elements uniquely up to units. That is there exists irreducible elements $\tau_1, \tau_2, \dots, \tau_n \in R$ such that $x = \tau_1\tau_2 \dots \tau_n$. Any for any other factorization $t_1, t_2, \dots, t_k \in R$, $n = k$ and $\exists \sigma \in S_n$ such that $t_i = u_i\tau_i$ for some unit $u_i \in R$.

Theorem 2.8.11. Any principle ideal domain is a unique factorization domain.

Theorem 2.8.12. If R is a unique factorization domain, then $R[x]$ is a unique factorization domain.

Corollary 2.8.13. If R is a unique factorization domain then $R[x_1, x_2, x_3, \dots]$ is a unique factorization domain.

Theorem 2.8.14. If $I \times J = R$ where I, J are ideals, then

$$R/(I \cap J) \cong R/I \times R/J$$

Corollary 2.8.15. If R is a PID, with elements $a, b \in R$ such that $\gcd(a, b) = 1$, then

$$R/(ab) \cong R/(a) \times R/(b)$$

2.9 Irreducibility

Definition 2.9.1. A **unit** is a ring R is an element which has a multiplicative inverse.

Proposition 2.9.2. If $x \in R$, x is a unit if and only if $(x) = R$.

Definition 2.9.3. An **irreducible** element $r \in R$ is a nonzero nonunit element where$x = ab$ implies a or b is a unit.

Theorem 2.9.4. If R is a principle ideal domain then a nonzero $I = (x)$ is maximal if and only if x is irreducible.

Lemma 2.9.5. Gauss's Lemma - If $p(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ then $p(x)$ is still irreducible in $\mathbb{Q}[x]$.

Lemma 2.9.6. Eisenstein's Criterion Let $p(x) \in \mathbb{Z}[x]$, let $\beta \in \mathbb{Z}$ be a prime. $p(x) = \sum_{i=0}^{n} a_i x^i$ If

$$\beta \not| a_n, \quad \beta | a_0, a_1, \dots, a_{n-1}, \quad \beta^2 \not| a_0$$

then $p(x)$ is irreducible.

2.10 Field Extensions

Definition 2.10.1. A **field extension** is an (injective) homomorphism between fields.

Proposition 2.10.2. If $F \to K$ is a field extension then K is a vector space over F.

Definition 2.10.3. An extension $F \to K$ is **simple algebraic** iff

$$K \cong F[x]/(p(x)) \quad \dim_F K = \deg p(x)$$

Definition 2.10.4. An extension $F \to K$ is **simple transcendental** iff

$$K \cong F(x) \quad \dim_F K = \infty$$

Definition 2.10.5. A element of a field $\alpha \in K$ is **algebraic** iff for some extension $F \to K$, $F \to F(\alpha)$ is simple algebraic

Definition 2.10.6. A element of a field $\alpha \in K$ is **transcendental** iff for some extension $F \to K$, $F \to F(\alpha)$ is simple transcendental.

Definition 2.10.7. An extension $F \to K$ is **algebraic** iff every element is $\alpha \in K$ is algebraic over F. In other words, $\exists p_\alpha(x) \in F[x]$ such that $p_{a\alpha}(\alpha) = 0$.

Proposition 2.10.8. If $F \to K$ is algebraic and $K \to L$ is algebraic then the composition $F \to L$ is algebraic.

Definition 2.10.9. The **degree** of a field extension is the dimension of the vector space formed.

Proposition 2.10.10. If $F \to K$ is a degree n field extension and $K \to L$ is a degree m extension, then $F \to K \to L$ is a degree mn extension.

Proposition 2.10.11. Every finite degree extension is a composition of simple algebraic extensions.

Proposition 2.10.12. Every finite degree extension is algebraic.

Definition 2.10.13. A polynomial $p(x) \in F[x]$ **splits** iff it factors into

$$c(x - r_1)(x - r_2) \ldots (x - r_n) \quad r_i \in F$$

Proposition 2.10.14. Let F be a field, $\exists$ field extension $F \to \Omega$ such that $p(x)$ splits as an element of $\Omega[x]$.

Definition 2.10.15. A field Ω is called algebraically closed iff every polynomial $p(x) \in \Omega[x]$ has a root in Ω.

Proposition 2.10.16. The following are equivalent:

1. Ω is algebraically closed.
2. Any polynomial $p(x) \in \Omega[x]$ splits.
3. The only irreducible polynomials in Ω are linear.
4. If $\Omega \to L$ is a finite field extension then $\Omega = L$.

Theorem 2.10.17. Fundamental Theorem of Algebra - $\mathbb{C}$ is algebraically closed.

Theorem 2.10.18. Any field can be embedded into any algebraically closed field.

Definition 2.10.19. An **algebraic closure** of a field F is an algebraic extension of F which is algebraically closed.

Theorem 2.10.20. Any field has an algebraic closure.

Definition 2.10.21. An **field automorphism** is an isomorphism from a field F to itself.

Proposition 2.10.22. If $\mathbb{Q} \to K$ is a finite field extension then

$$|\mathrm{Aut}(K)| \leq [K : Q]$$

where $\mathrm{Aut}(K)$ is the set of automorphisms on K.

2.11 Symmetric Polynomials

Definition 2.11.1. A polynomial $f \in K(x_1, x_2, \ldots, x_n)$ is **symmetric** iff $\forall \sigma \in S_n$,

$$f(x_1, x_2, \ldots, x_n) = f(x_{O(1)}, x_{O(2)}, \ldots, x_{O(n)})$$

Definition 2.11.2. The **elementary polynomial** $e_k \in F(x_1, x_2, \ldots, x_n)$ for $k \geq 0$ is the symmetric polynomial

$$e_k(x_1, x_2, \ldots, x_n) = \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq n} x_{j_1} x_{j_2} \ldots x_{j_k}$$

Theorem 2.11.3. Fundemental Theorem of Symmetric Polynomials Any symmetric polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ can be written uniquely as a linear combination of elementary symmetric polynomials with $\mathbb{Z}$ coefficients.

2.12 Noetherian Rings

Definition 2.12.1. A ring R is **noetherian** iff any ideal $I \subseteq R$ is finitely generated. That is $I = (r_1, r_2, \ldots, r_n)$ for $r_i \in R$.

Proposition 2.12.2. A ring R is noetherian if and only if any ascending chain of ideals stabilizes. That is if $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ is an infinite chain of ideals then for some $n \in \mathbb{N}$, $I_m = I_{m+1} \quad \forall m > n$.

Proposition 2.12.3. If R is a noetherian ring, then for any ideal $I \subseteq R$ any quotient R/I is noetherian.

Theorem 2.12.4. The **Hilbert Basis Theorem** states that if R is noetherian then $R[x]$ is noetherian.

Corollary 2.12.5. If R is noetherian and n is finite, then for any ideal $I \in R[x_1, x_2, \ldots, x_n]$, $R[x_1, x_2, \ldots, x_n]/I$ is noetherian.

Definition 2.12.6. A ring R is an **F-algebra** iff there exists a ring homomorphism $F \hookrightarrow A$ from some field F.

Definition 2.12.7. An F-algebra $F \hookrightarrow R$ is a **finitely generated F-algebra** if $\exists a_1, a_2, \ldots, a_n \in R$ such that any $r \in R$ can be produced by multiplying and adding elements of F and $a_1, a_2, \ldots, a_n$.

Corollary 2.12.8. Any finitely generated F-algebra is noetherian.

2.13 Modules

Definition 2.13.1. Let R be a ring. An **R-module** M is an abelian group with scalar multiplication $\times : R \times M \to M$ such that the following properties hold

1. $1 \times m = m, \quad \forall m \in M$
2. $r_1 \times (r_2 \times m) = c_1 c_2 \times m, \quad \forall m \in M, r_1, r_2 \in R$
3. $r \times (m_1 + m_2) = r \times m_1 + r \times m_2, \quad \forall m_1, m_2 \in M, r \in R$
4. $(r_1 + r_2) \times m = r_1 \times m + r_2 \times m, \quad \forall m \in M, r_1, r_2 \in R$

Definition 2.13.2. Let R be a ring. An **R-submodule** $N \subseteq M$ is an abelian subgroup such that $r \times n \in N \quad \forall r \in R, n \in N$

Definition 2.13.3. We say an R-module M is **finitely generated** if there are elements $m_1, m_2, \ldots, m_n \in M$ such that for any $x \in M$ there exists $r_i \in R$ such that $x = \sum_{i=1}^{n} r_i m_i$.

Definition 2.13.4. An **R-module homomorphism** $\varphi : M \to N$ is a map such that

1. φ is a group homomorphism.
2. $\varphi(r \times m) = r \times \varphi(m)$, $\forall r \in R$ and $\forall m \in M$.

Definition 2.13.5. The **direct sum** denoted $\oplus$ is the product group of two R-modules. Let M and N be R-modules the direct sum module is

$$M \oplus N = \{(m, n) | m \in M, n \in N\}$$

with the standard law of composition and scalar multiplication

$$r \times (m, n) = (r \times m, r \times n)$$

Definition 2.13.6. A **free R-module** is an R-module that is isomorphic to $R^n = R \oplus R \oplus R \oplus \cdots \oplus R$

Proposition 2.13.7. An R-module M is finely generate if and only if there exists a surjective homomorphism $R^n \twoheadrightarrow M$.

Definition 2.13.8. A **basis** is a set of elements $m_1, m_2, \ldots, m_n$ in an R-module M where every element in M is uniquely generated by a linear combination of $m_1, m_2, \ldots, m_n$.

Proposition 2.13.9. An $R[x]$-module uniquely determines and is determined by an R-module M and a homomorphism $T : M \to M$.

Definition 2.13.10. An R-module M is **Noetherian** if and only if any submodule $N \subset M$ is finitely generated.

Proposition 2.13.11. If R is Noetherian and m is a finitely generated R-module then M is Noetherian.

Theorem 2.13.12. Structure Theorem - If M is a fintely generated R-module where R is a principal ideal domain, then M is isomorphic to

$$M \cong R^n \oplus R/(d_1) \oplus R/(d_2) \oplus R/(d_3) \oplus \cdots \oplus R/(d_n)$$

for some $n, k > 0$ and $d_1, \ldots, d_k \in R$.

2.14 Linear Algebra

Proposition 2.14.1. Any R-module homomorphism $\varphi : R^m \to R^n$ equivalent to multiplication by some $n \times m$ matrix A.

Proposition 2.14.2. An $n \times n$ matrix A with entries in a ring R is invertible if and only if $\det(A)$ is a unit in R.

Proposition 2.14.3. For an $n \times m$ matrix A left multiplication by an $n \times n$ matrix S performs row operations on A and right multiplication by an $m \times m$ matrix T performs column operations on A.

Proposition 2.14.4. $\forall$ $n \times m$ matrix A, $\exists$ invertible matrices S and T such that SAT is diagonal.

Definition 2.14.5. An **eigenvector** of a linear transformation $T : V \to V$ on some F-module s a nonzero vector $v \in V$ such that $T(v) = \lambda v$ for some **eigenvalue** $\lambda \in F$

Definition 2.14.6. The **characteristic polynomial** of a linear transformation $T : V \to V$ acting on an F-module is

$$\mathrm{ch}_T(\lambda) = \det(T - \lambda I)$$

Proposition 2.14.7. If F is an algebraically closed field, then every $T : V \to V$ has an eigenvector.

Proposition 2.14.8. If $v_1, v_2, v_3, \ldots, v_k$ are eigenvectors with distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_k$ then $v_1, v_2, v_3, \ldots, v_k$ are linearly independent.

Corollary 2.14.9. If $\mathrm{ch}_T(\lambda)$ splits complete and has distinct roots then V has an eigenbasis.

Definition 2.14.10. A **generalized eigenvector** V for a linear transformation $T : V \to V$ acting on an F-module V is a nonzero vector such that $(T - \lambda I)^m v = 0$ for some $m \in [1, \dim V]$.

Theorem 2.14.11. Let T be a linear transformation acting on F-module V. If $\mathrm{ch}_T(t)$ splits completely then V has a basis of generalized eigenvectors.

Definition 2.14.12. The **minimal polynomial** $p_T(t)$ of a linear transformation $T : V \to V$ acting on an F-module V is the lowest degree polynomial such that $p_T(T) = 0$.

Theorem 2.14.13. Cayley-Hamilton Theorem - Let T be a linear transformation acting on F-module V.

$$p_T(t)|\mathrm{ch}_T(t), \quad \mathrm{ch}_T(T) = 0$$

Theorem 2.14.14. Let T be a linear transformation acting on F-module V. V has an eigenbasis if and only if $p_T(t)$ splits completely and has distinct roots.

Definition 2.14.15. A **Jordan block** are $n \times n$ matrices denoted $J_n(\lambda)$

$$J_m = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$$

Theorem 2.14.16. Jordan's Theorem Let F be algebraically closed and T be a linear transformation acting on F-module V. If $\mathrm{ch}_T(t)$ splits completely then $\exists$ a basis for V such that the matrix representation of T is block diagonal such that each block is a jordan block Jordan blocks (Jordan normal form).

Definition 2.14.17. the **companion matrix** of a polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is

$$\begin{pmatrix} 0 & 0 & 0 & -a_0/a_n \\ 1 & 0 & 0 & -a_1/a_n \\ 0 & 1 & 0 & -a_2/a_n \\ & & & \vdots \\ 0 & 0 & 1 & \\ 0 & 0 & 0 & -a_{n-1}/a_n \end{pmatrix}$$

Theorem 2.14.18. Let T be a linear transformation acting on F-module V. If $\mathrm{ch}_T(t)$ splits completely then $\exists$ a basis for V such that the matrix representation of T is block diagonal such that each block is a companion matrix for some monic polynomial.

Definition 2.14.19. A **projector** is a linear transformation $P : V \to V$ such that $P^2 = P$.

Proposition 2.14.20. If $P : V \to V$ is a projector then $V = \ker(P) \oplus \mathrm{im}(P)$.

Definition 2.14.21. The generalized eigenspace $V_\lambda \subseteq V$

$$V_\lambda = \{v \in V : (T - \lambda I)^m v = 0\}$$

Theorem 2.14.22. For each generalized eigenspace $V_\lambda \subset V$, there exists a projector $P : V \to V$ such that $P|_{V_\lambda} = I_{V_\lambda}$ and $P|_{V_\mu} = 0$ for $\mu \neq \lambda$.

Theorem 2.14.23. If $T : V \to V$ is a linear transformation such that $\mathrm{ch}_T(\lambda)$ splits

2.15 The Formal Derivative

Definition 2.15.1. The **discriminant** of a polynomial f denoted Δ is the symmetric polynomial

$$\Delta(f) = \prod_{i<j}^{n} (\alpha_i - \alpha_j)$$

where α_i are the roots of the polynomial f.

Proposition 2.15.2. $\Delta(f) = 0$ if and only if $f(x)$ has duplicate roots.

Definition 2.15.3. The **formal derivative** of a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ denoted $f'(x)$ is

$$f'(x) = a_n n x^{n-1} + a_{n-1}(n-1)x^{n-2} + \cdots + a_1$$

Proposition 2.15.4. The formal derivative satisfies the product rule, if $f, g \in F[x]$, then $D(fg) = fD(g) + gD(f)$.

Corollary 2.15.5. If F is a field of characteristic p then $D(x^p) = 0$.

Proposition 2.15.6. Let $f(x) \in F[x]$ with root $\alpha \in F$ such that $f(x) = (x - \alpha)q(x)$. $f'(\alpha) = 0$ if and only if $q(\alpha) = 0$.

Theorem 2.15.7. Let $f(x) \in F[x]$ such that f splits completely into linear factors in $K[x]$ where $F \subset K$ is some extension. The roots of f are distinct if and only if $\gcd(f, f') = 1$ in $F[x]$.

Chapter 3

Galois Theory

3.1 Finite Fields

Proposition 3.1.1. If F is a finite field ten $|F| = p^r$ for some prime $p = \text{char}(F)$ and some $r \in \mathbb{N}$.

Proposition 3.1.2. For a finite field F, $F^\times = F/\{0\}$ is a cyclic group.

Proposition 3.1.3. A field of characteristic p^r exists for any prime $p \in \mathbb{N}$ and $r \in \mathbb{N}$.

Proposition 3.1.4. A finite field F is a splitting field of $x^{p^r} - x$ for some prime $p = \text{char}(F)$ and some $r \in \mathbb{N}$.

3.2 Separable Extensions

Definition 3.2.1. A polynomial $f(x) \in F[x]$ is seperable iff it has distinct roots in K for some extension $F \subseteq K$.

Definition 3.2.2. A field F is perfect iff every irreducible polynomial in $F[x]$ is separable.

Proposition 3.2.3. Any finite field is perfect.

Proposition 3.2.4. Any field with characteristic zero is perfect.

Proposition 3.2.5. A field of characteristic p is perfect if and only if the Frobenius map $\phi : F \to F$ defined by $x \mapsto x^p$ is surjective.

Proposition 3.2.6. The only polynomials that can fail to be separable are of the form

$$f(x) = \sum_{i=0}^{n} a_i x^{ip}$$

Definition 3.2.7. For a ring homomorphism $\varphi : K \to L$ and a polynomial $p(x) \in K[x]$, let $p^\varphi(x)$ denote the polynomial

$$p^\varphi(x) = \varphi(a_n)x^n + \varphi(a_{n-1})x^{n-1} + \cdots + \varphi(a_1)x + \varphi(a_0)$$

Proposition 3.2.8. if $\alpha \in K$ is a root of $p(x) \in K[x]$ then $\varphi(\alpha)$ is a root of $p^\varphi(x) \in L[x]$.

Proposition 3.2.9. If $p(x) \in K[x]$ is separable then $p^\varphi(x)$ is separable.

Definition 3.2.10. Let $F \subseteq K$ be a field extension and $\alpha \in K$. We say α is **separable** over F iff the minimal polynomial $P_\alpha(x) \in F[x]$ such that $P_\alpha(\alpha) = 0$ is separable.

Definition 3.2.11. A field extension $F \subseteq K$ is **separable** iff every $\alpha \in K$ is separable.

Theorem 3.2.12. Let $F \subseteq K$ be a finite degree field extension. The following are equivalent

1. $F \subseteq K$ is a separable field extension.
2. $K = F(\alpha_0, \alpha_1, \alpha_2, \dots)$ such that $\alpha_0, \alpha_1, \alpha_2, \dots$ are separable.
3. $K = F(\alpha)$ such that α is separable.
4. The number of F embeddings $K \to \bar{F}$ is $[K : F]$.

Theorem 3.2.13. Primitive Element Theorem - If $F \subseteq K$ is a finite separable extension then $K = F(\alpha)$ for some primitive element $\alpha \in K$.

Proposition 3.2.14. Let $F \subseteq K \subseteq L$ be a tower of finite degree extensions. $F \subseteq K$ is separable if and only if $F \subseteq K$ and $K \subseteq L$ are separable.

3.3 Normal Extensions

Definition 3.3.1. A **splitting field** for a polynomial $f(x) \in F[x]$ is a finite extension $F \subseteq K$ such that

1. In $K[x]$, $f(x)$ splits completely
2. $K = F(a_1, a_2, \ldots, a_n)$

Proposition 3.3.2. A splitting field always exists

Proposition 3.3.3. Splitting fields are unique up to isomorphism

Definition 3.3.4. Let $F \subseteq K$ be a field extension. An F**-automorphism** $\varphi : K \to K$ is an automorphism such that it is the identity when restricted to F, $\varphi|_F = I_F$. The set of all F-automorphisms is denoted $\mathrm{Aut}_F(K)$.

Definition 3.3.5. A finite field extension $F \subseteq K$ is **normal** iff any irreducible polynomial $p(x) \in F[x]$ that has a root $\alpha \in K$ splits completely in $K[x]$.

Theorem 3.3.6. Let $F \subseteq K$ be a finite extension. The following are equivalent.

1. $F \subseteq K$ is a normal field extension.
2. All F-embeddings $\varphi : K \to \bar{F}$ have the same image.
3. K is a splitting field for some polynomial $f(x) \in F[x]$.

3.4 Galois Extensions

Definition 3.4.1. A field extension is **Galois** iff it is normal and separable.

Theorem 3.4.2. Let $F \subseteq K$ be a finite extension. The following are equivalent.

1. $F \subseteq K$ is Galois.
2. $|\mathrm{Aut}_F(K)| = [K : F]$
3. If $g(\alpha) = \alpha, \forall g \in \mathrm{Aut}_F(K)$ then $\alpha \in F$.

Definition 3.4.3. The **Galois group** of a Galois extension $F \subseteq K$ is the group of F-automorphisms denoted $\mathrm{Gal}(K/F)$.

Definition 3.4.4. The **conjugates** of α where $F \subseteq K$ is a Galois extension are the other roots of $P_\alpha(x) \in F[x]$.

Proposition 3.4.5. If $F \subseteq K$ is Galois then $L \subset K$ is also Galois for any intermediate field L.

Theorem 3.4.6. Fundamental Theorem of Galois Theory - If a fields extension $F \subseteq K$ is Galois then the poset of subfields is isomorphic to the poset of subgroups of the Galois group.

$$\{\text{intermediate fields } F \subseteq L \subseteq K\} \leftrightarrow \{\text{subgroups of } \mathrm{Gal}(K/F)\}$$

$$L \subseteq K \mapsto \mathrm{Gal}(K/L)$$
$$H \subseteq G \mapsto \{\alpha \in K | h(\alpha) = \alpha \forall h \in H\}$$

Proposition 3.4.7. Let $F \subseteq K$ be a Galois extension and let $g \in \mathrm{Aut}_F(K)$. If $\alpha \in K$ is a root of $p(x) \in F[x]$ then $g(\alpha)$ is also a root.

Proposition 3.4.8. Let $F \subseteq K$ be a Galois extension. If $f(x)$ gives K as its splitting field then $\mathrm{Aut}_F(K) \subseteq S_n$ for $n = \deg(f)$.

Proposition 3.4.9. Let $F \subseteq K$ be a Galois extension. If $f(x) \in F[x]$ is irreducible then for any two roots of f, $\alpha_1, \alpha_2 \in K$, there exists $g \in \mathrm{Aut}_F(K)$ sending $\alpha_1 \mapsto \alpha_2$.

Definition 3.4.10. A group action is **faithful** if there exists an injective homomorphism $G \hookrightarrow S_n$.

Theorem 3.4.11. Let $F \subseteq K$ be Galois, $f(x) \in F[x]$ be a polynomial that splits completely in $K[x]$ and let $R = \{\alpha \in K | f(\alpha) = 0\}$. For the action of $\mathrm{Gal}(K/F)$ on R.

1. K is the splitting field for $f(x)$ if and only if the action is faithful.
2. $f(x)$ is irreducible if and only if the action is transitive.

Theorem 3.4.12. Let L be an intermediate field $F \subseteq L \subseteq K$ of a Galoi extension $F \subseteq K$. $F \subseteq L$ is normal if and only if $\mathrm{Gal}(K/L)$ is a normal subgroup of $\mathrm{Gal}(K/F)$.

Theorem 3.4.13. There exists a Galois extension with Galois group S_n.

Theorem 3.4.14. Noether's Theorem - If you have an action of a finite group G on $\mathbb{Q}(S_1, S_2, \ldots, S_n)$ then there exists a Galois extension of $\mathbb{Q}$ wuth Galois group G.

Corollary 3.4.15. $\exists$ a Galois extension $\mathbb{Q} \subset K_n$ with Galois group S_n $\forall n \in \mathbb{N}$.

3.5 Trace and Norm

Definition 3.5.1. For a Galois extension $F \subset K$, the **trace** is an F-linear transformation $T : K \to K$ defined for $\alpha \in K$ by

$$T(\alpha) = \sum_{g \in \mathrm{Gal}(K/F)} g(\alpha) \in F$$

Definition 3.5.2. For a Galois extension $F \subset K$, the **Norm** is an F-linear transformation $N : K \to K$ defined for $\alpha \in K$ by

$$N(\alpha) = \prod_{g \in \mathrm{Gal}(K/F)} g(\alpha) \in F$$

Theorem 3.5.3. Hilbert's Theorem 90 - LEt $F \subseteq K$ be a Galois extension with cyclic Galois group $\mathrm{Gal}(K/F) = \{1, g, g^2, \dots, g^{n-1}\}$ for $\alpha \in K$,

$$N(\alpha) = 1 \quad \Leftrightarrow \quad \alpha = \frac{\beta}{g(\beta)}$$

$$T(\alpha) = 0 \quad \Leftrightarrow \quad \alpha = \beta - g(\beta)$$

5

Theorem 3.5.4. For a Galois extension $F \subset K$ and an element $\alpha \in K$, let $a_1, a_2, a_3, \dots, a_d$ be the coefficients of the minimal polynomial of m_α with degree d.

$$N(\alpha) = \det(m_\alpha) = a_1 a_2 a_3 \dots a_d$$

$$T(\alpha) = \mathrm{tr}(m_\alpha) = \frac{[K : F]}{d}(a_1 + a_2 + a_3 + \cdots + a_d)$$

Corollary 3.5.5. If m_α is the multiplication transformation of $\alpha \in K$ for a Galois extension $F \subset K$, then

$$\mathrm{ch}_{m_\alpha}(\lambda) = P_\alpha(\lambda)^{[K:F]/d}$$

Definition 3.5.6. Let G be a group, and let K be a field. A **character** is a group homomorphism $\chi : G \to K^\times$.

Proposition 3.5.7. The set of characters $\chi : G \to K^\times$ has a natural abelian group structure with law of composition

$$\chi_1 \circ \chi_2 = \chi_1(x)\chi_2(x)$$

Proposition 3.5.8. The set of all functions from a group G to a field K is a K-vector space with dimension $|G|$.

Theorem 3.5.9. Linear Interdependence of Characters The set of characters $\chi : G \to K^\times$ forms a basis in the vector space of all functions $G \to K$.

Proposition 3.5.10. The delta functions δ_g for each element $g \in G$, forms a basis in the vector space of all functions $G \to K$.

$$\delta_g(h) = \begin{cases} 1 & h = g \\ 0 & h \neq g \end{cases}$$

Theorem 3.5.11. The transformation between the delta basis and the basis of characters is the Fourier transform.

3.6 Constructable Extensions

Definition 3.6.1. An field K is **constructable** iff there exists intermediate degree 2 extensions K_i such that

$$0, 1 \subset K_1 \subset K_2 \subset K_3 \subset \cdots \subset K$$

Definition 3.6.2. An element $k \in K$ is **constructable** iff k is an element of a constructable field K.

Proposition 3.6.3. The fields $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}[i]$ are constructable.

Proposition 3.6.4. A complex number $z \in \mathbb{C}$ is constructable if and only if $|z|$, $\mathrm{Re}(z)$, and $\mathrm{Im}(z)$ are construtable.

Theorem 3.6.5. The set of constructable complex numbers is the smallest subfield of $\mathbb{C}$ that is closed under radicals and complex conjugation.

3.7 Kummer Theory

Proposition 3.7.1. Any subgroup of F^{times} is cyclic.

Definition 3.7.2. For a field F, the **roots of unity** $\zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$ are the roots of $x^n - 1$ in $F[x]$.

Proposition 3.7.3. If $\mathrm{char}(F) = 0, p$, $p \not| n$, then the order of the group of the nth roots of unity is n. If $\mathrm{char}(F) = 0$ and $p|n$, then $n = p^\ell k$ and the order the group of the nth roots of unity is k.

Proposition 3.7.4. There exists an injective group homomorphism

$$h : \mathrm{Gal}(F(\zeta_n)/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

Theorem 3.7.5. Kummer's Theorem Let F be a field containing ζ_n, the cyclic Galois extensions $F \subset K$ of degree $d|n$ are precisely the splitting fields of $x^n - a$ for $a \in F$.

Definition 3.7.6. An extension $F \subset K$ is **solvable** iff it can be created by a tower of Galois extensions with abelian Galois groups.

$$F \subset K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n = K$$

Definition 3.7.7. A group G is **solvable** iff there exists a tower of subgroups

$$\{e\} \subset G_0 \subset G_1 \subset \cdots \subset G_n = G$$

such that each G_i is a normal subgroup of G_{i+1} and G_{i+1}/G_i is abelian.

Definition 3.7.8. An extension $F \subset K$ is called **radical** if there exists a tower

$$F \subset K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n = K$$

such that each one $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ with $n_i \geq 2, a_i \in K_i$.

Definition 3.7.9. An extension $F \subset K$ is **solvable by radicals** if there exists a further extension $F \subset K \subset L$ such that $F \subset L$ is radical.

Proposition 3.7.10. If G is solvable then any subgroup $H \subset G$ and any quotient group G/N for normal $N \subset G$ is also solvable.

Theorem 3.7.11. Let $F \subset K$ be a finite Galois extension $F \subset K$ is solvable if and only if $\mathrm{Gal}(K/F)$ is a solvable group.

Corollary 3.7.12. Let $f(x) \in F[x]$ be irreducible and let $F \subset K$ be the splitting field of $f(x)$. If $\mathrm{Gal}(K/F)$ is a solvable group, then none of it's roots can be expressed by radicals.

Proposition 3.7.13. For a Galois extension $F \subset L$ and Galois algebraic closure $F \subset L \subset M$. If $F \subset L$ is radical, then $F \subset M$ is radical.