Rice University
Department of Mathematics

Introduction to UFDs, Modules, Finite Fields, and Galois Theory

Based on MATH 357 at Rice University

Author
Gabriel Gress

July 13, 2021

Contents

Chapter 0

Preamble

These notes covers modules, unital and commutative rings, and fields.

The lecture notes are based off two main sources. The overall outline and the major statements of theorems and definitions are based off lecture notes from Dr. Chelsea Walton during the Spring 2021 teaching of Rice's course MATH 357 – *Abstract Algebra II*. These notes are supplemented by exercises from Dummitt and Foote's *Abstract Algebra*, and some of the basic ring material is based on Goodman's *Algebra: Abstract and Concrete*. Finally, the applications of Galois theory are based on a section from Hungerford's *Algebra*.

Chapter 1

Modules

1.1 Ring Review

Recall the definition of a ring.

Definition 1.1.1: Ring

A **ring** is a nonempty set R with two operations: addition and multiplication, which has the properties

- R^+ is an abelian group
- $R^\times$ is a semigroup
- $\times$ distributes over $+$:

$$a(b+c) = ab + ac \quad (b+c)a = ba + ca$$

Definition 1.1.2: Types of Rings

A ring R is **commutative** if $\times$ is commutative. Furthermore, we say a ring is **unital** if there exists an element $1_R \in R$ so that $1_R a = a_{1_R} = a$ for all $a \in R$.

The ring R is **(in)finite** if it is (in)finite as a set.

A **subring** of R is an additive subgroup S of R that is closed under the multiplication of R. Furthermore, if it contains 1_R then it is a **unital subring**.

A **unit** of R is an element $a \in R$ that has a multiplicative inverse, i.e. $\exists b \in R$ so that $ab = ba = 1_R$. The set of units of R is sometimes denoted by $R^\times$.

In order to better classify commutative rings, we introduce a few more terminology.

Definition 1.1.3: Irreducibles and Primes

We say that $r \in R$ is **irreducible** if

$$r = ab \implies a \text{ or } b \text{ is a unit.}$$

We impose a stronger condition that $r \in R$ is **prime** if

$$r \mid ab \implies r \mid a \text{ or } r \mid b.$$

Note that every prime is irreducible, but not vice versa.

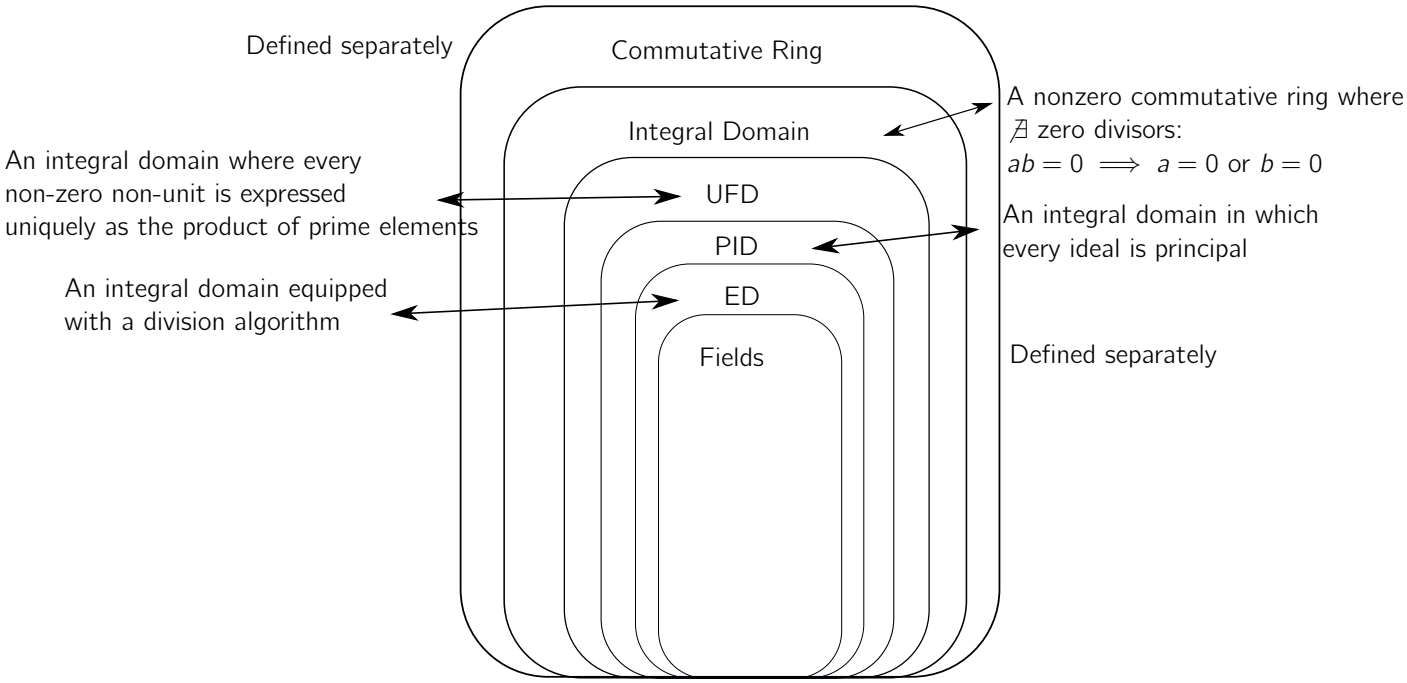


Figure 1.1: Hierarchy of Commutative Rings

1.2 Rings with Divison Structures

Definition 1.2.1: Norm of Integral Domain

Let R be an integral domain. Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0)$ is called a **norm** on the integral domain R. If $N(a) > 0$ for $a \neq 0$ then N is a **positive norm**

This is a pretty loose construction, and an integral domain can have many norms on it.

Definition 1.2.2: Euclidean Function

An integral domain R is a **Euclidean Domain** if there exists a norm called the **Euclidean function** $N : R \setminus \{0\} \to \mathbb{N}$ that satisfies $\forall a, b \in R \setminus \{0\}$:

$$N(ab) \geq \max\{N(a), N(b)\}$$
$$\exists q, r \in R \text{ such that } a = qb + r \text{ and } [r = 0 \text{ or } N(r) < N(b)]$$

We call the element q the **quotient** and the element r the **remainder**.

The existence of a Euclidean function is integral to constructing a Euclidean algorithm to perform division of elements $a, b \in R$. We can perform successive divisions to get

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

where r_n is the last nonzero remainder. This r_n always exists as the norms form a decreasing sequence of nonnegative integers. However, these elements are not necessarily unique.

Proposition 1.2.1

Every ideal in a Euclidean Domain is principal. That is, if $I \triangleleft R$ is a nontrivial ideal in R, then $I = (d)$ for some nonzero element of I with minimum norm.

This also makes it convenient to show an integral domain is not a Euclidean Domain by simply finding a non-principal ideal. Moreover, it motivates the notion of greatest common divisors from $\mathbb{Z}$ into comumutative rings.

Definition 1.2.3: Greatest Common Divisor

Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$. Then a is said to be a **multiple** of b if there exists an element $x \in R$ with $a = bx$. In this case, we say b **divides** a (or is a **divisor** of a) written $b \mid a$.

A **greatest common divisor** of a, b is a nonzero element d such that

$$d \mid a,\ d \mid b$$
$$d' \mid a\ d' \mid b \implies d' \mid d$$

We will denote a greatest common divisor by $\gcd(a, b)$, or sometimes simply (a, b) if it is clear from context.

If $gcd(a, b) = 1_R$, then we say that a and b are **relatively prime**.

We can easily extend this to finite sequences of elements $(a_1, a_2, \ldots, a_n)$.

Recall that in a ring $b \mid a \iff a \in (b) \iff (a) \subset (b)$. Hence, we can discuss greatest common factors in terms of ideals. That is, if $I = (a, b)$ is the ideal of R generated by a, b, then $d = \gcd(a, b)$ if $I \subset (d)$ and if $I \subset (d') \implies (d) \subset (d')$. Thus, it is the unique smallest principal ideal containing a and b. However, it may not exist in all rings.

Proposition 1.2.2: Sufficient Conditions for Existence

If $a, b \in R$ are nonzero elements in a commutative ring such that $I = (a, b) = (d)$, then d is the greatest common divisor of a, b.

Obviously this is a sufficient and not a necessary condition. But it also clarifies why (a, b) is used both for ideals and greatest common divisors. Any integral domain that satisfies the above condition for all ideals of two elements is called a **Bezout Domain**.

Proposition 1.2.3

Let R be an integral domain. If two elements $d, d' \in R$ generate the same principal ideal, i.e. $(d) = (d')$, then $d' = ud$ for some unit $u \in R$. In particular, this tells us that greatest common divisors are unique up to units.

Theorem 1.2.1

Let R be a Euclidean Domain and let $a, b \in R$ be nonzero. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a, b described earlier. Then $d = \gcd(a, b)$ and $(d) = (a, b)$. That is, d can be written as an R-**linear combination** of a, b:

$$d = ax + by$$

for some $x, y \in R$.

Notice that x, y are not unique in this case. One can show that that if x_0, y_0 are solutions to

$$ax + by = N$$

then any other solutions are of the form

$$x = x_0 + m\frac{b}{(a,b)}$$
$$y = y_0 - m\frac{a}{(a,b)}$$

for $m \in \mathbb{Z}$. This is really strong as it gives a complete solution of the first order Diophantine equation provided we have one solution. Our work here essentially tells us that $ax + by = N$ is solvable in integers x, y if and only if $\gcd(a, b) \mid N$.

Proof. ■

Finally, we discuss a definition that is useful to determine whether an integral domain is a Euclidean Domain.

Definition 1.2.4: Universal Side Divisor

Let R be an integral domain, and define $\tilde{R} = R^\times \cup \{0\}$. We say an element $u \in R - \tilde{R}$ is a **universal side divisor** if for every $x \in R$ there is a $z \in \tilde{R}$ such that

$$u \mid x - z$$

That is, every x can be written

$$x = qu + z$$

where z is either zero or a unit.

Proposition 1.2.4

Let R be an integral domain that is not a field. If R is a Euclidean Domain, then there exist universal side divisors in R.

It is often simpler to show that an integral domain can't have universal side divisors by assuming one exists of minimal norm, finding candidates, then showing they fail to satisfy the necessary properties.

Exercise 1.2.1

Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field with quadratic integer ring $\mathcal{O}$ and field norm N.

- Suppose $D \in \{-1, -2, -3, -7, -11\}$. Prove that $\mathcal{O}$ is a Euclidean Domain with respect to N.
- Suppose that $D \in \{-43, -67, -163\}$. Prove that $\mathcal{O}$ is not a Euclidean Domain with respect to any norm.

These numbers are specially chosen because they are the only negative values of D that makes every ideal in $\mathcal{O}$ principal.

1.2.1 Principal Ideal Domains

Definition 1.2.5: Principl Ideal Domain

A **Principal Ideal Domain** is an integral domain in which every ideal is principal.

We have already shown that every Euclidean Domain is a Principal Ideal Domain. The converse does not hold. The biggest difference from a practicality angle is that while PIDs have gcds, there is no algorithm to compute them.

Proposition 1.2.5

Let R be a Principal Ideal Domain and let $a, b \in R$ be nonzero. Let d be a generator for the principal ideal generated by a, b. Then $d = \gcd(a, b)$ and can be written as an R-linear combination

$$d = ax + by$$

for $x, y \in R$. Finally, d is unique up to multiplication by a unit.

Recall that maximal ideals are always prime ideals but the converse is not true in general. Fortunately, PIDs have enough structure so this holds.

Proposition 1.2.6

Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Proof. ■

Corollary 1.2.1

If R is any commutative ring such that $R[x]$ is a PID, then R is necessarily a field.

Proof. ■

We construct some definitions that help us distinguish PIDs and EDs.

Definition 1.2.6: Dedeking-Hasse Norm

Define N to be a **Dedekind-Hasse norm** if N is a positive norm and for every $a, b \in R$ nonzero either $a \in (b)$ or there exists $s, t \in R$ with $0 < N(sa - tb) < N(b)$ (that is, a nonzero element in the ideal (a, b) with norm smaller than b).

This is a weakening of the Euclidean condition. R is an ED with respect to a positive norm N if it is always possble to satisfy the above condition with $s = 1$.

Proposition 1.2.7

The integral domain R is a PID if and only if R has a Dedeking-Hasse norm.

Example 1.2.1

1.2.2 Unique Factorization Domain

Unique Factorization Domains capture the idea that some rings admit a proper factorization on elements.

Definition 1.2.7: Reducibility and Primes

Let R be an integral domain

- Suppose $r \in R$ is nonzero and not a unit. Then r is called **irreducible in** R if for all $a, b \in R$, $r = ab$ implies that either a or b is a unit. Otherwise, we say r is **reducible**.
- Let $p \in R$ be nonzero. We say it is **prime in** R if the ideal (p) is a prime ideal. An equivalent statement is that p is not a unit and if $p \mid ab$, then $p \mid a$ or $p \mid b$.
- If $a = ub$ for $a, b \in R$ and $u \in R$ a unit, then we say a and b are **associates**.

Proposition 1.2.8

In an integral domain, a prime element is always irreducible.

The converse does not hold in general. However, in a PID, the converse does hold.

Proof. ■

This is also a useful tool to show a ring is not a PID.

Definition 1.2.8: Proper Factorization

Let $a \in R$ be a nonzero nonunit. A **proper factorization** of a is a finite product $a = p_1 p_2 \dots p_n$, where p_i are not units of R. If this exists, we say $\{p_i\}$ are **proper factors** of a.

Of course, an irreducible element has no proper factorizations.

Definition 1.2.9: Unique Factorization Domain

An integral domain R is a **unique factorization domain** if every nonzero, non-unit element has a proper factorization

$$r = p_1 p_2 \dots p_n$$

where $\{p_i\}$ are irreducible elements and unique up to associates and reordering.

It turns out that primes are equivalent to irreducibles in a UFD as well.

Proposition 1.2.9

In a Unique Factorization Domain, a nonzero element is a prime if and only if it is an irreducible.

We will also see that UFDs admit a greatest common divisor via its factorization

Proposition 1.2.10

Let $a, b \in R$ be nonzero elements of a UFD R and suppose

$$a = u p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$
$$b = v p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$$

are prime factorizations with u, v units, primes $p_1, p_2, \dots, p_n$ distinct, and exponents $e_i, f_i \geq 0$. Then the element

$$d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_n^{\min(e_n, f_n)}$$

is a greatest common divisor of a and b.

Exercise 1.2.2

Let R be a UFD.

(a). Let b and $a_1, \dots, a_s$ be nonzero elements of R. For $d \in R$, show that

$$bd = gcd(ba_1, \dots, ba_s) \iff d = gcd(a_1, \dots, a_s)$$

(b). Let $f(x) \in R[x]$ where $f(x) = bf_1(x)$ for $f_1(x)$ **primitive** (i.e. $gcd(\text{coefficients of } f_1(x)) = 1_R$). Show that

$$b = gcd(\{\text{coefficients of } f(x)\}).$$

This leads us to the full description of the structure of these domains.

Theorem 1.2.2

Every Principal Ideal Domain is a Unique Factorization Domain. Hence, every Euclidean Domain is a Unique Factorization Domain.

Proof. ■

This forms a strict classification hierarchy by

Euclidean Domains $\subset$ **Principal Ideal Domains** $\subset$ **Unique Factorization Domains** $\subset$ **Integral Domains** $\subset$ **commutative rings**

Corollary 1.2.2

The integers $\mathbb{Z}$ are a UFD.

Corollary 1.2.3

Let R be a PID. Then there exists a multiplicative Dedekind-Hausse norm on R.

1.3 Properties of Ideals

Definition 1.3.1

Let $A \leq R$ be a subset of a ring R.

- The **ideal generated by** A is the smallest ideal of R containing A, written by (A).
- $$RA = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}_+\}$$
$$AR = \{a_1r_1 + a_2r_2 + \ldots + a_nr_n \mid a_i \in A,\ r_i \in R,\ n \in \mathbb{Z}_+\}$$
$$RAR = \{r_1a_1r_1' + r_2a_2r_2' + \ldots + r_na_nr_n' \mid r_i, r_i' \in R,\ a_i \in A,\ n \in \mathbb{Z}_+\}$$
  are the **left, right, and two-sided ideal generated by** A.
- If $|A| = n < \infty$, then (A) is a **finitely generated ideal**.
- If $|A| = 1$ then (A) is a **principal ideal**.

If $A = \{a_1, a_2, \ldots\}$ then we write $(A) = (a_1, a_2, \ldots)$ for simplicity. Notice that $b \in R$ is in (a) if and only if $b = ra$ for some $r \in R$, which is equivalent to $(b) \subset (a)$.

Proposition 1.3.1

Let $I \triangleleft R$. Then $I = R$ if and only if there exists a unit $u \in I$.

If R is commutative, then R is a field if and only if the only ideals of R are 0 and R.

Corollary 1.3.1

If R is a field and R' an arbitrary ring, then any nonzero ring homomorphism $\varphi : R \to R'$ is injective.

Definition 1.3.2: Maximal Ideal

A proper ideal M of a ring R is a **maximal ideal** of R if there does not exist another ideal of R that contains M besides R itself.

Every proper ideal is containd in a maximal ideal.

Theorem 1.3.1: Classification of Maximal Ideals

Let R be a commutative ring with identity and M an ideal in R. Then M is a maximal ideal of R if and only if R/M is a field.

Definition 1.3.3: Prime Ideal

A proper ideal P in a commutative ring R is a **prime ideal** if whenever $ab \in P$, then either $a \in P$ or $b \in P$.

Note that it is possible to define prime ideals in a noncommutative setting.

Proposition 1.3.2

Let R be a commutative ring with identity $1_R \neq 0$. Then P is a prime ideal in R if and only if R/P is an integral domain.

As an example, note that every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$, and that $\mathbb{Z}_n$ is an integral domain only when n is prime. This is why ideals of the form $\mathbb{Z}_p$ are viewed as prime ideals.

Corollary 1.3.2

Every maximal ideal in a commutative ring with identity is also a prime ideal.

For posterity we restate the definition of a polynomial ring.

Definition 1.3.4: Polynomial Ring

Let R be a commutative ring. We define a **polynomial** in x to be the formal sum

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

where $n \geq 0$ and $a_i \in R$. If $a_n \neq 0$, then the polynomial is of **degree** n, and $a_n x^n$ is te **leading term** (a_n is the **leading coefficient**). Furthermore, we say the polnyomial is **monic** if $a_n = 1$.

The set of all such polynomials is called the **ring of polynomials in** $\mathbb{R}$ and will be denoted $R[x]$. We define addition and multiplication by the standard version from algebra:

$$(a_n x^n + \ldots + a_1 x + a_0) + (b_n x^n + \ldots + b_1 x + b_0) = (a_n + b_n)x^n + \ldots + (a_1 + b_1)x + (a_0 + b_0)$$
$$(a_0 + a_1 x + a_2 x^2 + \ldots) \times (b_0 + b_1 x + b_2 x^2 + \ldots) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots$$

That is, the coefficient in the product of x^k is $\sum_{i=0}^{k} a_i b_{k-i}$.

Recall that $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ if $p, q \neq 0$. Furthermore, the units of $R[x]$ are the units of R, and $R[x]$ is an integral domain.

Proposition 1.3.3

Let $I \triangleleft R$ be an ideal and let $(I) = I[x]$ denote the ideal in $R[x]$ generated by I. Then

$$R[x]/(I) \cong (R/I)[x]$$

and hence if I is a prime ideal of R, (I) is a prime ideal of $R[x]$.

This does not hold for maximal ideals, but (I, x) is maximal in $R[x]$ if I is maximal in R.

Definition 1.3.5: Polynomial Rings over Multiple Variables

We inductively define the **polynomial ring in the variables** $x_1, x_2, \ldots, x_n$ with coefficients in R to be

$$R[x_1, x_2, \ldots, x_n] := R[x_1, x_2, \ldots, x_n][x_n]$$

Hence, we can view polynomial rings of multiple variables as polynomial rings on a single variable, with polynomials of $n-1$ variables as coefficients.

We say a polynomial is **homogeneous** if all its terms have the same degree. If f is a nonzero polynomial in n variables, the sum of all monomial terms in f of degree k is called the **homogeneous component of f of degree k**.

1.4 Polynomial Rings over Fields

Let $R = F$ be a field. We can define a natural norm on $F[x]$ by

$$N(p(x)) = \deg(p(x)).$$

Theorem 1.4.1

Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. This implies that if $a(x), b(x) \in F[x]$ with $b(x)$ nonzero, then

$$a(x) = q(x)b(x) + r(x)$$

where $q(x), r(x) \in F[x]$ are unique polynomials, and $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$.

Proof. ■

Of course, this tells us that $F[x]$ is a PID and a UID.

In fact, the quotient and remainder in the division algorithm are *independent of field extensions*. That is, if $F \subset E$ is a field extension, then $b(x) \mid a(x)$ in $E[x]$ if and only if $b(x) \mid a(x)$ in $F[x]$, and $\gcd(a(x), b(x))$ is the same in both fields.

Proposition 1.4.1

The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition 1.4.2

Let $g(x) \in F[x]$ be nonconstant and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \dots f_k(x)^{n_k}$$

be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \dots \times F[x]/(f_k(x)^{n_k}).$$

Notice that if $f(x)$ has roots $\alpha_1, \alpha_2, \dots, \alpha_k$ in F, then $f(x)$ has $(x-\alpha_1)\dots(x-\alpha_k)$ as a factor. In other words, a polynomial of degree n over a field has at most n roots in F.

Proposition 1.4.3

A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then $F^\times$ is a cyclic group.

Proof. ■

Corollary 1.4.1

Let p be a prime. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes $\pmod p$ is cyclic.

Corollary 1.4.2

Let $n \geq 2$ be an integer with factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

with $p_1, \dots, p_r$ are distinct. Then

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times,$$

in particular $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$ for all $\alpha \geq 2$.

Finally, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$ for all odd primes p.

These describe the group theory structure of the automorphism group of the cyclic group $\mathbb{Z}_n$, as $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. ■

1.5 Polynomial Rings and UFDs

Definition 1.5.1: Primitive

A polynomial $f(x) \in R[x]$ is **primitive** if $\gcd(\{\text{coeff of } f(x)\}) = 1_R$

Recall that since R is an integral domain, one can form its field of fractions by

$$F := \mathrm{Frac}(R) = \left\{ \frac{r}{s} \mid r, s \in R,\ s \neq 0 \right\}$$

Lemma 1.5.1: Gauss' Lemma

Let R be a UFD with $F = \mathrm{Frac}(R)$.

- If $f(x), g(x) \in R[x]$ are primitive, then so is $f(x) \cdot g(x)$.
- Take $f(x) \in R[x]$. Then $f(x) = \varphi(x)\psi(x) \in F[x]$ with $\deg(\varphi)\deg(\psi) \geq 1 \iff f(x) = \psi(x)\varphi(x)$ in $R[x]$.

The elements of the ring R become units in the UFD $F[x]$.

Corollary 1.5.1

Let R be a UFD. The irreducible elements of $R[x]$ are of two types:

- nonzero scalar polynomials that are irreducible as elements of R
- primitive polynomials in $R[x]$ that are irreducible in $F[x]$

Essentially, a polynomial $p(x)$ with $\deg(p(x)) \geq 1$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.

Theorem 1.5.1

R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.

Proof. ■

By induction, it holds that $R[x_1, x_2, \ldots, x_n]$ is a UFD if and only if R is a UFD.

1.6 Irreducibility Criteria

If R is an integral domain, then for $f(x) \in R[x]$ monic, of degree > 0, is irreducible if and only if $f(x)$ cannot be factored as a product of two polynomials of deg ≥ 1. Fortunately, we have a few tools to get irreducibility of polynomials, such as Gauss' Lemma.

Another direction we can take is roots:

Proposition 1.6.1

Let $f(x) \in F[x]$ for F a field. Then

- $f(x)$ has a degree 1 factor if and only if $f(x)$ has a root α in F, i.e. $\exists \alpha \in F$ such that $f(\alpha) = 0$
- $f(x)$ of degree 2 or 3 is reducible if and only if $f(x)$ has a root in F

If we look at $R = \mathbb{Z}$ and $F = \mathbb{Q}$ specifically, we have more options.

Proposition 1.6.2: Rational Root Test

Let $f(x) = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x]$.

- If $\frac{r}{s} \in \mathbb{Q}$ with $gcd(r, s) = 1$ and $\frac{r}{s}$ is a root of $f(x)$, then $r \mid a_0$ and $s \mid a_n$.
- If $f(x) \in Z[x]$ is monic and if $f(\alpha) \neq 0$ for all $\alpha \in \mathbb{Z}$ dividing α_0, then $f(x)$ has no roots in $\mathbb{Q}$.

Unfortunately, while these theorems are powerful, they are relatively dependent on the polynomial being of low degree. Ideals can help us extend these ideas to higher degree polynomials.

Proposition 1.6.3

Let R be an integral domain, and let $I \triangleleft R$ be a proper ideal of R. Take $f(x) \in R[x]$ a monic polynomial of degree ≥ 1. If the image of $f(x)$ in $(R/I)[x]$ is irreducible, then $f(x)$ is irreducible in $R[x]$.

While nice, unfortunately many irreducible polynomials are reducible when modulated by the ideal.

Theorem 1.6.1: Eisenstein-Schonemann Criteria

Let P be a prime ideal of an integral domain R, and take

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

to be a monic polynomial in $R[x]$ of degree ≥ 1. Suppose $a_{n-1}, \ldots, a_1, a_0 \in P$ and $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.

A trick we can use to help apply this is that if $f(x)$ doesn't satisfy the criteria, use $f(x-c)$ and try again. If it is (ir)reducible for $f(x-c)$, it is ir(reducible) for $f(x)$.

1.7 Modules

An R-module M is an abelian group that comes equipped with a binary operation $\cdot$ that maps from $R \times M$ to M that is compatible with operations of both M and R. It is the natural generalization of vector spaces to rings, but with the key difference that we may not have multiplicative inverses for elements in our R-module.

Definition 1.7.1: Left R-module

Let R be a ring. A **left R-module** is a pair ${}_R M := (M, \cdot : R \times M \to M)$ where M is an abelian group, and $\cdot$ is a binary operation so that

$$\begin{aligned} \forall r, s \in R,\ m, n \in M : \\ r \cdot (m+n) &= (r \cdot m) + (r \cdot n) \\ (r+s) \cdot m &= (r \cdot m) + (s \cdot m) \\ (rs) \cdot m &= r \cdot (s \cdot m) \end{aligned}$$

If R is unital, then we also require

$$1_R \cdot m = m.$$

The map is called the (left) R-**action map**.

Example 1.7.1: Free Module of Rank n

1. If R is a field F, then the R-module is an F-vector space.
2. Take $M = R^n := \{(t_1, \ldots, t_n) \mid t_i \in R\}$. Let the R-action map of ${}_R M$ be defined by

$$\begin{aligned} R \times M &\to M \\ (r, (t_1, \ldots, t_n)) &\mapsto (rt_1, \ldots, rt_n). \end{aligned}$$

One can check that this satisfies the necessary properties of a left R-action on $M = R^n$. This left R-module ${}_R R^n$ (which we will simply denote here on out by R^n) is called the **free left R-module of rank n**.

Example 1.7.2: $\mathbb{Z}$-Modules

An abelian group M can be made into a module ${}_{\mathbb{Z}}M$ over the integers in exactly one way. Consider the $\mathbb{Z}$-action map defined by

$$\begin{aligned} \mathbb{Z} \times M &\to M \\ (n, m) &\mapsto m + \ldots_n + m \end{aligned}$$

One can check that this indeed is a $\mathbb{Z}$-module over M.

Exercise 1.7.1

Prove that the $\mathbb{Z}$-action given above is the unique $\mathbb{Z}$-action for any $\mathbb{Z}$-module. Furthermore, show that ${}_{\mathbb{Z}}M$ is isomorphic to an abelian group.

Example 1.7.3: $F[x]$ Modules

Let $R = F[x]$ be a polynomial ring over a field F, and let V be a vector space over F with a linear operator $T \in \mathcal{L}(V)$. We can construct an $F[x]$-module on V via T (denoted ${}_{F[x]}V$)). To see this, let $p(x) \in F[x]$ be a polynomial given by

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

For each $v \in V$, we define the action of $p(x)$ on v by

$$\begin{aligned} p(x) \cdot v &= (a_n T^n + a_{n-1} T^{n-1} + \ldots + a_1 T + a_0)(v) \\ &= a_n T^n(v) + a_{n-1} T^{n-1}(v) + \ldots + a_1 T(v) + a_0 v \end{aligned}$$

Informally, we are defining an action of x on V by T, and then extending it onto $F[x]$ in a natural way.

Recall that $F \leq F[x]$ (as constant polynomials), and hence the action of F is exactly the same as constant polynomials, which correspond to the standard action of F on V. In other words, this action is an extension of the action of F onto a larger ring $F[x]$.

Because this action is dependent on the choice of T, this gives us many different $F[x]$-module structures on the same vector space V. One can check that $T = 0$ also yields us the standard action of F on V.

What is interesting to note is that the action of $F[x]$ via T encapsules *all* possible $F[x]$-modules– this holds because the action of $x \in F[x]$ on V is a linear transformation from V to V, and hence must correspond to some T which all actions $p(x)$ must adhere to.

One might ask what $F[x]$-submodules look like. We can see immediately that an $F[x]$-submodule ${}_{F[x]}W \leq {}_{F[x]}V$ must also be an F-submodule, and hence $W < V$ as a vector subspace. Furthermore, in order for it to be well-defined, W must be T-**invariant**, that is, $T(W) \subset W$. In fact this too is a bijection, so that all $F[x]$-submodules of V correspond to T-invariant subspaces of V.

This example shows that the ideal structure of $F[x]$ greatly restricts the module structure on V (and in fact can be used to derive its Jordan canonical form). In fact, the reasonings above can be applied to any PID R, and in the special case $R = \mathbb{Z}$ we can obtain the fundamental theorem of finitely generated abelian groups. In general, it is always interesting to see how the structure of a ring R will affect its modules.

1.8 Substructures of Modules

Definition 1.8.1: Submodule

Let R be a ring, let ${}_RM$ be a left R-module, and let $N \leq M$ be a subgroup of M. A R-**submodule of** ${}_RM$ is the R-module ${}_RN$ with the same R-action from ${}_RM$.

In other words, it is a subgroup with closure under the R-action.

Proposition 1.8.1: Submodule Criterion

Take a ring R with 1_R, and left R-module M. A subset N of M can be made into a R-submodule of M if and only if

- $N \neq \emptyset$ and
- $n + rn' \in N$ for all $r \in R$, $n, n' \in N$.

Proposition 1.8.2

Let M be an R-module, and let ${}_RN_i$ with $i \in I$ be R-submodules of M. Then

1. $\bigcap_{i\in I} {}_RN_i$ is an R-submodule of M
2. $\bigcup_{i\in I} {}_RN_i$ is not necessarily an R-submodule of ${}_RM$
3. If ${}_RN_1 \subset {}_RN_2 \subset {}_RN_3 \subset \ldots$ is an increasing chain of R-submodules of M, then $\bigcup_{i\in\mathbb{N}} {}_RN_i$ is an R-submodule of ${}_RM$
4. Let $N_1 + N_2 = \{n_1 + n_2 \mid n_1 \in N_1, n_2 \in N_2\}$ be the sum of N_1 and N_2. Then $N_1 + N_2$ can be made into an R-submodule of M.

Exercise 1.8.1

The submodules of the R-module ${}_RR$ are ${}_RI$ where $I \triangleleft R$ is an ideal.

1.9 R-module homomorphisms

Definition 1.9.1

Let R be a ring, and let ${}_RM$ and ${}_RN$ be R-modules. An R-**module homomorphism** is a group homomorphism

$$\varphi : M \to N \quad [\varphi(m + m') = \varphi(m) + \varphi(m')]$$

so that R-action is preserved. That is, for all $r \in R$, $m, m' \in M$, the group homomorphism satisfies:

$$[\varphi(rm) = r\varphi(m)]$$

for all $r \in R$, $m, m' \in M$.

The **kernel** of φ is

$$\mathrm{Ker}\varphi = \{m \in M \mid \varphi(m) = 0\},$$

and the **image** of φ is

$$\mathrm{Im}(\varphi) = \{\varphi(m) \mid m \in M\}.$$

The set of R-module homomorphisms from ${}_RM$ to ${}_RN$ is denoted by $\mathrm{Hom}_R(M,N)$. An R-**module isomorphism** is a bijective R-module homomorphism (trivial kernel and full range).

Example 1.9.1: $\mathbb{Z}$-submodules

Recall that any group homomorphism between abelian groups can be represented as a $\mathbb{Z}$-module homomorphism. Hence, if ${}_{\mathbb{Z}}N$ is a submodule of ${}_{\mathbb{Z}}M$, then $N \leq M$.

Exercise 1.9.1

If $\varphi \in \mathrm{Hom}_R(M,N)$ and $\psi \in \mathrm{Hom}_R(N,P)$ then $\psi \circ \varphi \in \mathrm{Hom}_R(M,P)$.

1.10 Quotient Modules and Isomorphism Theorems

Proposition 1.10.1: Modules of homomorphisms

Let R be a ring, and take R-modules ${}_RM$ and ${}_RN$.

1. If $\varphi, \psi \in \mathrm{Hom}_R(M,N)$, then define
$$(\varphi+\psi)(m) := \varphi(m)+\psi(m) \quad \forall m \in M$$
$$(r\varphi)(m) := r\varphi(m) \quad \forall r \in R, m \in M$$
This gives $\mathrm{Hom}_R(M,N)$ the structure of an R-module, which we denote by ${}_R\mathrm{Hom}_R(M,N)$.
2. We denote $\mathrm{Hom}_R(M,M)$ by $\mathrm{End}_R(M)$. We get that $\mathrm{End}_R(M)$ is a ring with addition defined as above, and multiplication as defined in the exercise. We call this the **endomorphism ring of** M, and elements are **endomorphisms**.

There is a structure that combines being an R-module and a ring, which we call R-algebras.

Definition 1.10.1: R-algebra

Let R be a commutative ring with 1_R. A **(unital)** R-**algebra** is a unital ring A equipped with a unital ring homomorphism $f : R \to A$ such that the subring $f(R) \leq A$ is contained in the center $Z(A)$.

It is easy to see that A has a natural R-module structure given by $ra \mapsto f(r)a$. This is not the only module structure, but it is the most natural.

Example 1.10.1: Endomorphism

If R is commutative, then ${}_R\mathrm{End}_R(M)$ is an R-algebra via the action of function composition $r\varphi \mapsto r(\varphi(m))$.

The unital ring homomorphism from $R \to \mathrm{End}_R(M)$ is given by $r \mapsto r \cdot \mathrm{Id}$, where Id is the identity endomorphism. When R has an identity, this gives $\mathrm{End}_R(M)$ an R-algebra structure, as the image is clearly in the center of $\mathrm{End}_R(M)$.

Notice that it isn't necessarily injective, as $rm = 0$ is possible. If R is a field, however, it will be injective in which case the image is the **subring of scalar transformations**.

Definition 1.10.2: R-algebra homomorphism

If A, B are two R-algebras, an **R-algebra homomorphism** is a ring homomorphism $\varphi : A \to B$ such that, for all $r \in R$ and $a \in A$:

$$\varphi(r \cdot a) = r \cdot \varphi(a).$$

It follows that if A is an R-algebra, then it satisfies $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$ because $f(r)$ is in the center. If these conditions hold for a ring, then it defines an R-algebra– hence it can be considered an alternate definition.

1.10.1 Quotient Modules

Proposition 1.10.2

Take R as a ring, and ${}_RM$ an R-module with R-submodule ${}_RN$.

1. The quotient group M/N can be made into an R-module ${}_R(M/N)$ via

$$\begin{aligned} R \times M/N &\to M/N \\ (r, m+N) &\mapsto rm+N \quad \forall r \in R,\ m+N \in M/N \end{aligned}$$

2. The canonical projection map of groups

$$\begin{aligned} \pi : M &\to M/N \\ m &\mapsto m+N \quad \forall m \in M \end{aligned}$$

   is a surjective R-module map, with $\mathrm{Ker}\pi = N$.

Theorem 1.10.1: Module Isomorphism Theorems

Let R be a ring, and ${}_RM, {}_RN$ to be R-modules.

(i). If $\varphi \in \mathrm{Hom}_R(M, N)$, then ${}_R\mathrm{Ker}\varphi$ is a R-submodule of M, and $M/\mathrm{Ker}\varphi \overset{R}{\cong} \varphi(M)$ as R-modules (by R-module isomorphism).

(ii). If ${}_RA, {}_RB$ are R-submodules of M, then $(A+B)/B \overset{R}{\cong} A/(A \cap B)$ as R-modules.

(iii). If ${}_RA, {}_RB$ are R-submodules of M and $A \subset B$, then

$$(M/A)/(B/A) \overset{R}{\cong} M/B$$

as R-modules.

(iv). Suppose ${}_RN$ is an R-submodule of ${}_RM$. Then there exists a bijection:

$$\{\text{submodules } {}_RA \text{ of } {}_RM \text{ containing } {}_RN\} \iff \{\text{submodules } {}_R(A/N) \text{ of } {}_R(M/N)\}.$$

1.10.2 Direct Products

Let R be a ring with 1_R.

Proposition 1.10.3

Let ${}_RM$ be an R-module, with ${}_RN_1, \ldots, {}_RN_t$ as R-submodules. Then

(i). The sum of $\{N_i\}_{i=1}$ is

$$N_1 + \ldots + N_t = \{n_1 + \ldots + n_t \mid n_i \in N_i,\ i = 1, \ldots, t\}$$

and forms an R-module.

(ii). The direct product of $\{N_i\}$ is

$$N_1 \times \ldots \times N_t = \{(n_1, \ldots, n_t) \mid n_i \in N_i,\ i = 1, \ldots, t\}$$

and forms an R-module.

One can also define the direct product of R-modules (i.e. not just submodules).

Proposition 1.10.4

Let ${}_RN_1, \ldots, {}_RN_t$ be R-submodules of an R-module ${}_RM$. Then the following are equivalent:

(i).

$$\begin{aligned} \varphi : N_1 \times \ldots \times N_t &\to N_1 + \ldots + N_t \\ (n_1, \ldots, n_t) &\mapsto n_1 + \ldots + n_t \end{aligned}$$

is an R-module isomorphism

(ii). $N_j \cap (N_1 + \ldots + N_{j-1} + N_{j+1} + \ldots N_t) = 0$ for all $j = 1, \ldots, t$

(iii). Every $x \in N_1 + \ldots + N_t$ can be written as $n_1 + \ldots + n_t$ uniquely for some $n_i \in N_i$ for all $i = 1, \ldots, t$

If the proposition holds, then

$$N_1 \times \ldots \times N_t \overset{R}{\cong} N_1 + \ldots + N_t$$

and we refer to the structure as the direct sum of R-modules.

1.11 Generating Sets

Definition 1.11.1

Take an R-module ${}_RM$ and a subset $X \subset M$.

1. The R-**submodule generated by** X is

$$RX = \{r_1x_1 + \ldots + r_mx_m \mid r_i \in R,\ x_i \in X,\ m \in \mathbb{Z} > 0\}.$$

The set X is called the **generating set** of RX.

2. A R-submodule ${}_RN$ of ${}_RM$ is **finitely generated** if $N = RX$ for $|X| < \infty$ and **cyclic** if $N = RX$ for $|X| = 1$.

1.11.1 Free Modules

Definition 1.11.2: Linear independence by R-modules

We say that $X = \{x_1, \ldots, x_n\}$ is R-**linearly independent** if

$$r_1x_1 + \ldots + r_nx_n = 0 \implies r_i = 0 \quad \forall i = 1, \ldots, n$$

Definition 1.11.3

We say that an R-module ${}_RM$ is **free on the subset** X of M if

$$M = RX$$
$$X \text{ is } R\text{-linearly independent}$$

In this case, we call X the **basis** of ${}_RM$, and sometimes denote ${}_RM$ by $F_R(X)$.

If R is commutative, then we call $|X|$ the **rank** of ${}_RM$.

This illustrates a key difference between vector spaces and modules– vector spaces are always free, while modules need not be.

Example 1.11.1: Free and non-free modules

Most modules have no basis! A free $\mathbb{Z}$-module is also called a **free abelian group**; lattices in $\mathbb{R}^2$ are free abelian groups, while finite, non-zero abelian groups are not free.

Definition 1.11.4: R-Matrix

Let R be a ring. An R-**matrix** is a matrix whose entries are in R. An **invertible** R-**matrix** is an R-matrix that has an inverse that is also an R-matrix. The $n \times n$ invertible R-matrices form a group called the **general linear group over** R:

$$GL_n(R) = \{n \times n \text{ invertible } R\text{-matrices}\}.$$

The **determinant** of an R-matrix $A = (a_{ij})$ is defined in the usual way

$$\det(A) = \sum_p \pm a_{1,p1} \ldots a_{n,pn}.$$

or the sum over all permutations of the indices and the sign being the sign of the permutation. Of course, all the usual properties of determinants hold for R-matrices.

Lemma 1.11.1

Le R be a non-zero ring. Then a square R-matrix A is invertible if and only if it has either a left inverse or a right inverse, and only if its determinant is a unit of the ring. Furthermore, an invertible R-matrix is square.

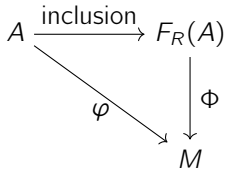
Proposition 1.11.1: Free modules and R-matrices

Let R be a non-zero ring. Then the matrix P of a change of basis in a free module is an invertible R-matrix. Furthermore, any two bases of the same free module over R have the same cardinality.

Every homomorphism f between two free modules is given by left multiplication by an R-matrix.

Theorem 1.11.1: Universal Property of Free Modules

For any set A there is a free R-module $F_R(A)$ on the set A and $F_R(A)$ satisfies the *universal property*: if ${}_RM$ is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F_R(A) \to M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$. In other words, the following diagram commutes:



Furthermore, if $A = \{a_1, \ldots, a_n\}$, then

$$F_R(A) = Ra_1 \oplus Ra_2 \oplus \ldots \oplus Ra_n \overset{R}{\cong} R^n$$

This corresponds to the notion of free groups from group theory.

Exercise 1.11.1

If F_R, F'_R are free modules on the same set A, there is a unique isomorphism between F_R and F'_R which is the identity map on A.

If ${}_RF$ is any free R-module with basis A, then ${}_RF \cong F_R(A)$.

If we have a free R-module with a basis A, the above statement says that we can define R-module homomorphisms from the free module into other R-modules by simply specifying how the homomorphism acts on elements of A.

The free module $F_{\mathbb{Z}}(A)$ is called the **free abelian group on** A. If A is finite, then we say it is of **rank** $|A|$ and is isomorphic to

$$\mathbb{Z} \oplus \ldots^n \oplus \mathbb{Z}.$$

Chapter 2

Group Representation Theory

2.1 Ties to Group Representation Theory

If, when taking an R-module M, we may work over a field K and modify $M = V$ to be a K-vector space by $K \times V \to V$. This then gives us that an R-module over V is a pair V with $R \times V \to V$.

Definition 2.1.1: Group Module

Let G be a group. We say that a K-vector space V is a G-**module** if it comes equipped with a G-action map

$$G \times V \to V \quad (g, v) \mapsto g * v := gv$$

compatible with operations of G and V :

(a). $e_G v = v$

(b). $(gh)v = g(hv)$

(c). $g(v + w) = gv + gw$

(d). $g(\lambda v) = \lambda(gv)$

for all $g, h \in G$, $v \in V$, $\lambda \in K$.

If one is given a G-module V, then there is a natural group homomorphism

$$\rho : G \to \mathrm{End}_K(V)$$
$$g \mapsto [\rho g : V \to V,\ v \mapsto g * v := gv]$$

The image of ρ is inside of $GL(V)$.

Definition 2.1.2

A K-**linear representation of a group** G is a K-vector space V equipped with a group homomorphism $\rho : G \to GL(V)$.

Definition 2.1.3

Given a representation of a group G, $(V : \rho)$, its **degree** is $\dim V$.

Note that when $\dim_K V = n$, we get that

$$GL(V) \cong GL_n(K)$$

as groups.

Representations of G of degree n over a field K are congruent to group homomorphisms $\rho : G \to GL_n(K)$.

Definition 2.1.4

For any group G, the **trivial representation of** G **over** K is $(V = K, \rho : G \to GL_1(K) = K^\times)$ given by $g \mapsto 1_K$ for all $g \in G$.

Definition 2.1.5

Let $\rho : G \to GL(V)$ and $\rho' : G \to GL(V')$ be two representatives of a group G. We say that p and p' are **equivalent** or isomorphic if there exists an invertible linear transformation

$$\tau : V \to V'$$

so that τ **intertwines** with action of G :

$$\tau(\rho g(v)) = \rho' g(\tau(v)) \quad \forall g \in G, v \in V$$

Remark 2.1.1

$\rho : G \to GL_n(K)$ and $\rho' : G \to GL_{n'}(K)$ are equivalent if and only if $n = n'$ and $\exists T \in GL_n(K)$ such that $T\rho(g)T^{-1} = \rho'(g)$ for all $g \in G$.

This notion will be captured more clearly later with homomorphism/isomorphisms.

2.2 Subrepresentations and Irreducibility

Let K be a field and G a group. Recall that if $\dim_K V = n$, we can identify the group $GL(V)$ with $GL_n(K)$, the group of invertible K-linear operators on V under composition.

Definition 2.2.1: Subrepresentations

Let $\rho : G \to GL(V)$ be a representation of G. Suppose that W is a subspace of V which is G-invariant. That is, for all $w \in W$, $g \in G$, it holds that $\rho_g(w) \in W$. Then W becomes a representation of G and we say that

$$(W, \rho w : G \to GL(W))$$
$$g \mapsto [\rho_g \mid W : W \to W \quad w \mapsto \rho_g(w)]$$

is a **subrepresentation** of (V, ρ).

Definition 2.2.2

The **direct sum** of two representations of G, (V', ρ'_V) and (V'', ρ''_V) is the representation of G given by:

$$(V := V' \bigoplus V'', \rho_{V' \bigoplus V''} : G \to GL(V))$$
$$g \mapsto \left[\rho_g : V \to V \quad v = v' + v'' \mapsto \rho'_g(v') + \rho''_g(v'')\right]$$

If we fix a basis for both V' and V'', then their union is a basis of $V = V' \bigoplus V''$.

Definition 2.2.3: Irreducible

A representation is called **irreducible** if it contains no proper subrepresentations– otherwise it is called **reducible**. A representation is called **completely reducible** if it decomposes as a direct sum of irreducible subrepresentations.

Irreducible representations will turn out to be the building blocks of group representation theory. This is complemented by Mascinke's Theorem, which will state that every $\mathbb{C}$-linear representation of a finite group G of finite degree is completely reducible.

2.3 Complete Reducibility

Recall that the **characteristic** of a field K is the smallest positive integer p such that $p1_K = 0$. If p exists, then it is prime; else we say K has characteristic 0.

Theorem 2.3.1

Let (V, ρ) be a representation of a finite group G of finite degree n over a field K of characteristic p with $p \not| |G|$. If W is a subrepresentation of (V, ρ), then there exists another subrepresentation W' of V so that

$$V \cong W \bigoplus W'$$

as K-vector spaces. We refer to W' as the **complement** of the subrepresentation W of (V, ρ).

Corollary 2.3.1: Maschke's Theorem

Let V be a representation of a finite group G of finite degree over a field of characteristic p with $p \not| |G|$. Then V is completely reducible.

This can be proven by induction on $\dim V$. Note that this fails for infinite groups.

2.4 G-homomorphisms

Let K be a field and G be a group. We are going to look at a structure of interest: we define K-linear representations of G as a K-vector space V equipped with a group homomorphism

$$\rho : G \to GL(V)$$
$$g \mapsto [\rho g : V \to V]$$

Definition 2.4.1: G-homomorphism

Let (V', ρ') and (V'', ρ'') be representations of G over K. A G-**homomorphism from** (V', ρ') **to** $V'', \rho'')$ is a K linear map $\varphi : V' \to V''$ which intertwines with the action of G :

$$\varphi(\rho' g(v')) = \rho'' g(\varphi(v')) \quad \forall g \in G, v' \in V'$$

We denote the collection of G-homomorphisms from (V', ρ') to (V'', ρ'') by $\mathrm{Hom}_G(V', V'')$, and $\mathrm{End}_G(V') := \mathrm{Hom}_G(V', V')$. Finally, a G-**isomorphism** is an invertible G-homomorphism.

This is really just a change in basis.

Proposition 2.4.1

If $\varphi \in \mathrm{Hom}_G(V, W)$, then $\varphi^{-1} \in \mathrm{Hom}_G(W, V)$.

Proposition 2.4.2

Take $\varphi \in \mathrm{Hom}_G(V, W)$. Then

(a). $\mathrm{Ker}\varphi$ is a subrepresentation of V, and

(b). $\mathrm{Im}\varphi$ is a subrepresentation of W.

For the rest of the section, we take $K = \mathbb{C}$.

Lemma 2.4.1: Schur's Lemma

Let (V, ρ) be an irreducible representation of G. If $\varphi \in \mathrm{End}_G(V)$, then φ is a scalar multiple of $\mathrm{Id}V$:

$$\exists \lambda \in \mathbb{C} \; s.t. \; \varphi(v) = \lambda v \quad \forall v \in V$$

This result has many applications.

Theorem 2.4.1

All nonzero complex irreducible representations of an abelian group G have degree 1.

Using these tools, we now can complete a few problems.

Exercise 2.4.1

Given a finite abelian group G, describe its irreducible representations, up to equivalence. Illustrate this for the Klein-four group $G = C_2 \times C_2$.

Moreover, one can apply Schur's lemma to complete the following problem:

Exercise 2.4.2

Let V and W be irreducible representations of G, and take $\varphi \in \mathrm{Hom}_G(V, W)$. Show that

(a). If $V \ncong W$, then φ is the zero map.

(b). If $V \cong W$ and $\varphi \neq 0$, then φ is a G-isomorphism.

2.5 Character Theory

Character theory will serve as a very convenient bookkeeping tool for representations of G when G is finite. We still keep $K = \mathbb{C}$.

Definition 2.5.1

Let (V, ρ) be a $\mathbb{C}$-representation of G of finite degree n. Choose any basis of V and express ρ_g as a matrix in $GL_n(\mathbb{C})$, for all $g \in G$. The **character of** (V, ρ), denoted X_V is the function

$$\begin{aligned} X_V : G &\to \mathbb{C} \\ g &\mapsto \mathrm{Tr}(\rho g) \end{aligned}$$

We say that X_V is **irreducible** if (V, ρ) is irreducible.

It turns out that characters detect irreducibility. Let X_V, ψ_W be given. We define a scalar by

$$\langle X_V, \psi_W \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{X_V(g)} \psi_W(g).$$

Proposition 2.5.1

Let V be a representation of G. Then

$$V \text{ is irreducible} \iff \langle X_V, X_V \rangle = 1.$$

Of course, we need to be sure that our construction of characters is well-defined. It turns out that they capture the properties of our representation well and are unique.

Proposition 2.5.2

1. The definition of X_V is independent of choice of basis of V
2. If $V \cong W$, then $X_V = X_W$
3. If $g, h \in G$ are conjugate, then $X_V(g) = X_V(h)$

Definition 2.5.2

The **character table** of G is defined as

$$\begin{bmatrix} X_{V_1}(g_1) & X_{V_1}(g_2) & \dots & X_{V_1}(g_k) \\ \vdots & & & \vdots \\ X_{V_\ell}(g_1) & X_{V_\ell}(g_2) & \dots & X_{V_\ell}(g_k) \end{bmatrix}$$

The number of irreducible characters of G is the same as the number of conjugacy classes of elements of G. Furthermore, the character table is a square matrix with entries in $\mathbb{C}$ when the rows are indexed by irreducible representations of G and the columns are indexed by conjugacy classes representations of elements of G.

In this case, $(X_{V_i}(g_j))$ is an invertible matrix.

Proposition 2.5.3

Let (V, ρ) be a representation of G, and take $g \in G$. Then

1. $X_V(e) = \dim(V)$
2. $X_V(g)$ is a sum of roots of unity
3. $X_{V \oplus W}(g) = X_V(g) + X_W(g)$
4. $X_V(g^{-1}) = \overline{X_V(g)}$
5. $\overline{X_V}$ is a character of G

Let $X_1, \dots, X_r$ be irreducible characters of a finite group G. Define

$$\langle X_i, X_j \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{X_i(g)} X_j(g)$$

Theorem 2.5.1

1. $\langle X_i, X_j \rangle = \delta_{ij}$
2. $$\sum_{i=1}^{r} \overline{X_i(x)} X_i(y) = \begin{cases} |C_G(x)| & x, y \text{ conjugate in } G \\ 0 & \text{otherwise} \end{cases}$$

Here, $C_G(x)$ is the centralizer of $x \in G$, that is, $C_G(x) = \mathrm{Stab}_x(G) = \{g \in G \mid gxg^{-1} = x\}$.

Theorem 2.5.2

If V, W are irreducible representations of G, then

$$\langle X_V, X_V \rangle = 1$$
$$\langle X_V, X_W \rangle = 0 \text{ when } V \ncong W$$

This shows us that characters completely determine representations, and forthermore characters completely determine irreducibility.

Chapter 3

Field Extensions

Recall the definition of a field.

Definition 3.0.1

A **field** is a commutative ring F with multiplicative identity 1_F in which every nonzero element has a multiplicative inverse.

Furthermore, recall that the **characteristic** of a field F, denoted $\mathrm{char}(F)$, is the smallest positive integer n such that

$$1_F + 1_F + \ldots_n + 1_F = 0_F$$

if such an $n \in \mathbb{N}$ exists. Otherwise, we say that $\mathrm{char}(F) = 0$.

Proposition 3.0.1

For a field F, we have that $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) = p$ for a prime integer p. If $\mathrm{char}(F) = p$, then $p \cdot \alpha = \alpha + \ldots_p + \alpha = 0_F$ for all $\alpha \in F$.

We often refer to fields with prime characteristics as **fields of positive characteristic**.

Some fields of characteristic zero include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Any field of the form $\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ is a field of characteristic p.

3.1 Subfields

Definition 3.1.1

A **subfield** of a field F is a nonempty subset S containing 1_F that is a subring under the addition and multiplication of F, and so that S is closed under taking multiplicative inverse.

The **prime subfield** of a field F is the subfield generated by the multiplicative identity 1_F of F, that is, it is the smallest subfield of F containing 1_F.

Proposition 3.1.1

The prime subfield of a field F is either $\mathbb{Q}$ if $\mathrm{char}(F) = 0$, or $\mathbb{F}_p$ if $\mathrm{char}(F) = p$.

Definition 3.1.2

A **homomorphism** $\Phi : F_1 \to F_2$ **between fields** F_1 **and** F_2 is a unital ring homomorphism: $\forall x, y \in F_1$

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$
$$\varphi(xy) = \varphi(x)\varphi(y), \quad \varphi(1_{F_1}) = 1_{F_2}$$

Notice that either $F \cong \mathrm{Im}(\varphi)$ or $0 \cong \mathrm{Im}(\varphi)$. This follows from the fact that the only ideals of F are 0 and F.

A lot of fields are better viewed via a ring homomorphism. We can quotient out a ring R by any maximal ideal I of R to get an object isomorphic to a field.

Example 3.1.1

Consider the principal ideal domain $\mathbb{Q}[x]$. For any irreducible polynomial $p(x)$, we have that

$$\mathbb{Q}[x]/(p(x))$$

is a field, where $(p(x))$ denotes the root of $p(x)$. We can in fact see that this space is equivalent to $\mathbb{Q}$ but including the roots of $x^2 - 2$, namely $\sqrt{2}$. One can construct a unital isomorphism so that

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$$

3.2 Extension of Fields

Definition 3.2.1

If K is a field containing a subfield F, then K is said to be an **extension of** F, denoted by K/F.

The field F is sometimes called the **base field** of the extension.

Note that if K is an extension of a field F, then K is a F-vector space via the typical F action.

Definition 3.2.2

The **degree** or **index** of a field extension K/F, denoted $[K : F]$, is defined to be $\dim_F K$, the dimension of K as an F-vector space.

For example, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{C} : \mathbb{R}] = 2$. One can see the latter example by observing that $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$.

Theorem 3.2.1

Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial. Then $\exists$ a field extension K of F in which $p(x)$ has a root.

This field is given by $K := F[x]/(p(x))$, but we will show this more formally later.

Theorem 3.2.2

Let $p(x) \in F[x]$ be an irreducible polynomial of degree over F, and let K be the field $F[x]/(p(x))$. Take $\theta := x + (p(x))$ (root of $p(x)$). Then

1. The elements $\left\{1_F, \theta, \theta^2, \ldots, \theta^{n-1}\right\}$ are an F-vector space basis of the F-vector space K.
2. $[K : F] = n$
3. $K = \left\{a_0 + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1} \mid a_0, \ldots, a_{n-1} \in F\right\}$ as an F-vector space.

Another nice example to be familiar with is $K = \mathbb{F}_2[x]/(x^2 + x + 1)$. This is a field extension of $\mathbb{F}_2$ as $x^2 + x + 1$ is irreducible in $\mathbb{F}_2$. We can see that $[\mathbb{F}_2[x]/(x^2 + x + 1) : \mathbb{F}_2[x]] = 2$ simply because the degree of the polynomial is 2, but we can also directly count elements in the set and see that it has twice the elements of $\mathbb{F}_2[x]$.

Now let's define fields formed by adjoining roots more formally.

Definition 3.2.3

Let K/F be a field extension, and let $\alpha_1, \alpha_2, \ldots \in K$ be elements. The smallest subfield of K containing both F and the elements $\alpha_1, \alpha_2, \ldots$, denoted $F(\alpha_1, \alpha_2, \ldots)$ is called the **field generated by** $\alpha_1, \alpha_2, \ldots$ **over** F.

Definition 3.2.4

The field $F(\alpha)$ generated by a single element α over F is called a **simple extension of** F, and the element α in this case is called **primitive**.

Theorem 3.2.3

Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension of F containing a root α of $p(x)$. Then $F[x]/(p(x)) \cong F(\alpha)$.

It is natural to view field extensions as the base field appended with roots, and as a result a few definitions arise.

Definition 3.2.5: Algebraic and Transcendental Elements

An element $\alpha \in K$ is called **algebraic over** F if α is a root of some nonzero polynomial $f(x) \in F[x]$.

If $\alpha \in K$ is not algebraic over F, then we say that α is **transcendental over** F.

The extension K/F is **algebraic over** F if all elements of K are algebraic over F.

Example 3.2.1: Examples of Algebraic and Transcendental Elements

- $\sqrt{2}$ is an algebraic element over $\mathbb{Q}$ via the polynomial $x^2 - 2$. This actually holds for all $\sqrt[n]{2}$ with $x^n - 2$.
- i is algebraic over $\mathbb{R}$ and $\mathbb{Q}$ via the polynomial $x^2 + 1$
- Transcendental elements are much rarer– examples include π and e, but it is non-trivial to show an element is transcendental.

3.3 Minimal Polynomials

Proposition 3.3.1

Let α be an algebraic element over F.

(a). Then there exists a monic irreducible polynomial of minimal degree $m_{\alpha,F}(x) \in F[x]$ which has α as a root.

(b). A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x) \mid f(x)$ in $F[x]$.

(c). The polynomial $m_{\alpha,F}(x)$ with the property in (a) is unique.

We can see the minimal polynomial must be irreducible, because otherwise one of its factors would have α as a root and hence has degree smaller than $m_{\alpha,F}(x)$, contradicting our hypothesis. The divisibility $m_{\alpha,F}(x) \mid f(x)$ follows from the division algorithm in $F[x]$. The divisibility and minimality conditions together give uniqueness.

Corollary 3.3.1

If K/F is a field extension, and α is algebraic over both F and K, then $m_{\alpha,K}(x)$ divides $m_{\alpha,F}(x)$ in $K[x]$.

This directly follows as $m_{\alpha,F}(x)$ has a root α in K and hence (b) gives us divisibility.

Definition 3.3.1

The polynomial $m_{\alpha,F}(x)$ is called the **minimal polynomial of α over F**. The degree of $m_\alpha(x)$ is called the **degree of α**.

In other words, the minimal polynomial of α over F is a monic irreducible polynomial over F that has α as a root. Alternatively, it is a monic polynomial over F of minimal degree with α as a root– both imply the other.

Proposition 3.3.2

Let α be algebraic over F. Then

$$F(\alpha) \cong F[x]/(m_\alpha(x))$$

So that $[F(\alpha) : F] = \deg m_\alpha(x) \equiv \deg\alpha$.

Proposition 3.3.3

An element $\alpha \in F$ is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite.

If $\alpha \in K$ with $[K : F] = n$, then $\deg(\alpha) \leq n$.

This follows by applying linear dependence to powers α^i with $i = 0, 1, \ldots, n$.

Corollary 3.3.2

If K/F is finite, then K/F is algebraic.

Example 3.3.1

Take F to be a field with $\mathrm{char}(F) \neq 2$. Consider K/F of degree 2, which is hence algebraic. Let $\alpha \in K/F$ so that α is a root of a polynomial over F of degree 1 or 2. Because $\alpha \notin F$, the polynomial must has degree 2.

This implies that $m_{\alpha,F}(x) = x^2 + bx + c$ for $b, c \in F$. This implies that $F(\alpha)$ has the same dimension of K and hence $K = F(\alpha)$ (as K is a field extension of $F(\alpha)$. This implies that $K = F(\sqrt{b^2 - 4ac})$ and so any degree 2 extension of a field F with characteristic not equal to 2 is of the form $F(\sqrt{D})$ for D a non-square element of F.

Conversely, for such a field, $[F(\sqrt{D}) : F] = 2$ and hence extensions of the form $F(\sqrt{D})/F$ are called **quadratic extensions of F**.

3.4 Algebraic Extensions

Theorem 3.4.1: Tower Theorem

Let $F \hookrightarrow E \hookrightarrow K$ be a composition of field extensions. Then $[K : F] = [K : E][E : F]$.

One can show this via vector space arguments (look at the bases of the spaces).

Corollary 3.4.1

If K/F is a finite extension, and E is a subfield of K containing F, then $[E : F] \mid [K : F]$.

Example 3.4.1

Let

$$K = \mathbb{Q}(\sqrt[6]{2})$$
$$E = \mathbb{Q}(\sqrt{2})$$
$$F = \mathbb{Q}$$

It follow directly from previous work that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. As for K/E, the minimal polynomial is $x^3 - \sqrt{2}$, which gives $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$, which corresponds to what the tower theorem gives us.

Definition 3.4.1

An extension K/F is called **finitely generated** if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that

$$K = F(\alpha_1, \alpha_2, \ldots, \alpha_n) \quad \text{for } n < \infty$$

Such an extension can be obtained recursively via simple extensions.

We have that $F(\alpha, \beta) = (F(\alpha))(\beta)$, hence the definition above is consistent.

Example 3.4.2

- $\mathbb{Q}(\sqrt[6]{2}, \sqrt{2}) = \left(\mathbb{Q}(\sqrt[6]{2})\right)(\sqrt{2}) = \mathbb{Q}(\sqrt[6]{2})$ because $\sqrt{2} = (\sqrt[6]{2})^3$.
- One can check that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a proper field extension for both $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$.

Theorem 3.4.2

K/F is finite if and only if K is generated by a finite number of algebraic elements over F.

We denote by $\overline{\mathbb{Q}}$ the subfield of $\mathbb{C}$ generated by all algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$. $\overline{\mathbb{Q}}$ is an infinite algebraic extension of $\mathbb{Q}$, and referred to as the **field of algebraic numbers**.

Theorem 3.4.3

If E/F and K/E are algebraic, then K/F is algebraic.

3.5 Composite Field Extensions

Definition 3.5.1: Composite Field

Let K_1 and K_2 be two subfields of a field K. Then the **composite field of** K_1 **and** K_2, denoted by K_1K_2 is the smallest subfield of K containing both K_1 and K_2.

The composite of any collection of subfields $\{K_i\}$ is defined similarly.

Proposition 3.5.1

Let K_1 and K_2 be two finite extensions of F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F-vector space basis for K_1 is linearly independent over K_2 (or vice versa).

If the F-vector space basis of K_1 is $\alpha_1, \ldots, \alpha_n$ and the F-vector space basis of K_2 is $\beta_1, \ldots, \beta_m$, then $\{\alpha_i\beta_j\}_{i,j=1}^{n,m}$ is a F-vector span of K_1K_2.

Corollary 3.5.1

If, furthermore, $[K_1 : F] = n$ and $[K_2 : F] = m$ with $\gcd(n, m) = 1$, then $[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$.

Example 3.5.1

- Consider $K = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2})$. We have

$$\mathbb{Q} \hookrightarrow^2 \mathbb{Q}(\sqrt{2}) \hookrightarrow^3 \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$$
$$\mathbb{Q} \hookrightarrow^3 \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow^2 \mathbb{Q}(\sqrt[6]{2})$$
$$\mathbb{Q} \hookrightarrow^6 \mathbb{Q}(\sqrt[6]{2})$$

  where $\hookrightarrow^k$ represents a degree k extension.

3.6 Splitting Fields

Recall that for any field F and any polynomial $f(x) \in F[x]$, there exists a field extension K over F that contains a root, say $\alpha \in K$, of $f(x)$. In this case, $f(x) = (x - \alpha)g(x)$ in $K[x]$ as $K[x]$ is a Euclidean domain.

Now we want a field extension K/F so that $f(x) \in F[x]$ splits completely into linear factors in $K[x]$.

Definition 3.6.1

A field extension K of F is called a **splitting field for** $f(x) \in F[x]$ if $f(x) = \prod_i (x - \alpha_i)$ in $K[x]$ and $f(x)$ does NOT factor completely in $K'[x]$ for any proper subfield K' of K.

$f(x) \in K[x]$ splits completely if and only if K contains all roots of $f(x)$.

Example 3.6.1

- The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$
- The splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
- The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is NOT $\mathbb{Q}(\sqrt[3]{2})$. The roots $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$ are in fact imaginary and hence are not in $\mathbb{Q}(\sqrt[3]{2})$ (note that ω represents the principal root of unity).

Theorem 3.6.1

Splitting fields always exist. For any field F, if $f(x) \in F[x]$, then there exists a field extension K of F that is a splitting field for $f(x)$.

Proposition 3.6.1

Take $f(x) \in F[x]$ of degree n. Then for $K :=$ splitting field of $f(x)$, we get that $[K : F] \leq n!$.

Now we discuss the uniqueness of splitting fields.

Theorem 3.6.2

Let $\varphi : F \to F'$ be an isomorphism of fields. Let

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in F[x]$$
$$f'(x) = \varphi(a_n)x^n + \ldots + \varphi(a_1)x + \varphi(a_0) \in F'[x].$$

Let E be the splitting field of $f(x)$ over F and E' be the splitting field of $f'(x)$ over F'. Then the isomorphism φ extens to an isomorphism $\sigma : E \to E'$, so that $\sigma \mid_F = \varphi$.

This can be proven by induction on the degree of $f(x)$.

Corollary 3.6.1

Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.

Thus we can safely refer to -the- splitting field of a polynomial over a field.

Definition 3.6.2

If K is an algebraic extension of F, which is the splitting field over F for a collection of polynomials $\{f_i(x)\} \in F[x]$, then K is called a **normal** extension of F.

In other words, a normal extension is simply an algebraic extension that is also a splitting field.

Exercise 3.6.1

Determine the splitting field of $x^6 - 4$ over $\mathbb{Q}$ and its degree over $\mathbb{Q}$.

We now focus on the splitting field of $x^n - 1$ in $\mathbb{Q}[x]$. Roots of $x^n - 1$ are of the form $\left\{e^{2\pi ik/n} \mid k = 0, 1, \ldots, n-1\right\}$. Some useful notation:

1. $\zeta_n := e^{2\pi i/n}$, the primitive n-th root of 1
2. $\mu_n := \langle \zeta_n \rangle$, the cyclic group of order n under multiplication with identity 1
3. $\varphi(n)$ is the number of integers between $1, \ldots, n$ that are coprime– the Euler-Phi function.

Definition 3.6.3: Cyclotomic Field

The **cyclotomic field of n-th roots of unity** or the **n-th cyclotomic field** is $\mathbb{Q}(\zeta_n)$.

The **n-th cyclometric polynomial** is

$$\Phi_n(x) = \prod_{\zeta \text{primitive} \in \mu_n} (x - \zeta).$$

Recall that an n-th root of 1 (that is, $e^{2\pi ik/n}$) is primitive if and only if $(k, n) = 1$. We conventionally choose 1 to be a primitive.

Theorem 3.6.3

(a). $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$

(b). $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible

(c). The minimal polynomial of a primitive n-th root of unity over $\mathbb{Q}$ is $\Phi_n(x)$

(d). $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

These will be proved in various ways by later constructions.

Corollary 3.6.2

$$\Phi_n(x) = (x^n - 1) \Big/ \prod_{d|n, d<n} \Phi_d(x)$$

We can compute $\Phi_n(x)$ inductively.

As an example, for a prime p:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

3.7 Algebraic Closure

Before, we were looking at extensions of some polynomial in $F[x]$ that contains all the roots of the polynomial. Now we consider field extensions that contain *all* the roots of all $f(x) \in F[x]$.

Definition 3.7.1: Algebraic Closure

Given a field F, a field $\overline{F}$ is the **algebraic closure** of F if

(a). $\overline{F}$ is algebraic over F,

(b). Every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$

Recall that splitting completely implies that $f(x)$ factors into a product of degree 1 polynomials.

Definition 3.7.2: Algebraically Closed

A field K is **algebraically closed** if every polynomial with coefficients in K has a root in K.

Proposition 3.7.1

If $\overline{F}$ is the algebraic closure of F, then $\overline{F}$ is algebraically closed.

Exercise 3.7.1

For a field K, the following are equivalent:

- K is algebraically closed
- Every $f(x) \in K[x]$ nonconstant splits completely over K
- Every irreducible $f(x) \in K[x]$ has degree 1
- There does not exist an algebraic extension of K other than K itself

Proposition 3.7.2

For every field F there exists an algebraically closed field K containing F.

Exercise 3.7.2

Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$.

3.8 Separability

Definition 3.8.1: Multiplicity

Take $f(x) \in F[x]$. Then over a splitting field over F, we get $f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\dots(x-\alpha_k)^{n_k}$ where $\alpha_1, \dots, \alpha_k$ are distinct elements of the splitting field and $n_1 \geq 1$ for all i. The value n_i is called the **multiplicity** of α_i, and if $n_i > 1$, α_i is a **multiple root** of $f(x)$. If $n_i = 1$ instead, then we say that α_i is a **simple root**.

Definition 3.8.2: Separable polynomials

A polynomial $f(x) \in F[x]$ is called **separable** if it has no multiple roots over a splitting field for F. Else, $f(x)$ is called **inseparable**.

Definition 3.8.3: Polynomial derivative

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + a_0 \in F[x]$, then its **derivative** is

$$D_x f(x) = na_n x^{n-1} + \dots + 2a_2x + a_1 \in F[x]$$

Proposition 3.8.1

Take $f(x) \in F[x]$ with root α. Then the multiplicity of α is greater than one if and only if $D_x f(\alpha) = 0$.

In other words, $f(x)$ is separable when $f(x)$ and $D_x f(x)$ share no roots.

Corollary 3.8.1

(a). Every irreducible polynomial over a field F of characteristic zero is separable

(b). A polynomial over a field of characteristic zero is separable if and only if it is the product of distinct irreducible factors

Now we discuss how separability relates to field extensions.

Definition 3.8.4: Separable

Let K/F be a field extension. An element $\alpha \in K$ is **separable over** F if α is algebraic over F and $m_{\alpha,F}(x)$ is separable.

The extension K/F is **separable** if every element of K is separable over F. If there is an $\alpha \in K$ that is not separable over F, then K/F is an **inseparable** extension.

Proposition 3.8.2

Every finitely generated algebraic extension of $\mathbb{Q}$ is separable.

3.9 Techniques in Characteristic p > 0

Proposition 3.9.1

Let F be a field of characteristic $p > 0$. Then for all $a, b \in F$, we get that

$$(a+b)^p = a^p + b^p$$
$$(ab)^p = a^p b^p$$

This is the "Freshman's Dream".

Definition 3.9.1: Frobenius Endomorphism

For a field F of characteristic $p > 0$, the function

$$\varphi : F \to F$$
$$a \mapsto a^p$$

is the **Frobenius endomorphism** of F.

Corollary 3.9.1

The Frobenius endomorphism of F is an injective field homomorphism. When F is finite, it is also surjective.

Now we will go back to some propositions about finite fields using these ideas.

Proposition 3.9.2

Every irreducible polynomial over a finite field F is separable. Moreover, $f(x) \in F[x]$ is separable if and only if it is the product of distinct irreducible polynomials in $F[x]$.

This follows by contradiction. One can express the irreducible polynomial as a polynomial of the form $g(x^p)$, but this polynomial can be shown to be reducible, and so cannot occur.

Definition 3.9.2: Perfect

A field K of characteristic $p > 0$ is called **perfect** if every element of K is a p-th power in K– that is, $K = K^p$.

By convention any field of characteristic zero is also called perfect.

We have just shown that every irreducible polynomial over a perfect field is separable, and hence finite extensions of perfect fields are separable.

Exercise 3.9.1

Prove that there exists a non-perfect infinite field F, i.e. find $f(x) \in F[x]$ so that f is irreducible and not separable.

These concepts can be used to prove that the n-th cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible.

Theorem 3.9.1

Let $K/\mathbb{F}_p$ be a field extension of the prime subfield $\mathbb{F}_p$.

- If K is finite, then $|K| = p^n$ for some positive integer n.
- $|K| = p^n$ if and only if K is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

By the uniqueness of splitting fields, we can simply denote K by $\mathbb{F}_{p^n}$.

This theorem gives us a complete characterization of finite fields. The first part is proven in Dummitt-Foote 13.2 #1.

Corollary 3.9.2

For all prime p, for all $n \in \mathbb{Z}_+$, there exists a field of cardinality p^n. Furthermore, any two finite fields of the same cardinality are isomorphic.

3.10 Simple Extensions

Theorem 3.10.1

If $|F| < \infty$, and K/F is a finite extension of F, then $K = F(\alpha)$ for some $\alpha \in K$.

This holds because $K^\times$ is a cyclic group, and so there must exist α so $\langle \alpha \rangle = K^\times$, and hence $K = F(\alpha)$.

Theorem 3.10.2

If F is an infinite field, and K/F is a finite separable extension, then $K = F(\alpha)$ for some $\alpha \in K$.

Every field extension can be written by appending a sequence of elements, and we can reduce the elements to one by the combination $\alpha = \beta + \gamma\delta$, where (β, γ) is the two additional elements, and $\delta \neq \frac{\beta_i - \beta}{\gamma - \gamma_j}$. Often we can simply choose $\delta = 1$ if we are lucky.

Chapter 4

Galois Theory

Galois theory studies the connection between finite field extensions via roots of polynomials and the structures of groups that permute those roots.

Let F, K be fields, and K/F a field extension.

Definition 4.0.1: Field Automorphism

We say that $\sigma : K \to K$ is a **field automorphism** if σ is a bijective unital ring homomorphism. We denote the collection of field automorphisms of K by $\mathrm{Aut}(K)$.

An automorphism $\sigma \in \mathrm{Aut}(K)$ **fixes an element** $\alpha \in K$ if $\sigma(\alpha) = \alpha$.

An automorphism $\sigma \in \mathrm{Aut}(K)$ **fixes a subset** E **of** K if $\sigma(\alpha) = \alpha$ for all $\alpha \in E$.

For $\sigma \in \mathrm{Aut}(K)$ and $E \subset K$, $\sigma(E)$ denotes the subset $\{\sigma(\alpha) \mid \alpha \in E\}$

Recall that the prime subfield of a field K is given by

$$K_{\text{prime}} = \begin{cases} \mathbb{Q} & K \text{ has characteristic } 0 \\ \mathbb{Z}_p & p \text{ prime} \end{cases}$$

because $\sigma \in \mathrm{Aut}(K)$ fixes 1_K, it must hold that σ fixes K_{prime} and hence prime subfields are fixed by any automorphism of a field.

4.1 Automorphisms fixing subfields

Definition 4.1.1

We define $\mathrm{Aut}(K/F)$ to be the collection of automorphisms of K that fix F.

Proposition 4.1.1

$\mathrm{Aut}(K)$ is a group under composition, and $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$.

Proposition 4.1.2

Let $\alpha \in K$ be an algebraic element over F. Then for any $\alpha \in \mathrm{Aut}(K/F)$, we get that $m_{\alpha,F}(\sigma(\alpha)) = 0$.

In other words, automorphisms permute roots of minimal polynomials.

4.2 Subfields and Subgroups

Proposition 4.2.1

Let H be a subgroup of $\mathrm{Aut}(K)$. Then

$$\{\alpha \in K \mid \sigma(\alpha) = \alpha \quad \forall \sigma \in H\}$$

is a subfield of K. We call this subfield the **fixed field of** H denoted by K^H.

In fact, this structure induces a correspondence between field extensions and chains of subgroups.

Proposition 4.2.2

Let $F_1 \subset F_2 \subset K$ be a sequence of field extensions. Then $\mathrm{Aut}(K/K) = \mathrm{Id}_{\mathrm{Aut}(K)} \leq \mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$.

Conversely, let $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ be a chain of subgroups. Then $K^{\mathrm{Aut}(K)} = K_{\mathrm{prime}} \subset K^{H_2} \subset K^{H_1}$

Proposition 4.2.3

Let E be the splitting field over F of a polynomial $f(x) \in F[x]$. Then

$$|\mathrm{Aut}(E/F)| \leq [E : F]$$

with equality if and only if $f(x)$ is separable over F.

The techniques used to prove this proposition also tell us that if K/F is finite, then $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Definition 4.2.1

Let K/F be a finite extension.

- If $|\mathrm{Aut}(K/F)| = [K : F]$ then K is **Galois over** F and K/F is a **Galois extension**.
- If K/F is Galois, then the group $\mathrm{Aut}(K/F)$ is called the **Galois group** of K/F and is denoted $\mathrm{Gal}(K/F)$.

Example 4.2.1

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then one can see that $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{6})$ are all subfields for which K is a Galois extension. Furthermore, these fields are all Galois extensions of $\mathbb{Q}$.

Example 4.2.2

Consider the quotient field $\mathbb{F}_2(t)$ of $\mathbb{F}_2[t]$ and consider $f(x) = x^2 - t \in \mathbb{F}_2(t)[x]$. One can show that $f(x)$ is irreducible but not separable over $\mathbb{F}_2(t)$, and hence if θ is a root of $f(x)$, $\mathbb{F}_2(t)(\theta)$ is NOT a Galois extension of $\mathbb{F}_2(t)$.

Example 4.2.3

Let K be the splitting field of $x^3 - 2$, i.e. $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. K is Galois over $\mathbb{Q}$, but $\mathbb{Q}(\sqrt[3]{2})$ is NOT Galois over $\mathbb{Q}$.

In fact, $\mathrm{Gal}(K/\mathbb{Q})$ is a nonabelian group of order 6, and thus is isomorphic to S_3.

We can summarize our characterization thus far by a set of equivalences. The following are equivalent:

- A finite field extension K/F is Galois
- $|\mathrm{Aut}(K/F)| = [K : F]$
- K/F is the splitting field of a separable polynomial over F
- K/F is normal and separable
- $F = K^{\mathrm{Aut}(K/F)}$

4.3 Fundamental Theorem of Galois Theory

Theorem 4.3.1: Fundamental Theorem of Galois Theory

Let K/F be Galois and set $G := \mathrm{Gal}(K/F)$. Then there exists a bijection between the subfields $E \subset K$ with $F \subset E$ and the subgroups $H \leq G$ given by

$$E \mapsto \mathrm{Aut}(K/E)$$
$$H \mapsto K^H$$

and these maps are inverses of each other. Furthermore, this bijection has some additonal properties:

- If $E_1 \leftrightarrow H_1$ and $E_2 \leftrightarrow H_2$, then $E_1 \subset E_2 \iff H_2 \leq H_1$.
- If $E \leftrightarrow H$, then $[K : E] = |H|$ and $[E : F] = [G : H]$.
- K/E is always Galois for $F \subset E \subset K$.
- E/F is Galois if and only if $H \triangleleft G$. In this case, $\mathrm{Gal}(E/F) \cong G/H$.
- If $E_1 \leftrightarrow H_1$ and $E_2 \leftrightarrow H_2$, then $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$ and $E_1E_2 \leftrightarrow H_1 \cap H_2$.

Remember that $H \triangleleft G$ is equivalent to $\mathrm{Aut}(K/E) \triangleleft \mathrm{Aut}(K/F)$. Also recaall that $\langle H_1, H_2 \rangle$ is the smallest subgroup of G that contains H_1, H_2, and E_1E_2 is the smallest subfield of K containing E_1, E_2. They are not necessarily equivalent!

Now we apply this theorem to finite fields. Consider $\mathbb{F}_{p^n}$, the splitting field of $x^{p^n} - x$. This is Galois over $\mathbb{F}_p$. Thus we have $|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. This gives us $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$ and the Galois group consists solely of the Frobenius endomorphism.

One can see then that all subfields $\mathbb{F}_p \subset E \subset \mathbb{F}_{p^n}$ have the form $E \cong \mathbb{F}_{p^d}$ for some $d \mid n$. Of course, this means that E/F is necessarily Galois as well!

4.4 Applications of Galois Theory

Proposition 4.4.1

The irreducible polynomial $x^4 + 1 \in \mathbb{Z}[x]$ is reducible over $\mathbb{F}_p$ for any prime p.

Proof. One can check this directly for $p = 2$. If $p > 2$, then observe that $p \cong 1, 3, 5$ or $7 \mod 8$, and hence $p^2 \cong 1 \mod 8$. Therefore we have that $x^8 - 1 \mid x^{p^2-1} - 1$ over $\mathbb{F}_p$.

Of course, $x^4 + 1 \mid x^8 - 1$ and so any root of $x^4 + 1$ is a root of $x^{p^2} - x$ and hence are elements of the field $\mathbb{F}_{p^2}$. Since $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, the degree of the extension is no more than 2. Of course, if $x^4 + 1$ were irreducible over $\mathbb{F}_p$, then it would necessarily be 4, and hence it must be reducible. ∎

Proposition 4.4.2

$$x^{p^n} - x = \prod_{d|n} \{\text{irreducible polynomial in } \mathbb{F}_p[x] \text{ of degree } d\}$$

We can use this recursively as n increases.

Now we discuss composite field extensions.

Proposition 4.4.3

If K/F is Galois, and F'/F is any field extension, then KF'/F' is Galois and $\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$.

Example 4.4.1

Consider $K = \mathbb{Q}(\omega), F' = \mathbb{Q}(\sqrt[3]{2}), F = \mathbb{Q}$. Then $KF' = \mathbb{Q}(\omega, \sqrt[3]{2})$ and by this theorem is Galois over $\mathbb{Q}(\sqrt[3]{2})$. Furthermore, the Galois group is isomorphic to $\mathbb{Q}(\omega) \cap \mathbb{Q}(\sqrt[3]{2})$.

Notice that $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$!

Corollary 4.4.1

If K/F is Galois and F'/F is any field extension, then

$$[KF' : F] = [KF' : F'][F' : F] \equiv [K : K \cap F'][F' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Proposition 4.4.4

If K_1/F and K_2/F are Galois, then K_1K_2/F and $K_1 \cap K_2/F$ are Galois. Furthermore,

$$\mathrm{Gal}(K_1K_2/F) \cong \{(\sigma, \tau) \mid \sigma \mid_{K_1 \cap K_2} = \tau \mid_{K_1 \cap K_2}\} \leq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Equality holds if and only if $K_1 \cap K_2 = F$.

Corollary 4.4.2

Let E/F be a finite separable extension. Then there exists K/F Galois extension with $F \subset E \subset K$, and the choice of K is minimal in the sense that, if $E \subset K'$ and $K' \subset \overline{K}$, then $K \subset K'$.

We call the Galois extension above the **Galois closure** of E/F.

4.5 Solvable Groups

Definition 4.5.1: Radical Extension

A field K is said to be a **radical extension** of a field F if there is a chain of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_n = K$$

such that, for each $i = 1, \ldots, n$, $F_i = F_{i-1}(\alpha_i)$ and some power of α_i is in F_{i-1}.

Let $f \in F[x]$. The equation $f(x) = 0_F$ is **solvable by radicals** if there exists a radical extension of F that contains a splitting field of $f(x)$. This is equivalent to the notion of there existing a "formula" for the solutions.

Definition 4.5.2: Solvable

A group G is said to be **solvable** if it has a chain of subgroups

$$\langle e \rangle = G_n \triangleleft \ldots \triangleleft G_1 \triangleleft G_0 = G$$

such that each quotient group G_{i-1}/G_i is abelian.

Notice that all abelian groups are solvable.

Proposition 4.5.1

For $n \geq 5$ the group S_n is not solvable.

Theorem 4.5.1

Every homomorphic image of a solvable group G is solvable.

Our goal is to prove the Galois Criterion. That is, let $f \in F[x]$. $f(x) = 0_F$ is solvable by radicals if and only if the Galois group of $f(x)$ is a solvable group.

Lemma 4.5.1

Let F be a field and η a primitive n-th root of unity in F. Then F contains a primitive d-th root of unity for every positive $d \mid n$.

This combined with the next two theorems will allow us to prove the Galois Criterion.

Theorem 4.5.2

Let F be a field of characteristic zero and η a primitive n-th root of unity in some field extension of F. Then $K = F(\eta)$ is a normal extension of F and $\mathrm{Gal}_F(K)$ is abelian.

Theorem 4.5.3

Let F be a field of characteristic zero that contains a primitive n-th root of unity. If α is a root of $x^n - c \in F[x]$ in some extension field of F, then $K = F(\alpha)$ is a normal extension of F and $\mathrm{Gal}_F(K)$ is abelian.

Lemma 4.5.2

Let F, E, K be fields of characteristic zero with

$$F \subset E \subset K = E(\alpha) \quad \alpha^k \in E$$

If K is finite-dimensional over F and E is normal over F, then there exists a field extension L of K which is a radical extension of E and a normal extension of F.

Theorem 4.5.4: Galois Criterion

Let $f \in F[x]$. $f(x) = 0_F$ is solvable by radicals if and only if the Galois group of $f(x)$ is a solvable group.

We can use this to show that there is no formula for the solutions of all fifth-degree polynomials, as there are fifth-degree polynomials whose Galois group is S_5.

Theorem 4.5.5

Let F be a field of characteristic zero and $f(x) \in F[x]$. If $f(x) = 0_F$ is solvable by radicals, then there is a normal radical field extension of F that contains the splitting field of $f(x)$.

Theorem 4.5.6

Let K be a normal radical field extension of F and E an intermediate field, all of characteristic zero. If E is normal over F, then $\mathrm{Gal}_F(E)$ is a solvable group.