Contents

1 Hilbert Theorems 3
   1.1 Noetherian and artinian rings and modules .................. 3
   1.2 The Hilbert nullstellensatz .............................. 7

2 Dedekind Rings 9
   2.1 Definitions and basic properties ............................. 9
   2.2 Integrality ............................................. 11
   2.3 Discrete valuations ..................................... 15
   2.4 Fractional ideals ....................................... 16
   2.5 Modules over Dedekind domains ............................. 18

3 Semisimple Modules and Rings 23
   3.1 Definitions and basic properties ............................. 23
   3.2 The Jacobson radical ................................... 29

4 Representations of Finite Groups 33
   4.1 The three languages ..................................... 33
   4.2 One-dimensional representations ............................ 35
   4.3 Characters .............................................. 36
   4.4 The main theorem ....................................... 37
   4.5 Hurwitz’s theorem ....................................... 38
   4.6 More properties of representations .......................... 39
   4.7 Tensor products ....................................... 41
   4.8 Tensor products of representations ........................... 42
   4.9 Burnside’s theorem .................................... 43

5 Algebras 45
   5.1 Definitions and basic properties ............................. 45
   5.2 Algebras over fields ..................................... 46
   5.3 The Brauer group ....................................... 48
   5.4 Maximal subfields ....................................... 52
   5.5 Cyclic algebras ....................................... 56
1 Hilbert Theorems

1.1 Noetherian and artinian rings and modules

Throughout, \( R \) is a ring, not necessarily commutative. Typically, we give definitions and prove statements about left \( R \)-modules. In most of the cases similar definitions and results hold for right \( R \)-modules. To indicate that we write (left) in parenthesis.

**Definition 1.1.1 (ACC / DCC).**

1. A (left) \( R \)-module \( M \) satisfies the *ascending chain condition* (ACC) if every increasing sequence of submodules

\[ M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots \]

is stable, i.e. there exists \( n \) such that \( M_i = M_{i+1} \) for all \( i \geq n \).

2. A (left) \( R \)-module \( M \) satisfies the *descending chain condition* (DCC) if every decreasing sequence of submodules

\[ M_1 \supset M_2 \supset \cdots \supset M_n \supset \cdots \]

is stable.

**Proposition 1.1.2.** Let \( R \) be a ring and \( M \) be a (left) \( R \)-module. The following are equivalent:

(1) \( M \) satisfies ACC (resp. DCC);

(2) every non-empty set of submodules of \( M \) has a maximal (resp. minimal) element.

**Proof.** (1) \( \Rightarrow \) (2): If a non-empty set \( A \) of submodules of \( M \) has no maximal element, then we can construct a strictly increasing sequence of submodules

\[ M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n \subsetneq \cdots , \]

where \( M_i \) are in \( A \).

(2) \( \Rightarrow \) (1): If we have increasing sequence of submodules as above, choose a maximal element \( M_n \) in the set \( \{ M_i \}_{i \geq 1} \). Then \( M_n = M_{n+1} = \ldots \). \( \square \)

**Definition 1.1.3 (Noetherian / artinian).** A (left) \( R \)-module \( M \) is

1. noetherian if \( M \) satisfies either of these properties for the ACC.
2. artinian if $M$ satisfies either of these properties for the DCC.

A ring $R$ is (left) noetherian (resp. (left) artinian) if $R$ as a (left) $R$-module is noetherian (resp. artinian).

**Example 1.1.4.**  
1. Fields are noetherian and artinian.
2. $\mathbb{Z}$ is noetherian but not artinian: $2\mathbb{Z} \subseteq 4\mathbb{Z} \subseteq 8\mathbb{Z} \subseteq \ldots$.

**Proposition 1.1.5.** Let $0 \rightarrow N \rightarrow M \rightarrow P \rightarrow 0$ be a short exact sequence of (left) $R$-modules. Then $M$ is noetherian (artinian) if and only if $N$ and $P$ are noetherian (artinian).

**Proof (noetherian case).** ($\Rightarrow$) Let $N_1 \subset N_2 \subset \cdots$ be submodules of $N$. Since the map $N \rightarrow M$ is injective, we can regard these as submodules of $M$, so the sequence is stable since $M$ is noetherian. Hence $N$ is noetherian.

Let $P_1 \subset P_2 \subset \cdots$ be submodules of $P$. Then $f^{-1}(P_1) \subset f^{-1}(P_2) \subset \cdots$ in $M$ is stable, so $P_1 \subset P_2 \subset \cdots$ is stable. Hence $P$ is noetherian.

($\Leftarrow$) Let $M_1 \subset M_2 \subset \cdots$ be submodules of $M$. Let $N_i = N \cap M_i$, so then $N_1 \subset N_2 \subset \cdots$ is stable since $N$ is noetherian. Similarly, if $P_i = f(M_i)$, then $P_1 \subset P_2 \subset \cdots$ is stable. Hence there exists $n$ such that $N_i = N_n$ and $P_i = P_n$ for all $i \geq n$, so $M_i = M_n$ for all $i \geq n$.

**Corollary 1.1.6.** If $M_1, \ldots, M_n$ are noetherian (artinian) modules, then so is $M_1 \oplus \cdots \oplus M_n$.

**Proof.** $0 \rightarrow M_1 \rightarrow M_1 \oplus M_2 \rightarrow M_2 \rightarrow 0$ is a short exact sequence. Induct on $n$. □

**Proposition 1.1.7.** Let $f : R \rightarrow S$ be a surjective ring homomorphism and $M$ be a (left) $S$-module. Then $M$ is noetherian (artinian) as an $S$-module if and only if $M$ is noetherian (artinian) as an $R$-module.

**Proof.** Every $S$-submodule of $M$ is also an $R$-submodule of $M$. Conversely, given any $R$-submodule $M' \subset M$, we have $(\text{Ker} \ f)M' = 0$, so $M'$ can be realized as a module over $R/\text{Ker} \ f \cong S$. Hence every $R$-submodule of $M$ is also an $S$-submodule. □

**Corollary 1.1.8.** Let $f : R \rightarrow S$ be a surjective ring homomorphism. If $R$ is (left) noetherian (artinian), then $S$ is noetherian (artinian).
Proof. Since $S \cong R/\text{Ker} f$, we have a short exact sequence $0 \to \text{Ker} f \to R \to S \to 0$ of $R$-modules. Hence $S$ is noetherian (artinian) as an $R$-module, so also as an $S$-module, so also as a ring.

**Proposition 1.1.9.** Let $R$ be a (left) noetherian (artinian) ring. Then every finitely generated (left) $R$-module is noetherian (artinian).

Proof. Let $M$ be a finitely generated $R$-module. There is a short exact sequence $0 \to N \to R^n \to M \to 0$. Since $R^n = R \oplus \cdots \oplus R$ is noetherian (artinian), so is $M$.

**Proposition 1.1.10.** Let $M$ be a (left) noetherian $R$-module. Then $M$ is finitely generated.

Proof. If $M$ is not finitely generated, then we can find $m_1, m_2, \ldots \in M$ such that $m_{i+1} \notin M_i = \text{span}(m_1, \ldots, m_i)$. This gives us a strictly increasing sequence

$$M_1 \subsetneq M_2 \subsetneq \cdots$$

so $M$ is not noetherian.

**Proposition 1.1.11.** If $R$ is (left) noetherian, then every submodule of a finitely generated (left) $R$-module is finitely generated.

Proof. If $M$ is finitely generated, then $M$ is noetherian. Submodules of noetherian rings are noetherian, hence finitely generated.

**Proposition 1.1.12.** A ring $R$ is (left) noetherian if and only if every (left) ideal is finitely generated.

Proof. If $R$ is (left) noetherian, then any (left) ideal $I$ is a (left) submodule of $R$, which is finitely generated, hence $I$ is finitely generated.

Let $I_1 \subset I_2 \subset \cdots$ be (left) ideals. Then $I = \bigcup_i I_i$ is a (left) ideal, hence finitely generated. Some $I_n$ contains all of the generators, and then $I_i = I = I_n$ for all $i \geq n$.

**Theorem 1.1.13** (Hilbert basis theorem). If $R$ is (left) noetherian, then so is $R[x_1, \ldots, x_n]$. 

5
Proof. It suffices to show that if \( R \) is noetherian, then so is \( R[x] \). We will show that every left ideal in \( R[x] \) is finitely generated.

Let \( I \subset R[x] \) be a left ideal, and let \( J \subset R \) be the set of all leading coefficients of polynomials in \( I \). Clearly, \( J \) is a left ideal in \( R \). Since \( R \) is left noetherian, \( J \) is finitely generated by some \( a_1, \ldots, a_s \in R \). Pick polynomials \( f_i \in I \) with leading coefficients \( a_i \) and let \( k_i = \deg(f_i) \) and \( k = \max(k_i) \). If

\[
M = R \oplus Rx \oplus Rx^2 \oplus \cdots \oplus Rx^k \subset R[x]
\]

is the \( R \)-submodule of polynomials of degree at most \( k \), then \( M \) is finitely generated, hence left noetherian. Therefore, \( I \cap M \subset M \) is finitely generated by some \( g_1, \ldots, g_m \).

We claim that \( f_1, \ldots, f_s; g_1, \ldots, g_m \) generate \( I \).

To see this, we use induction on \( n = \deg h \) for \( h \in I \). If \( \deg h \leq k \), then \( h \) is in the span of \( g_1, \ldots, g_m \). Otherwise, let \( a \in R \) be the leading coefficient of \( h \). Write \( a \) in the form \( a = b_1a_1 + \cdots + b_sa_s \) for some \( b_1, \ldots, b_s \in R \) and consider the polynomial

\[
h' = b_1x^{n-k_1}f_1 + \cdots + b_sx^{n-k_s}f_s \in I.
\]

The polynomials \( h \) and \( h' \) have the same degree and the leading coefficients. Then \( h - h' \in I \) has smaller degree, so it lies in the span of \( f_1, \ldots, f_s; g_1, \ldots, g_m \) by the inductive hypothesis. Hence \( h \) lies in their span as well.

Corollary 1.1.14. Let \( R \) be a subring of a commutative ring \( S \). If \( S \) is finitely generated as an \( R \)-algebra, i.e. there exist finitely many \( s_1, \ldots, s_n \in S \) such that every element of \( S \) can be written as a polynomial in \( s_1, \ldots, s_n \) with coefficients in \( R \), and \( R \) is noetherian, then so is \( S \).

Proof. Let \( S \) be generated as an \( R \)-algebra by \( s_1, \ldots, s_n \). Then \( R[x_1, \ldots, x_n] \) is noetherian and the evaluation map \( R[x_1, \ldots, x_n] \to S \) given by \( f(x_1, \ldots, x_n) \mapsto f(s_1, \ldots, s_n) \) is surjective, so \( S \) is noetherian. 

\[\square\]
1.2 The Hilbert nullstellensatz

Throughout, all rings are commutative.

**Lemma 1.2.1.** Let $R \subset S \subset T$ be rings. Suppose that $R$ is noetherian, $T$ is finitely generated as an $R$-algebra, and $T$ is finitely generated as an $S$-module. Then $S$ is finitely generated as an $R$-algebra.

**Proof.** Write $T = R[a_1, \ldots, a_n]$ for $a_1, \ldots, a_n \in T$ and $T = Sb_1 + \cdots + Sb_m$ for $b_1, \ldots, b_m \in T$. Then in particular,

$$a_i = \sum_j \alpha_{ij}b_j \quad \text{for some } \alpha_{ij} \in S,$$

$$b_ib_j = \sum_k \beta_{ijk}b_k \quad \text{for some } \beta_{ijk} \in S.$$ 

Let $S_0 = R[\alpha_{ij}, \beta_{ijk}] \subset S$, so that

$$R \subset S_0 \subset S \subset T.$$ 

We claim that $T = S_0b_1 + \cdots + S_0b_m$. To see this, we have

$$T = R[a_1, \ldots, a_n] = S_0[b_1, \ldots, b_m] = S_0b_1 + \cdots + S_0b_m,$$

where the last step follows from expressing quadratic monomials in terms of linear monomials with the coefficients $\beta_{ijk}$. Since $T$ is a finitely generated $S_0$-module and $S_0$ is noetherian, $S$ is finitely generated as an $S_0$-module. Therefore, as $S_0$ is finitely generated as an $R$-algebra, $S$ is finitely generated as an $R$-algebra. $\square$

**Proposition 1.2.2.** Let $E/F$ be a field extension. If $E$ is finitely generated as an $F$-algebra, then $E/F$ is a finite field extension (i.e., $E$ is finitely generated as an $F$-module).

**Proof.** We claim that if $E = F(x_1, \ldots, x_n)$ is a field of rational functions, then $E = F$ (so $n = 0$). Let $E = F[f_1, \ldots, f_m]$ with $f_i \in E$ and write $f_i = g_i/h$ with $g_i, h \in F[x_1, \ldots, x_n]$. The denominators of elements of $F[f_1, \ldots, f_m]$ can only be powers of $h$, hence $F[f_1, \ldots, f_n] \neq F(x_1, \ldots, x_n)$. This is a contradiction, so the claim follows.

Now let $E = F[f_1, \ldots, f_m]$ with $\{f_1, \ldots, f_k\}$ be a maximal algebraically independent subset for some $k \leq m$. Then every element in $E$ is algebraic over the field
1.2 The Hilbert nullstellensatz

As $E$ finitely generated as a field over $F$, hence over $F(f_1,\ldots,f_k)$, the field extension $E/F(f_1,\ldots,f_k)$ is finite.

Note that $E_0 = F(f_1,\ldots,f_k) \cong F(x_1,\ldots,x_k)$ is the rational function field over $F$. Since $E$ is finitely generated over $F$ as an algebra and $E$ is finitely generated over $E_0$, we know that $E_0$ is finitely generated over $F$ as an algebra. By the claim, $E_0 = F$, so we are done.

For simplicity, write $a = (a_1,\ldots,a_n) \in F^n$ and $f(a) = f(a_1,\ldots,a_n)$ for $f \in F[x_1,\ldots,x_n]$.

**Theorem 1.2.3** (Hilbert nullstellensatz, weak form). Let $F$ be algebraically closed and $f_1,\ldots,f_m \in F[x_1,\ldots,x_n]$. Then $f_1,\ldots,f_m$ span $F[x_1,\ldots,x_n]$ if and only if there is no $a \in F^n$ such that $f_i(a) = 0$ for all $i$.

**Proof.** ($\implies$) Choose $g_1,\ldots,g_m$ such that $f_1g_1 + \cdots + f_mg_m = 1$. Then $f_1(a)g_1(a) + \cdots + f_m(a)g_m(a) = 1$ for all $a \in F^n$, so there is no $a$ where $f_i(a) = 0$ for all $i$.

($\impliedby$) Let $I = (f_1,\ldots,f_m)$ and suppose $I \neq F[x_1,\ldots,x_n]$. Then $I$ is contained in a maximal ideal $M$, and by Homework C1 Problem 4, there is a point $a \in F^n$ for which $f(a) = 0$ for all $f \in M$, hence for $f_1,\ldots,f_m$.

**Theorem 1.2.4** (Hilbert nullstellensatz, strong form). Let $F$ be algebraically closed and consider $f_1,\ldots,f_m, g \in F[x_1,\ldots,x_n]$. Then $g^k \in (f_1,\ldots,f_m)$ for some $k$ if and only if whenever $f_i(a) = 0$ for all $i$, we also have $g(a) = 0$.

**Proof.** ($\implies$) This is clear.

($\impliedby$) If $g = 0$, then we are done. Otherwise, introduce a new variable $t$ and let $f_{m+1} = 1 - t \cdot g \in F[x_1,\ldots,x_n,t]$. If $f_i(a) = 0$ for all $i$, then $f_{m+1}(a) = 1$. By the weak form of the nullstellensatz, $f_1,\ldots,f_{m+1}$ generate $F[x_1,\ldots,x_n,t]$, so we can write $1 = f_1h_1 + \cdots + f_mh_m + (1 - t \cdot g)h_{m+1}$ for some $h_1,\ldots,h_{m+1} \in F[x_1,\ldots,x_n,t]$. Substitute $t = 1/g$ and clear denominators to get the result.
2 Dedekind Rings

Throughout, all rings are commutative.

2.1 Definitions and basic properties

Definition 2.1.1 (Divisibility of ideals). Let \( \mathfrak{a}, \mathfrak{b} \subset R \) be ideals with \( \mathfrak{b} \neq 0 \). We say that \( \mathfrak{a} \) is divisible by \( \mathfrak{b} \) (or \( \mathfrak{b} \) divides \( \mathfrak{a} \)) if there is an ideal \( \mathfrak{c} \subset R \) such that \( \mathfrak{a} = \mathfrak{bc} \).

Proposition 2.1.2. If \( a, b \in R \) with \( b \neq 0 \). Then \( a \) divisible by \( b \) if and only if \( aR \) is divisible by \( bR \).

Definition 2.1.3 (Dedekind domain). An integral domain \( R \) is a Dedekind domain if for any two ideals \( \mathfrak{a} \subset \mathfrak{b} \neq 0 \), we have that \( \mathfrak{b} \) divides \( \mathfrak{a} \).

Example 2.1.4. Every PID is a Dedekind domain.

Remark 2.1.5. For this course, we will consider fields to be Dedekind domains.

Proposition 2.1.6. Let \( R \) be a Dedekind domain. If \( ab \subset ab' \) and \( a \neq 0 \), then \( b \subset b' \). If \( ab = ab' \) and \( a \neq 0 \), then \( b = b' \).

Proof. Let \( a \in \mathfrak{a} \) be non-zero, so then \( aR \subset \mathfrak{a} \). Since \( R \) is a Dedekind domain, there exists \( c \) such that \( aR = ac \). Then \( ab = acb \subset acb' = ab' \), so \( b \subset b' \).

Proposition 2.1.7. Every ideal of a Dedekind domain \( R \) is a finitely generated projective \( R \)-module.

Proof. Let \( \mathfrak{a} \subset R \) be an ideal. If \( \mathfrak{a} = 0 \), then we are done. Otherwise, let \( a \in \mathfrak{a} \) be non-zero, so then \( aR = \mathfrak{ab} \) for some ideal \( \mathfrak{b} \subset R \). Write \( a = x_1y_1 + \cdots + x_ny_n \) for \( x_i \in \mathfrak{a} \) and \( y_i \in \mathfrak{b} \). Define \( f : R^n \to \mathfrak{a} \) by \( f(r_1, \ldots, r_n) = r_1x_1 + \cdots + r_nx_n \in \mathfrak{a} \) and \( g : \mathfrak{a} \to R^n \) by \( g(z) = (zy_i/a)_i \in R^n \). Then \( f \circ g = \text{id}_A \), so \( A \) is a direct summand of \( R^n \).

Corollary 2.1.8. A Dedekind domain is noetherian.

Definition 2.1.9 (Krull dimension). Let \( R \) be a commutative ring. The Krull dimension of \( R \) is the largest \( n \) for which there is a chain of prime ideals \( p_0 \subset \cdots \subset p_n \) in \( R \).

Example 2.1.10. 1. \( \dim F = 0 \) for any field \( F \).
2.1 Definitions and basic properties

Proposition 2.1.11. Let \( R \) be a domain. Then \( \dim R \leq 1 \) if and only if every non-zero prime ideal is maximal.

Theorem 2.1.12. If \( R \) is a Dedekind domain, then \( \dim R \leq 1 \).

Proof. It suffices to show that every non-zero prime ideal \( p \) is maximal. Let \( m \) be a maximal ideal containing \( p \). Since \( R \) is a Dedekind domain, there is an ideal \( a \) such that \( p = am \). Since \( p \) is prime, either \( a \subset p \) or \( m \subset p \). If \( a \subset p = am \subset a \), then \( a = p = am \), so by cancellation, \( m = R \), a contradiction. Thus \( m \subset p \subset m \), so \( p = m \) is maximal.

Theorem 2.1.13. Let \( R \) be a Dedekind domain and \( a \subset R \) be a non-zero ideal. Then \( a = p_1 \cdots p_n \) for some prime ideals \( p_1, \ldots, p_n \) which are unique up to rearrangement.

Proof. Let \( A \) be the set of all non-zero proper ideals that have no such factorization. If \( A \) is non-empty, then since \( R \) is noetherian, \( A \) has a maximal element \( a \). Let \( m \) be a maximal ideal containing \( a \). There exists an ideal \( b \) such that \( a = bm \subset b \). If \( a = b \), then \( m = R \) by cancellation. This is a contradiction, so \( a \neq b \). By maximality of \( a \in A \), it must be that \( b = p_1 \cdots p_n \). Then \( a = p_1 \cdots p_n m \), contradicting \( a \) having no factorization.

For uniqueness, suppose \( p_1 \cdots p_n = q_1 \cdots q_m \). For some \( j \), we have \( q_j \subset p_n \). Since \( \dim R \leq 1 \), we have \( q_j = p_n \). WLOG, \( j = m \), so then cancellation gives \( p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1} \). Proceed inductively.

Example 2.1.14. The ring \( R = \mathbb{Z}[\sqrt{-5}] \) is a Dedekind domain, but not a PID. We have \( (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5}) \) as elements, hence also as ideals. Although the elements are all irreducible, they are not prime, so the corresponding ideals are not prime. Therefore, we can factor the ideals further. Specifically, let

\[
p_{2,\pm} = (2, 1 \pm \sqrt{-5}), \quad p_{3,\pm} = (3, 1 \pm \sqrt{-5}).
\]

(To see that these are primes, write \( R = \mathbb{Z}[t]/(t^2 + 5) \).) Then

\[
(2) = p_{2,+}p_{2,-}, \quad (3) = p_{3,+}p_{3,-}, \quad (1 \pm \sqrt{-5}) = p_{2,\pm} p_{3,\pm},
\]

so we restore uniqueness of factorization in the context of ideals.
2.2 Integrality

Definition 2.2.1 (Integral element). Let \( R \subset S \) be rings. An element \( \alpha \in S \) is integral over \( R \) if there exists a monic polynomial \( f \in R[x] \) such that \( f(\alpha) = 0 \).

Definition 2.2.2 (Faithful module). An \( R \)-module \( M \) is faithful if \( aM = 0 \) implies that \( a = 0 \). Equivalently, \( M \) is faithful if the corresponding ring homomorphism \( R \to \text{End } M \) is injective.

Example 2.2.3. If \( R \subset S \) are rings, then \( S \) is faithful as an \( R \)-module.

Proposition 2.2.4. Let \( R \subset S \) be rings and \( \alpha \in S \). Then the following are equivalent:

1. \( \alpha \) is integral over \( R \);
2. The ring \( R[\alpha] \) is finitely generated as an \( R \)-module;
3. there is a faithful \( R[\alpha] \)-module \( M \) such that \( M \) is finitely generated as an \( R \)-module.

Proof. (1) \( \implies \) (2) Suppose \( f(\alpha) = 0 \) for a monic \( f \in R[x] \) with \( \deg f = n \). Then \( R[x] \) is generated as an \( R \)-module by \( 1, x, \ldots, x^{n-1} \).

(2) \( \implies \) (3) Take \( M = R[\alpha] \).

(3) \( \implies \) (1) Suppose \( M \) is generated by \( m_1, \ldots, m_n \) as an \( R \)-module. For each \( i \), we have \( \alpha m_i = \sum_j a_{ij}m_j \) for some \( a_{ij} \in R \), so \( (\alpha I - A)X = 0 \), where \( X = (m_1, m_2, \ldots, m_n)^t \). Multiplying through by \( \text{adj}(\alpha I - A) \), we get \( \det(\alpha I - A) \cdot X = 0 \), hence \( \det(\alpha I - A) \cdot M = 0 \). Since \( M \) is faithful as an \( R[\alpha] \)-module, we have \( \det(\alpha I - A) = 0 \) in \( R[\alpha] \). Expanding the determinant, we obtain a monic polynomial with coefficients in \( R \) which evaluates to 0 at \( \alpha \), so \( \alpha \) is integral over \( R \).

Corollary 2.2.5. Let \( R \subset S \) be rings and \( \alpha_1, \ldots, \alpha_n \in S \) be integral over \( R \). Then \( R[\alpha_1, \ldots, \alpha_n] \) is finitely generated as an \( R \)-module.

Corollary 2.2.6. Let \( R \subset S \) be rings. The set of elements of \( S \) which are integral over \( R \) is a subring of \( S \) containing \( R \).

Proof. It is clear that the set contains \( R \). Suppose \( \alpha, \beta \in S \) are integral over \( R \). Then \( R[\alpha, \beta] \) is finitely generated as an \( R \)-module. For any \( \gamma \in R[\alpha, \beta] \), we have that \( R[\gamma] \subset R[\alpha, \beta] \), so \( R[\alpha, \beta] \) is faithful as an \( R[\gamma] \)-module. Hence \( \gamma \) is integral over \( R \). In particular, \( \alpha + \beta \) and \( \alpha \beta \) are integral over \( R \).
Definition 2.2.7 (Integral closure). Let $R \subseteq S$ be rings. The ring of elements of $S$ which are integral over $R$ is the \textit{integral closure} of $R$ in $S$.

If the integral closure of $R$ in $S$ is $S$, we say that $S$ is \textit{integral} over $R$. Equivalently, $S$ is integral over $R$ if every element of $S$ is integral over $R$.

If the integral closure of $R$ in $S$ is $R$, we say that $R$ is \textit{integrally closed} in $S$.

Definition 2.2.8 (Normal ring). Let $R$ be a domain and $F$ be its quotient field. We say that $R$ is \textit{normal} (or \textit{integrally closed}) if $R$ is integrally closed in $F$.

Example 2.2.9. Every UFD is normal.

Proposition 2.2.10. Let $R \subseteq S \subseteq T$ be rings with $S/R$ integral. If $\alpha \in T$ is integral over $S$, then $\alpha$ is integral over $R$.

Proof. Suppose $\alpha^n + s_1\alpha^{n-1} + \cdots + s_n = 0$ for $s_i \in S$. Since $s_1, \ldots, s_n$ are integral over $R$, the ring $R[s_1, \ldots, s_n]$ is finitely generated as an $R$-module. Thus $\alpha$ is integral over $R[s_1, \ldots, s_n]$, so $R[s_1, \ldots, s_n, \alpha]$ is finitely generated as an $R[s_1, \ldots, s_n]$-module. Finite generation is transitive, so $R[s_1, \ldots, s_n, \alpha]$ is finitely generated as an $R$-module. Thus $\alpha$ is integral over $R$. \qed

Corollary 2.2.11. Let $R \subseteq S \subseteq T$ be rings with $S/R$ integral. If $T/S$ is integral, then $T/R$ is integral.

Corollary 2.2.12. Let $S^{\text{int}}$ be the integral closure of $R$ in $S$. Then $S^{\text{int}}$ is integrally closed in $S$.

Example 2.2.13. Let $R$ be a subring of a field $F$, $K/F$ a field extension and $S$ the integral closure of $R$ in $K$. Then $S$ is integrally closed in $K$ and hence in its quotient field (which is a subfield of $K$), hence $S$ is normal.

Let us assume that $F$ is the quotient field of $R$ and $K/F$ an algebraic field extension. We claim that $K$ is the quotient field of $S$. Indeed, every $\alpha \in K$ satisfies $\alpha^n + \beta_1\alpha^{n-1} + \cdots + \beta_n = 0$ with $\beta_i \in F$. Choose a nonzero $r \in R$ such that $b_i := r\beta_i \in R$. Then $(r\alpha)^n + b_1(r\alpha)^{n-1} + \cdots + r^{n-1}b_n = 0$, hence the element $s := r\alpha$ is integral over $R$, therefore, $s \in S$. Overall, $\alpha = s/r$. Note that the denominator $r$ is contained in $R$, not only in $S$.

Proposition 2.2.14. Let $R$ be a normal domain, $F$ the quotient field of $R$, $K/F$ a field extension and $\alpha \in K$ algebraic over $F$. Then $\alpha$ is integral over $R$ if and only if the minimal polynomial of $\alpha$ in $F[x]$ is in fact contained in $R[x]$.
Proof. If the minimal polynomial $m$ of $\alpha$ is contained in $R[x]$, then $\alpha$ is integral over $R$ as $m$ is monic. Conversely, if $\alpha$ is integral over $R$, choose a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$. Let $L$ be a splitting field of $f$ over $K$. All roots of $f$ are integral over $R$. As $m$ divides $f$, all roots of $m$ are integral over $R$. As all coefficients of $m$ are standard symmetric functions of the roots, the coefficients of $m$ are integral $R$ and hence $m \in R[x]$ since $R$ is normal.

**Theorem 2.2.15.** Every Dedekind domain is normal.

**Proof.** Let $R$ be a Dedekind domain and $\alpha \in F$ be integral over $R$. Then $R[\alpha] \subset F$ is finitely generated as an $R$-module, so there exists $c \in R$ non-zero with $a = c \cdot R[\alpha] \subset R$ an $R$-submodule, hence an ideal of $R$. Let $\alpha = a/b$ for $a, b \in R$. Since $\alpha a \subset a$ by construction, $aa \subset ba$. As $R$ is a Dedekind domain, $aa = \delta ab$ for some ideal $b \subset R$. Then $aR = bb$, so $\alpha \in (a/b)R \subset b \subset R$.

**Lemma 2.2.16.** Let $R$ be a noetherian normal domain with quotient field $F$, let $a \subset R$ be a non-zero ideal, and $\alpha \in F$. If $\alpha a \subset a$, then $\alpha \in R$.

**Proof.** The ideal $a$ is a finitely generated $R$-module which is faithful as an $R[\alpha]$-module, so $\alpha$ is integral over $R$, i.e. $\alpha \in R$.

**Theorem 2.2.17.** A domain $R$ is a Dedekind domain if and only if $R$ is noetherian, $\dim R \leq 1$, and $R$ is normal.

**Proof.** We already showed that Dedekind domains have these properties. Suppose $R$ is noetherian, $\dim R \leq 1$, and $R$ is normal.

**Lemma 2.2.18.** Let $a \subset R$ be a non-zero ideal. Then $a$ contains a finite product of nonzero prime ideals.

**Proof.** If $a$ is prime, then we are done. Otherwise, there exist $a, b \in R$ such that $ab \in a$ but $a, b \notin a$. Supposing $a$ is a maximal counterexample,

$$a \subsetneq a + aR \supsetneq p_1 \cdots p_n,$$

$$a \subsetneq a + bR \supsetneq q_1 \cdots q_m,$$

but then

$$a \supsetneq (a + aR)(a + bR) \supsetneq p_1 \cdots p_n q_1 \cdots q_m.$$  

**Lemma 2.2.19.** Let $b \subsetneq R$ be a nonzero ideal. Let $F$ be the quotient field of $R$. Then there exists $\alpha \in F \setminus R$ with $\alpha b \subset R$.  

13
2.2 Integrality

Proof. Let $b \in \mathfrak{b}$ be non-zero. By lemma, there exist primes such that $p_1 \cdots p_k \subset b\mathfrak{R}$; choose these primes so that $k$ is as small as possible. Let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{b}$. Then $p_i \subset \mathfrak{p}$ for some $i$, wlog $i = 1$, so since $\dim(\mathfrak{R}) \leq 1$, $p_1 = \mathfrak{p}$. By minimality of $k$, we have $p_2 \cdots p_k \not\subset b\mathfrak{R}$, so there exists $c \in p_2 \cdots p_k$ with $c \not\subset b\mathfrak{R}$. Then $cb \subset cp = c\mathfrak{p} = p_1 \cdots p_k \subset b\mathfrak{R}$, so we can choose $\alpha = c/b$.

Now suppose that $a \subset \mathfrak{b}$ are ideals with $\mathfrak{b} \neq 0$. To show that $a = bc$ for some ideal $c$, we use noetherian induction on $\mathfrak{b}$. We may assume that $a \neq 0$.

If $\mathfrak{b} = \mathfrak{R}$, then take $c = a$, so assume that $\mathfrak{b} \neq \mathfrak{R}$. Let $\alpha \in F \setminus \mathfrak{R}$ be as in the second lemma. Since $\alpha \not\in \mathfrak{R}$, we have $\alpha \mathfrak{b} \not\subset \mathfrak{b}$ (since $\mathfrak{R}$ is normal), but $\alpha \mathfrak{b} \subset \mathfrak{R}$. Letting $\mathfrak{b}' = \mathfrak{b} + \alpha \mathfrak{b}$, we have $a \subset \mathfrak{b} \subset \mathfrak{b}' \subset \mathfrak{R}$, so by induction, there exists $c'$ such that $a = \mathfrak{b}' c'$. Let $c = (\mathfrak{R} + \alpha \mathfrak{R}) c' \subset F$. Then

$$bc = b(R + \alpha \mathfrak{R}) c' = \mathfrak{b}' c' = a.$$

To see that $c \subset \mathfrak{R}$, let $c \subset c$. Then $cb \subset \mathfrak{b}' c' = a \subset \mathfrak{b}$, so $c \subset \mathfrak{R}$ as $\mathfrak{R}$ is normal.

Theorem 2.2.20. Let $\mathfrak{R}$ be a Dedekind domain with quotient field $F$ and let $K/F$ be a finite separable field extension. If $S$ is the integral closure of $\mathfrak{R}$ in $K$, then $S$ is a Dedekind domain.

Proof. Let $\alpha \in S$. Then $\sigma(\alpha) \in S$ for any $\sigma$ in the Galois group of a normal closure of $K/F$, so $\text{tr}_{K/F}(\alpha) \in F$ is integral over $\mathfrak{R}$. Since $\mathfrak{R}$ is normal, $\text{tr}_{K/F}(\alpha) \in \mathfrak{R}$.

Let $\alpha \in K$. Since $K/F$ is finite, we know that $K$ is the quotient field of $S$ and there exists $a \in \mathfrak{R}$ non-zero such that $aa \in S$.

Let $a_1, \ldots, a_n \in K$ be a basis over $F$. From the proof that $K$ is the quotient field of $S$, there exists $a \in \mathfrak{R}$ non-zero such that $b_i = aa_i \in S$. Let $f : K \to F^n$ be given by $f(x)_i = \text{tr}((xb_i))$. This is an $F$-linear map, and we claim that $f$ is injective, so that it is an isomorphism. Let $\alpha \in K$ be non-zero. Since $\text{tr}$ is non-zero as a function, there exists $\beta \in K$ such that $\text{tr} \beta \neq 0$. Write $\beta/\alpha = \sum \gamma_i b_i$ for $\gamma_i \in F$. Then $\beta = \sum \gamma_i ab_i$, so for some $i$, we have $\text{tr}(\alpha b_i) = 0$. Therefore, $f(\alpha) \neq 0$.

From this result, $S \cong f(S) \subset R^n$ as $R$-modules. Since $R$ is noetherian, $S$ is finitely generated as an $R$-module, hence as an $R$-algebra, so $S$ is noetherian.

Finally, let $q \subset S$ be non-zero prime and $p = q \cap \mathfrak{R}$, so then $p$ is prime in $\mathfrak{R}$. If $a_1 \in q$ is non-zero, then $a_1/\alpha$ is a root of some $x^m + a_{m-1}x^{m-1} + \cdots + a_m = 0$ with $a_1 \in \mathfrak{R}$ and $a_m \neq 0$. Then $\alpha^m + \cdots + a_1 \alpha \in q \cap \mathfrak{R} = p$ and is non-zero, so $p \neq 0$. Since $\dim(\mathfrak{R}) \leq 1$, the ideal $p$ is maximal. The inclusion $\mathfrak{R} \hookrightarrow S$ then induces an embedding $R/p \hookrightarrow S/q$. Since $S/q$ is a domain and finitely generated over the field $R/p$, it is also a field. Thus $q$ is maximal, so $\dim S = 1$. 

14
Having showed that $S$ is normal, noetherian, and of dimension 1, $S$ is a Dedekind domain.

**Example 2.2.21.** 1. If $R = \mathbb{Z}$ and $F = \mathbb{Q}$, then for any number field $K$ (finite extension of $\mathbb{Q}$), the integral closure of $\mathbb{Z}$ in $K$ is a Dedekind domain.

   2. Let $F$ be a field and $R = F[x]$. If $K$ is a finite extension of $F(x)$, then the integral closure of $R$ in $K$ is a Dedekind domain.

### 2.3 Discrete valuations

**Definition 2.3.1** (Discrete valuation). Let $F$ be a field. A discrete valuation on $F$ is a map $\nu : F^* \to \mathbb{Z}$ such that

(i) $\nu(xy) = \nu(x) + \nu(y)$;

(ii) if $x + y \neq 0$, then $\nu(x + y) \geq \min(\nu(x), \nu(y))$.

If we set $\nu(0) = \infty$, then (i) and (ii) hold for all $x, y \in F$.

**Remark 2.3.2.** Usually, it is assumed that $\nu \neq 0$. We will allow the valuation to be zero and call such valuation discrete valuation or rank zero. If $\nu \neq 0$, we call $\nu$ discrete valuation of rank one.

**Example 2.3.3** ($p$-adic valuation). Let $R$ be a Dedekind domain and $F$ be the quotient field of $R$. If $0 \neq p \subset R$ is prime, then for any $a \in R$ non-zero, we can write $aR = p^n a$ for $a$ not divisible by $p$ (equivalently, $a$ is not contained in $a$) and set $\nu_p(a) = n$. For $\alpha = a/b \in F$ non-zero, define $\nu_p(\alpha) = \nu_p(a) - \nu_p(b)$.

**Example 2.3.4.** 1. A theorem of Ostrowski states that the only discrete valuations on $\mathbb{Z}$ are the $p$-adic valuations.

   2. Let $F$ be a field. In addition to the $p$-adic valuations on $F(x)$, there is also the valuation $\nu_\infty(f/g) = \deg g - \deg f$.

**Proposition 2.3.5.** Let $F$ be a field and $\nu$ be a discrete valuation on $F$. The set $R_\nu = \{a \in F \mid \nu(a) \geq 0\} \subset F$ is a local ring with unique maximal ideal $\mathfrak{m} \subset \{a \in F \mid \nu(a) > 0\}$.

**Proof.** That $R_\nu$ is a ring and $\mathfrak{m}$ is an ideal follows from $\nu(ab) = \nu(a) + \nu(b)$ and $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$. That $\mathfrak{m}$ is the unique maximal ideal follows from using $\nu(a^{-1}) = -\nu(a)$ to show that $R_\nu \setminus \mathfrak{m} = R_\nu^\ast$. \qed
### 2.4 Fractional ideals

**Definition 2.3.6** (Discrete valuation ring). The ring $R_\nu$ is the *valuation ring* of $\nu$. A domain $R$ is a *discrete valuation ring* (DVR) if $R = R_\nu$ for some discrete valuation $\nu$ (on its quotient field).

For example, fields are DVRs.

**Proposition 2.3.7.** Let $R$ be a domain. Then the following are equivalent:

1. $R$ is a DVR;
2. $R$ is a local PID;
3. $R$ is a local Dedekind domain.

*Proof.* Let $F$ be the quotient field of $R$.

(1) $\implies$ (2) If $R$ is a field, we are done. Otherwise, since $R = R_\nu$ for some $\nu \neq 0$, we know that $R$ is local. By rescaling if needed, we can suppose $\nu : F^\times \to \mathbb{Z}$ is surjective. Choose $\pi \in R$ so that $\nu(\pi) = 1$, and let $a \subset R$ be non-zero. Let $n = \min\{\nu(a) \mid a \in a\}$. We claim that $a = \pi^nR$. For $a \in a$, we have $\nu(a/\pi^n) \geq 0$, so $a/\pi^n \in R$. Hence $a \in \pi^nR$, so $a \subset \pi^nR$. For the other inclusion, choose $a \in a$ so that $\nu(a) = n$. Then $\nu(\pi^n/a) = 0$, so $\pi^n/a \in R$. Hence $\pi^n \in aR \subset a$, so $\pi^nR \subset a$.

(2) $\implies$ (3) Every PID is a Dedekind domain.

(3) $\implies$ (1) We may assume that $R$ is not a field. Let $m$ be the maximal ideal of $R$ and define on $F$ the $m$-adic valuation $\nu$. Then clearly $R \subset R_\nu$, and if $a/b \in R_\nu$, then $aR = m^k$ and $bR = m^l$ with $k \geq l$. Hence $aR \subset bR$, so $a = bc$ for some $c \in R$, and then $a/b = c \in R$. $\square$

### 2.4 Fractional ideals

**Definition 2.4.1** (Fractional ideal). Let $R$ be a Dedekind domain and $F$ be its quotient field. A *fractional ideal* of $R$ is a nonzero finitely generated $R$-submodule of $F$.

**Proposition 2.4.2.** 1. If $a \subset R$ is an ideal and $\alpha \in F^\times$, then $\alpha a$ is a fractional ideal. Conversely, all fractional ideals are of this form.

2. The product of fractional ideals is a fractional ideal.
Proposition 2.4.3. The set Frac(R) of all fractional ideals is a group with multiplication.

Proof. Associativity is clear.
The identity element is $R$.
For inverses, let $f \subset F$ be a fractional ideal, and write $f = \alpha a$ for some ideal $a \subset R$.
Choose $a \in a$ non-zero, then write $aR = ab$ for some ideal $b \subset R$. The required $f^{-1}$
is $a^{-1}\alpha^{-1}b$.  

Proposition 2.4.4. Frac(R) is a free abelian group with basis the set of all non-zero prime ideals of $R$.

Proof. Let $f \in \text{Frac}(R)$ and write $f = (1/a)a$ for some $a \in R$ and $a \subset R$. If $aR = p_1 \cdots p_n$, then $(1/a)R = p_1^{-1} \cdots p_n^{-1}$. Writing $a = q_1 \cdots q_m$, we have
$$f = p_1^{-1} \cdots p_n^{-1} q_1 \cdots q_m.$$  
This shows that Frac(R) is generated by non-zero primes, and uniqueness follows from clearing inverses and uniqueness of factorization of ideals in $R$.  

Definition 2.4.5 (Principal fractional ideal). A fractional ideal $j$ is principal if $j = \alpha R$ for some $\alpha \in F$.

Proposition 2.4.6. The principal fractional ideals form a subgroup PFrac(R) of Frac(R).

Definition 2.4.7 (Class group). The class group is Cl(R) = Frac(R)/PFrac(R).

Proposition 2.4.8. The sequence
$$1 \longrightarrow R^\times \longrightarrow F^\times \xrightarrow{\alpha \mapsto \alpha R} \text{Frac}(R) \longrightarrow \text{Cl}(R) \longrightarrow 1$$
is exact.

Proposition 2.4.9. Let $R$ be a Dedekind domain. Then the following are equivalent:

1. $R$ is a PID.
2. $R$ is a UFD.
3. Cl($R$) = 1.
Proof. (1) \implies (2) Clear.

(2) \implies (3) It suffices to show that every non-zero prime ideal \( p \) is principal. Let \( a \in p \) be non-zero and write \( a = p_1 \cdots p_k \in P \) for primes \( p_i \in R \). Then wlog \( p_1 \in p \), i.e. \( p_1 R \subset p \). Since \( \dim R \leq 1 \), we have \( p_1 R = p \).

(3) \implies (1) Since every fractional ideal is principal, every ideal is principal.

Example 2.4.10. Let \( K/\mathbb{Q} \) be a finite field extension and \( R = \mathcal{O}_K \subset K \) be the integral closure of \( \mathbb{Z} \) in \( K \). The groups \( K^\times \) and \( \text{Frac}(R) \) are not finitely generated, while results from algebraic number theory state that \( \text{Cl}(R) \) is finite and \( R^\times \) is finitely generated. However, the structure of \( \text{Cl}(R) \) is not clear. For example, it is an open problem whether there are infinitely many Dedekind domains of the form \( \mathbb{Z}[\sqrt{d}] \) for which the class group is trivial.

2.5 Modules over Dedekind domains

Let \( M \) be a finitely generated torsion \( R \)-module, where \( R \) is a Dedekind domain, so then there exists a non-zero \( a \in R \) such that \( aM = 0 \).

Definition 2.5.1 (\( p \)-primary module). Let \( p \subset R \) be a non-zero prime ideal. We say that \( M \) is \( p \)-primary if \( p^n M = 0 \) for some \( n > 0 \).

By a similar proof as before, using the fact that \( p_1 + p_2 = R \) whenever \( p_1 \neq p_2 \) are non-zero primes,

\[
M = \bigoplus_{0 \neq p \subset R} M(p),
\]

with \( M(p) \) a \( p \)-primary module. Hence it suffices to consider the structure of \( p \)-primary modules.

Let \( M \) be \( p \)-primary, \( p^n M = 0 \), and \( s \in S := R \setminus p \). Then \( p^n + sR = R \), since no maximal ideal contains both \( p^n \) and \( s \).

Lemma 2.5.2. The map \( M \to M \), \( m \mapsto sm \) is an isomorphism.

Proof. If \( sm = 0 \), then \( m = am + bsm = 0 \), where \( a + bs = 1 \) for some \( a \in p^n \) and \( b \in R \). This shows injectivity, and for surjectivity, we have \( m = am + bsm = s(bm) \), where \( a, b \) are as before. \( \square \)

Hence \( M \) is a finitely generated module over the local ring \( S^{-1}R = R_p \), which is a PID (see HW3), so we can use the structure theorems from that case.

Note that \( R_p/p^n R_p \simeq R/p^n \) as elements of \( S \) are invertible in \( R/p^n \).
Theorem 2.5.3 (Elementary divisor form). Let $M$ be a finitely generated torsion module over a Dedekind domain $R$. Then there exist unique (up to permutation) ideals $p_1^{m_1}, \ldots, p_k^{m_k}$ such that

$$M \cong \bigoplus_{i=1}^{k} R/p_i^{m_i}.$$ 

Theorem 2.5.4 (Invariant factor form). Let $M$ be a finitely generated torsion module over a Dedekind domain $R$. Then there are unique ideals $a_1 \supset a_2 \supset \cdots \supset a_r$ such that

$$M \cong \bigoplus_{i=1}^{r} R/a_i.$$ 

Now we consider finitely generated torsion-free modules.

Lemma 2.5.5. Every finitely generated torsion-free $R$-module $M$ is isomorphic to a submodule of $R^n$ for some $n$.

Proof. Let $F$ be the quotient field of $R$ and write $S = R \setminus \{0\}$. Then $S^{-1}M$ is a finitely generated $F$-module, hence $S^{-1}M \cong F^n$. The canonical map $M \to S^{-1}M$ has kernel $M_{\text{tors}} = 0$, so $M$ embeds in $F^n$ and is an $R$-module. Hence there exists $a \in R$ non-zero such that $M \cong aM \subset R^n$. \hfill\qed

Theorem 2.5.6. Let $M$ be a finitely generated torsion-free $R$-module. Then there exist ideals $a_1, \ldots, a_n \subset R$ such that

$$M \cong \bigoplus_{i=1}^{n} a_i.$$ 

In particular, $M$ is projective.

Proof. By the lemma, we can suppose $M \subset R^n$. When $n = 1$, the result is clear.

In the general case, consider the projection $f : R^n \to R$ onto the last coordinate. By restricting, we have a surjective map $M \to f(M)$ whose kernel is $M \cap (R^{n-1} \times \{0\})$. By construction, $f(M) \subset R$ is an ideal, hence projective. This gives us a short exact sequence, so

$$M \cong (M \cap R^{n-1}) \oplus f(M).$$

The result follows by induction. \hfill\qed
For any finitely generated $R$-module $M$, the short exact sequence

$$0 \longrightarrow M_{\text{tors}} \longrightarrow M \longrightarrow M/M_{\text{tors}} \longrightarrow 0$$

is split, since $M/M_{\text{tors}}$ is finitely generated and torsion-free, hence projective. Thus

$$M \cong M_{\text{tors}} \oplus (M/M_{\text{tors}}),$$

so since $M$ is finitely generated, $M_{\text{tors}}$ is finitely generated. Thus we have a decomposition, but up to this point, we do not have uniqueness of the ideals in the previous theorem. By localizing to $F$, the number of ideals $n$ is fixed. We will see later that $[a_1 \cdots a_n] \in Cl(R)$ is a well-defined invariant.

Let $a, b \subset R$ be non-zero ideals. For $x \in ba^{-1}$, the “multiplication by $x$” map $l_x : m \mapsto xm$ is an $R$-module homomorphism $a \rightarrow b$.

**Proposition 2.5.7.** Every homomorphism $a \rightarrow b$ is of the form $l_x$ for some $x \in ba^{-1}$. Moreover, the choice of $x$ is unique, so $\text{Hom}_R(a, b) = ba^{-1}$.

**Proof.** Uniqueness is clear, so we must show existence. Let $f : a \rightarrow b$, then choose $m \in a$ and $a \in a$ non-zero. Then $af(m) = f(am) = f(a)m$, so $f(m) = xm$, where $x = f(a)/a \in F$ and $x \in xR = xaa^{-1} \subset ba^{-1}$. \hfill $\square$

**Remark 2.5.8.** The composition map $\text{Hom}(b, c) \times \text{Hom}(a, b) \rightarrow \text{Hom}(a, c)$ coincides with the product map $cb^{-1} \times ba^{-1} \rightarrow ca^{-1}$.

**Corollary 2.5.9.** If $a, b \subset R$ are non-zero ideals, then $a \cong b$ as $R$-modules if and only if $[a] = [b]$.

**Proof.** An isomorphism between $a$ and $b$ is given by multiplication by some $x \in ba^{-1}$, so $b = xa$ and hence $[a] = [b]$. Conversely, if $[a] = [b]$, we have $b = xa$ for some $x \in F$, therefore, multiplication by $x$ yields an isomorphism $a \cong b$. \hfill $\square$

For $a \in \text{Frac}(R)$, write $[a]$ for its class in $\text{Cl}(R)$.

**Proposition 2.5.10.** Let $a_1, \ldots, a_n, b_1, \ldots, b_m \subset R$ be non-zero ideals such that $M = \bigoplus_i a_i \cong \bigoplus_j b_j$. Then $n = m$ and $[a_1 \cdots a_n] = [b_1 \cdots b_m]$.

**Proof.** We noted earlier that $n = m = \dim_F(S^{-1}M)$, where $S = R \setminus \{0\}$.

Let $f : \bigoplus_i a_i \rightarrow \bigoplus_j b_j$ be an isomorphism represented by the matrix $C = (c_{ij})$, where $c_{ij} \in \text{Hom}(a_i, b_j) = b_j a_i^{-1} \subset F$. We claim that if $a_i \in a_i$, then

$$\det(C)a_1 \cdots a_n \subset b_1 \cdots b_n.$$
Indeed, let $D = C \cdot \text{diag}(a_1, \ldots, a_n)$, so then $d_{ij} = c_{ij}a_j \in b_i$. Taking determinants we get $\det(C)a_1 \cdots a_n \in b_1 \cdots b_n$. This proves the claim.

Using the claim in both directions, we get equality, so $\det(C)a_1 \cdots a_n = b_1 \cdots b_n$. In the class group, this reduces to the desired result. 

**Definition 2.5.11** (Determinant of a module). Let $M$ be a finitely generated torsion-free $R$-module and write $M \cong \bigoplus_i a_i$. The **determinant** of $M$ is

$$\det(M) = [a_1 \cdots a_n] \in \text{Cl}(R).$$

**Proposition 2.5.12.**

1. $\det(M \oplus N) = \det(M) \det(N)$.

2. If $a \subset R$ is a non-zero ideal, then $\det(a) = [a]$.

**Lemma 2.5.13.** Let $p_1, \ldots, p_n \subset R$ be distinct non-zero prime ideals and $k_1, \ldots, k_n \geq 0$. Then there exists $a \in R$ such that $\nu_{p_i}(a) = k_i$ for all $i$.

**Proof.** Note that if $a \in p^k$ but $a \notin p^{k+1}$, then $\nu_{p_i}(a) = k$.

Choose $a_i \in p^{k_i} \setminus p^{k_i+1}$. By the Chinese remainder theorem, there exists $a \in R$ such that $a \equiv a_i \pmod{p^{k_i+1}}$. 

**Corollary 2.5.14** (Prime avoidance lemma for Dedekind domains). Let $a \subset R$ be a non-zero ideal and $p_1, \ldots, p_n$ be non-zero prime ideals. Then there is a non-zero ideal $a'$ such that $[a'] = [a]$ and $a' \notin p_i$ for $i = 1, \ldots, n$.

**Proof.** Let $a \in a$ be non-zero and write $aR = ab$. Let $S$ be the set of prime divisors of $b$ and $T = \{p_1, \ldots, p_n\}$. The result then follows by applying the lemma to $S \cup T$: there is $b \in R$ such that $\nu_{p_i}(b) = \nu_{p_i}(b)$ (the latter being the largest power of $p$ dividing $b$) for all $p \in S \cup T$. Then

$$b \in \bigcap_p p^{\nu_p(b)} = \prod_p p^{\nu_p(b)} = b.$$ 

Let $a'$ be an ideal such that $bR = a'b$. By the choice of $b$ we have $\nu_{p_i}(a') = 0$ for all $i$, i.e., $a' \notin p_i$ for all $i$. In view of $aR = ab$ we have $[a'] = [a]$. 

**Corollary 2.5.15.** Let $a, b \subset R$ be non-zero ideals. Then there is a non-zero ideal $a'$ such that $a' \cong a$ as $R$-modules and $a' + b = R$.

**Proposition 2.5.16.** Let $a$ and $b$ be non-zero ideals. Then $a \oplus b \cong R \oplus ab$. 

21
Proof. Find $a'$ as in the previous corollary. Then the kernel of the surjective map $(a,b) \mapsto a + b$ from $a' \oplus b$ to $R$ is $a' \cap b = a'b$, so

$$a \oplus b \cong a' \oplus b \cong R \oplus a'b \cong R \oplus ab.$$ \hfill \Box

Theorem 2.5.17. Let $R$ be a Dedekind domain.

1. Every finitely generated torsion-free $R$-module $M$ of rank $n$ is isomorphic to $R^{n-1} \oplus a$, where $a$ is a nonzero ideal such that $[a] = \det(M)$.

2. Two finitely generated torsion-free $R$-modules are isomorphic if and only if they have the same rank and determinant.

Definition 2.5.18 (Picard group). The Picard group of $R$ is the group $\text{Pic}(R)$ of rank 1 projective $R$-modules with the tensor product over $R$ as the group operation.

Proposition 2.5.19. For Dedekind domains, $\text{Pic}(R) \cong \text{Cl}(R)$. 
3 Semisimple Modules and Rings

Throughout, \( R \) is a ring (not necessarily commutative).

3.1 Definitions and basic properties

Definition 3.1.1 (Simple module). A (left) \( R \)-module \( M \) is simple if \( M \neq 0 \) and \( M \) has no non-trivial submodules.

Lemma 3.1.2. Let \( M \) be a (left) \( R \)-module. Then \( M \) is simple if and only if \( M \cong R/I \) as \( R \)-modules for some maximal (left) ideal \( I \).

Proof. Suppose \( M \) is simple. Fix \( m \in M \) non-zero and define \( f : R \to M \) by \( f(a) = am \). Since \( m \in f(R) \), we have \( 0 \neq f(R) \subset M \), so \( f(R) = M \). Hence \( M \cong R/\text{Ker} f \), and by the correspondence of submodules, it follows that \( \text{Ker} f \) is maximal as a left ideal. Conversely, the correspondence tells us that \( R/I \) is simple whenever \( I \) is a maximal left ideal. \( \square \)

Corollary 3.1.3. Every \( R \neq 0 \) admits simple modules.

Proposition 3.1.4. Let \( M \) be an \( R \)-module. Then \( M \) is simple if and only if \( M \neq 0 \) and for any non-zero \( m \in M \), we have \( Rm = M \).

Example 3.1.5. 1. If \( F \) is a field, then the only simple \( F \)-module is \( F \). More generally, if \( D \) is a division ring, the only simple \( D \)-module is \( D \).

2. The simple \( \mathbb{Z} \)-modules are of the form \( \mathbb{Z}/p\mathbb{Z} \) for \( p \) a prime number.

3. Let \( D \) be a division ring. Then all modules are free. Let \( S = M_n(D) \), so then \( S^\times = \text{GL}_n(D) \) acts transitively on \( M/0 \), where \( M = D^n \). It follows that \( M = D^n \) is a simple \( S \)-module.

4. Let \( L \subset R \) be a (left) ideal. Then \( L \) is a minimal (left) ideal if and only if \( L \) is a simple (left) \( R \)-module.

Lemma 3.1.6 (Schur). Let \( f : M \to N \) be an \( R \)-module homomorphism of simple (left) \( R \)-modules. Then \( f = 0 \) or \( f \) is an isomorphism.

Proof. If \( f \neq 0 \), then \( f(M) \neq 0 \), so \( f(M) = N \). Then \( \text{Ker} f \neq M \), so \( \text{Ker} f = 0 \). \( \square \)

Corollary 3.1.7. If \( M \) is a simple \( R \)-module, then \( \text{End}_R(M) \) is a division ring.
**Definition 3.1.8** (Semisimple module). A (left) $R$-module $M$ is *semisimple* if there is a family of simple submodules $M_i$ such that $M = \bigoplus_i M_i$.

We say that $R$ is a (left) *semisimple ring* if $R$ is semisimple as a (left) $R$-module.

**Remark 3.1.9.** The zero module is semisimple but not simple. The zero ring is semisimple.

If $R$ is a semisimple ring, then there is a family $L_i$ of left minimal ideals such that $R = \bigoplus_i L_i$. Then there exist $e_i \in L_i$, all but finitely many zero, such that $1 = \sum_i e_i$. Hence $a = \sum_i a e_i$ for all $a \in R$, so if $\Delta$ is the set of indices with $e_i \neq 0$, then $R = \bigoplus_{i \in \Delta} L_i$. Moreover, from the fact that $R$ is a direct sum, it follows that the $\{e_i\}$ for $i \in \Delta$ are orthogonal idempotents that partition 1, with $L_i = Re_i$.

**Proposition 3.1.10.** Let $R$ be a left semisimple ring with $R = \bigoplus_i Re_i$ with $Re_i$ minimal left ideals. Then the right ideal $e_i R$ is minimal for all $i$ and $R = \bigoplus_i e_i R$, so $R$ is a right semisimple ring.

**Proof.** That $R = \bigoplus_i e_i R$ follows from the $e_i$ being orthogonal idempotents which partition 1. It remains to show that $e_i R$ is minimal. Write $e = e_i$ and let $a \in e R$ be non-zero. We must show that $aR = eR$. The inclusion $aR \subset eR$ is clear.

Since $a \in e R$ and $e^2 = e$, we have $ea = a$. We also have $a = \sum_j a_j e_j$, so there exists $j$ such that $ae_j \neq 0$. Then $0 \neq Rae_j \subset Re_j$ and $Re_j$ is simple, so $Rae_j = Re_j$. There exists $b \in R$ such that $bae_j = e_j$.

Now let $f : Re \to Re_j$ be given by $f(c) = cae_j$. This is a homomorphism of left $R$-modules which is non-zero since $f(e) = eae_j = ae_j \neq 0$. By Schur’s lemma, $f$ is an isomorphism. We compute $f(abe) = abae_j = abae_j = ae_j$, so $e = abe \in aR$, hence $eR \subset aR$. \qed

**Definition 3.1.11.** We say that a ring $R$ is *semisimple* if $R$ is left semisimple = right semisimple.

**Example 3.1.12.**

1. If $R_1, \ldots, R_n$ are semisimple, then $R_1 \times \cdots \times R_n$ is semisimple.

2. Let $D$ be a division ring and $R = M_n(D)$. The left ideal $L_i$ of matrices with all columns zero except possibly the $i$-th column is a minimal left ideal with $L_i \cong D^n$ as an $R$-module. Since $R \cong L_1 \oplus \cdots \oplus L_n$, we have that $R$ is semisimple. The idempotents are the matrices $e_{ii}$ with a 1 in entry $ii$ and 0’s everywhere else.
3. If $D_1,\ldots,D_k$ are division rings, then $M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ is semisimple.

**Lemma 3.1.13.** Let $M$ be a left $R$-module that is a sum of simple left modules. Then $M$ is semisimple.

**Proof.** Write $M = \sum_{i \in \Gamma} M_i$ for $M_i$ simple. Let

$$A = \left\{ \Delta \subset \Gamma \mid \sum_{i \in \Delta} M_i = \bigoplus_{i \in \Delta} M_i \right\}.$$

This satisfies the conditions of Zorn’s lemma, so we can extract a maximal set of indices $\Delta$. Then $M = \sum_{i \in \Delta} M_i = \bigoplus_{i \in \Delta} M_i$. □

**Lemma 3.1.14.** Let $R$ be a semisimple ring and write $R = \bigoplus_{i=1}^n L_i$ for $L_i$ minimal left ideals. Then any simple left $R$-module is isomorphic to $L_i$ for some $i$.

**Proof.** Let $M$ be a simple left $R$-module. Then

$$0 \neq M \cong \text{Hom}_R(R,M) = \text{Hom}_R\left(\bigoplus_{i=1}^n L_i, M\right) \cong \prod_{i=1}^n \text{Hom}_R(L_i, M),$$

so some $\text{Hom}_R(L_i, M)$ is non-zero. Let $f : L_i \to M$ be non-zero. By Schur’s lemma, $f$ is an isomorphism. □

**Corollary 3.1.15.** There are finitely many simple (left) $R$-modules up to isomorphism. Every minimal (left) ideal is isomorphic to $L_i$ for some $i$.

**Example 3.1.16.** Let $D$ be a division ring and $R = M_n(D)$. Then $M = D^n$ is the only (up to isomorphism) simple (left) $R$-module.
Theorem 3.1.17. Let $R$ be a ring. The following are equivalent:

1. $R$ is semisimple;
2. every (left) $R$-module is semisimple;
3. every (left) $R$-module is projective;
4. every (left) $R$-module is injective;
5. every short exact sequence of (left) $R$-modules is split.

Proof. (1) $\implies$ (2) Write $R = \bigoplus_{i=1}^{n} L_i$ and let $M$ be a left $R$-module. Then

$$M = RM = \sum_{i=1}^{n} L_i M = \sum_{1 \leq i \leq n, m \in M} L_i m$$

is a sum of simple modules, hence semisimple.

(2) $\implies$ (3) In particular, $R$ is semisimple, so $R = \bigoplus_{i=1}^{n} L_i$. Let $M$ be a module, hence semisimple, and write $M$ as a direct sum of the $L_i$. Each $L_i$ is projective, so $M$ is projective.

(3) $\implies$ (5) This follows from the characterization of projective modules.

(5) $\implies$ (4) This follows from the characterization of injective modules.

(4) $\implies$ (1) Let $I$ be the sum of all left minimal ideals in $R$. We must show that $I = R$. If not, then $I$ is contained in a maximal left ideal $M \subset R$. The short exact sequence

$$0 \to M \to R \to R/M \to 0$$

is split since $M$ is injective, so there is a submodule $J \subset R$ such that $J \to R \to R/M$ is an isomorphism. Then $J \cap M = 0$ and $J$ is simple, hence a minimal left ideal, contradicting the choice of $M$. 

$\square$
Theorem 3.1.18 (Artin-Wedderburn). A ring $R$ is semisimple if and only if

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

for some division rings $D_1, \ldots, D_k$.

Proof. Let $L_1, \ldots, L_k$ be non-isomorphic minimal left right ideals. Then

$$R \cong N_1 \oplus \cdots \oplus N_k$$

for some $N_i \cong L_i^{n_i}$. There is a canonical isomorphism $R \cong \text{End}_R(R)$ as right $R$-modules, where $r \in R$ corresponds to left multiplication by $r$ in $\text{End}_R(R)$. On the other hand, $\text{End}_R(R)$ is the ring of matrices $(s_{ij})$ with $s_{ij} \in \text{Hom}_R(N_j, N_i)$. By Schur’s lemma, we have $\text{Hom}_R(L_j, L_i) = 0$ if $i \neq j$ and $\text{Hom}_R(L_j, L_i) = D_i = \text{End}_R(L_i)$ if $i = j$. Therefore,

$$S_{ij} = \text{Hom}_R(N_j, N_i) = \begin{cases} 0 & \text{if } i \neq j, \\ M_{n_i}(D_i) & \text{if } i = j. \end{cases}$$

The result follows. \qed

Remark 3.1.19. 1. The central orthogonal idempotents $e_1, \ldots, e_k \in R$ with $1 = e_1 + \cdots + e_k$ are unique up to permutation. Therefore, the decomposition $R = N_1 \oplus \cdots \oplus N_k$ is unique up to permutation. These are the isotypic components of $R$.

2. Since every simple right $R$-module $M$ is isomorphic to exactly one $L_i$, we have that $k$ is the number of simple right $R$-modules up to isomorphism. The same is true for left $R$-modules.

3. Every $N_i$ is the sum of the minimal right ideals isomorphic to $L_i$. A direct sum can be chosen from this, but not uniquely. However, the matrix ring components $M_{n_i}(D_i)$ are unique, with $D_i = \text{End}_R(L_i)$ and $n_i = \dim_D(\text{Hom}_R(L_i, R))$.

More generally, let $M$ be a right $R$-module with $M \cong L_1^{a_1} \oplus \cdots \oplus L_k^{a_k}$. Then $a_i = \dim_D(\text{Hom}_R(L_i, M))$. 27
Remark 3.1.20. (Morita equivalence) Let $R$ be a ring and $P$ a right $R$-module. Set $S = \text{End}_R(P)$. Then $P$ is also a left $S$-module: $sP_R$. If $M$ is a left $R$-module, the tensor product $P \otimes_R M$ is a left $S$-module, and we have a functor

$$F : R\text{-Mod} \to S\text{-Mod}, \quad M \mapsto P \otimes_R M.$$  

If $N$ is a left $S$-module, then $\text{Hom}_S(P, N)$ is a left $R$-module, and we have got a functor

$$G : S\text{-Mod} \to R\text{-Mod}, \quad N \mapsto \text{Hom}_S(P, N).$$

For a left $R$-module $M$, the natural $R$-module homomorphism

$$M \to \text{Hom}_S(P, P \otimes_R M) = (G \circ F)(M), \quad m \mapsto (p \mapsto p \otimes m)$$

yields a morphism of functors $\alpha : 1_{R\text{-Mod}} \to G \circ F$ from $R\text{-Mod}$ to itself. For a left $S$-module $N$, the natural $S$-module homomorphism

$$(F \circ G)(M) = P \otimes_R \text{Hom}_S(P, N) \to N, \quad p \otimes f \mapsto f(p)$$

yields a morphism of functors $\beta : F \circ G \to 1_{S\text{-Mod}}$ from $S\text{-Mod}$ to itself. Under certain conditions on $sP_R$, the morphism of functors $\alpha$ and $\beta$ are isomorphisms, so that $F$ and $G$ are two equivalences between the categories $R\text{-Mod}$ and $S\text{-Mod}$. In particular, this holds if $P = R^n$ is a free right $R$-module. In this case $S = M_n(R)$:

$$M_n(R)\text{-Mod} \cong R\text{-Mod}.$$  

From the Morita equivalence, it follows that if $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ is a semisimple ring, we have a categorical equivalence

$$R\text{-Mod} \cong D_1\text{-Mod} \times \cdots \times D_k\text{-Mod}.$$
3.2 The Jacobson radical

Definition 3.2.1 (Radical of a module). Let \( R \) be a ring and \( M \) be a left \( R \)-module. The radical of \( M \), denoted \( \text{rad}_R(M) \), is the intersection of all maximal submodules of \( M \).

Example 3.2.2. 1. \( \text{rad}(\mathbb{Z}) = 0 \)

2. \( \text{rad}_R[M/\text{rad}_R(M)] = 0 \)

Proposition 3.2.3. Let \( M \) be a left \( R \)-module.

1. If \( M \) is semisimple, then \( \text{rad}_R(M) = 0 \).

2. If \( M \) is artinian and \( \text{rad}_R(M) = 0 \), then \( M \) is semisimple.

Proof. 1. Write \( M \) as a direct sum of simple modules.

2. Let \( N \subset M \) be the sum of all simple submodules. If \( N \neq M \), then let \( N' \) be a minimal submodule of \( M \) such that \( N + N' = M \).

We claim that \( N \cap N' = 0 \). Suppose \( N \cap N' \neq 0 \). Since \( \text{rad}_R(M) = 0 \), there is a maximal submodule \( M' \subset M \) with \( N \cap N' \) not contained in \( M' \), so then \( (N \cap N') + M' = M \).

We claim that

\[ N + (M' \cap N') = M. \]

Let \( m \in M \). Write \( m = n + n' \), where \( n \in N \) and \( n' \in N' \), and \( n' = n'' + m' \) with \( n'' \in N \cap N' \) and \( m' \in M' \). Then \( m' = n' - n'' \in M' \cap N' \) and \( m = n + n' = (n + n'') + m' \in N + (M' \cap N') \). The second claim is proved.

By the choice of \( N' \), we have \( M' \cap N' = N' \), hence \( N' \subset M' \), contradicting the choice of \( M' \). The first claim is proved.

Thus, \( N \cap N' = 0 \), hence \( M = N \oplus N' \) with \( N' \neq 0 \), and we can choose a simple submodule of \( N' \) which is not in \( N \).

\[ \square \]
Lemma 3.2.4. rad($R$) is the set of all elements $a \in R$ such that $1 - ba$ has a left inverse for all $b \in R$.

Proof. If $a \in \text{rad}(R)$ but $R(1 - ba) \neq R$ for some $b \in R$, then there is a maximal left ideal $M \subset R$ such that $R(1 - ba) \subset M$. Since $a \in M$, we have $1 \in M$, a contradiction.

Conversely, suppose $1 - ba$ has a left inverse for all $b \in R$ and let $M$ be a maximal left ideal. If $a \notin M$, then $Ra + M = R$, so $1 = ba + m$ for some $m \in M$. Then $1 - ba = m \in M$ has a left inverse by hypothesis, so $1 \in M$, a contradiction. \hfill \Box

Lemma 3.2.5. If $1 - ab$ is left invertible, then so is $1 - ba$.

Proof. If $c(1 - ab) = 1$, then $(bca + 1)(1 - ba) = 1$. \hfill \Box

Proposition 3.2.6. rad($R$) is the set of all elements $a \in R$ such that $1 - bac \in R^\times$ for all $b, c \in R$.

Proof. If $1 - bac \in R^\times$ for all $b, c \in R$, then in particular $1 - ba \in R^\times$ for all $b \in R$, so $a \in \text{rad}(R)$.

Conversely, if $a \in \text{rad}(R)$, then $1 - cba$ is left invertible for all $c, b \in R$, so then $1 -bac$ is left invertible. If $d$ is its left inverse, then since $1 + cdba$ is left invertible, $d = 1 + dbac$ is left invertible. Hence $d$ is left and right invertible, so $d \in R^\times$ and $d^{-1} = 1 - bac \in R^\times$. \hfill \Box

Corollary 3.2.7. rad($R$) is the intersection of all right maximal ideals of $R$ and the intersection of all left maximal ideals of $R$, hence a two-sided ideal.

Definition 3.2.8 (Jacobson radical). The Jacobson radical is the two-sided ideal $J(R) = \text{rad}(R)$.

Theorem 3.2.9. A ring $R$ is semisimple if and only if $R$ is artinian and $J(R) = 0$.

Proof. It is only necessary to check that $R$ is artinian if it is semisimple. This follows from $R$ being isomorphic to a finite product of matrix rings $M_n(D)$ for division rings $D$. \hfill \Box

Definition 3.2.10 (Simple ring). A non-zero ring $R$ is simple if $R$ has no non-trivial two-sided ideals.

Example 3.2.11. If $D$ is a division ring, then $M_n(D)$ is simple.
Theorem 3.2.12. A ring $R$ is simple and artinian if and only if $R = M_n(D)$ for some division ring $D$.

Proof. Let $R$ be a simple and artinian. Since $J(R) \neq R$ and is a two-sided ideal, we have $J(R) = 0$, so $R$ is semisimple. By Artin-Wedderburn, $R$ is a product of matrix rings. If the product has at least two factors, then there are non-trivial proper two-sided ideals, so the product has just one factor. \qed
4 Representations of Finite Groups

4.1 The three languages

Definition 4.1.1 (G-space). Let $G$ be a group. A vector space $V$ over a field $F$ is a $G$-space if $G$ acts linearly on $V$, i.e. the action has the additional property that $v \mapsto gv$ is a linear operator for each $g$.

Definition 4.1.2 (Representation). A (linear) representation of a group $G$ is a homomorphism $\rho : G \to GL(V)$ for some vector space $V$ over a field $F$.

Given a $G$-space $V$, we can define $\rho : G \to GL(V)$ by $\rho(g)v = gv$. Conversely, given $\rho : G \to GL(V)$, we can make $V$ a $G$-space by $gv = \rho(g)(v)$.

Example 4.1.3. 1. Any group $G$ can act trivially on any vector space $V$. The corresponding representation is the trivial homomorphism.

2. If $V$ is a $G$-space of dimension $n$, then choosing a basis, we get $GL(V) \cong GL_n(F)$, so the corresponding representation can be regarded as a homomorphism $\rho : G \to GL_n(F)$.

Definition 4.1.4 (Group algebra). Let $G$ be a group and $F$ be a field. The group algebra of $G$ over $F$, denoted $F[G]$, is the free vector space generated by the set $G$, together with multiplication induced by the group law on the generators.

If $V$ is a $G$-space, then $V$ is a left $F[G]$-module by extending linearly. Conversely, given a left $F[G]$-module $V$, restriction of the action to $G \subset F[G]$ gives $V$ the structure of a $G$-space.

We therefore have the following equivalent categories for representation theory.

<table>
<thead>
<tr>
<th>Objects</th>
<th>Morphisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G$-spaces $V$</td>
<td>$F$-linear maps $f : V \to W$ such that $f(gv) = gf(v)$</td>
</tr>
<tr>
<td>Representations $\rho : G \to GL(V)$</td>
<td>$F$-linear maps $f : V \to W$ such that $f(\rho(g)(v)) = \mu(g)(f(v))$</td>
</tr>
</tbody>
</table>

Example 4.1.5. 1. Let $G = \mathbb{Z}/n$. Then

$$Q[G] = Q[t]/(t^n - 1) \cong \prod_{d|n} Q[t]/(\Phi_d(t)) \cong \prod_{d|n} Q(\zeta_d).$$
2. Let $F$ be a field with char $F = p > 0$ and let $G = \mathbb{Z}/p$. Then
\[ F[G] = F[t]/(t^p - 1) = F[s]/(s^p). \]

**Theorem 4.1.6.** Let $G$ be a finite group and $F$ be a field. Then $F[G]$ is semisimple if and only if char $F \nmid |G|$.

**Proof.** ($\Rightarrow$) Consider the augmentation map $\varepsilon : F[G] \to F$ given by the sum of coefficients. Note that $F$ has the structure of an $F[G]$-module by the trivial action, so if $I = \text{Ker} \varepsilon$, then $0 \to I \to F[G] \to F \to 0$ is a short exact sequence of $F[G]$-modules. By assumption, $F[G]$ is semisimple, so the sequence splits and there exists $f : F \to F[G]$ such that $f \circ \varepsilon = \text{id}_F$. If $f(1) = u$, then $gu = u$ for all $g \in G$, so then $u = a \sum g$ for some $a \in F$. Applying $\varepsilon$, we get $a |G| = 1$.

($\Leftarrow$) Let $0 \to N \to M \to P \to 0$ be a short exact sequence of $F[G]$-modules. Then this is also a short exact sequence of $F$-modules, i.e. free vector spaces, so we can find a linear map $h : P \to M$ such that $f \circ h = \text{id}_P$. The hypotheses allow us to replace $h$ with the averaged map
\[ h'(p) = \frac{1}{|G|} \sum_{g \in G} g(h(g^{-1}p)). \]

\[ \blacksquare \]

**Proposition 4.1.7.** Let $F$ be algebraically closed of characteristic zero and let $D$ be a finite-dimensional $F$-algebra which is also a division ring with $F \subset Z(D)$. Then $D = F$.

**Proof.** Let $a \in D$. Then $1, a, \ldots, a^n$ are linearly dependent for sufficiently large $n$, so there is a non-zero polynomial $f \in F[x]$ such that $f(a) = 0$. Since $F$ is algebraically closed, $a \in F$. \[ \blacksquare \]

As a corollary, the Artin-Wedderburn theorem tells us that $F[G] = M_{d_1}(F) \times \cdots \times M_{d_k}(F)$. There are finitely many simple $F[G]$-modules, which have the form $M_i \cong F^{d_i}$. Hence $d_i = \dim_F (M_i)$. Every $G$-space is a direct sum of spaces $M_i$. Computing dimensions,
\[ |G| = d_1^2 + \cdots + d_k^2. \]

Equivalently, there are finitely many irreducible representations $\rho_i : G \to GL(M_i)$. Every representation $\rho : G \to GL(V)$ can be written as a finite direct sum $\rho \cong \bigoplus \rho_i^{\oplus n_i}$. 34
Consider the center $Z(\mathbb{F}[G])$. The condition that $\alpha \in Z(\mathbb{F}[G])$ is equivalent to the condition that $\alpha$ commutes with all basis elements $g \in G$. Writing $\alpha = \sum g a_g g$, it can be computed that this happens if and only if $a_g = a_{g'}$ whenever $g$ and $g'$ are in the same conjugacy class. If $C_1, \ldots, C_l$ are the conjugacy classes of $G$ and $u_i = \sum_{g \in C_i} g$, then $\{u_1, \ldots, u_l\}$ is a basis for $Z(\mathbb{F}[G])$. In particular, $\dim(Z(\mathbb{F}[G]))$ is the number of conjugacy classes of $G$.

On the other hand, since $\mathbb{F}[G] \cong \prod_i M_d_i(\mathbb{F})$ (with $k$ factors) and $Z(M_d(\mathbb{F})) = \mathbb{F} \cdot I_d$ is one-dimensional, we have $\dim(Z(\mathbb{F}[G])) = k$. Hence the number of irreducible representations is equal to the number of conjugacy classes of $G$.

### 4.2 One-dimensional representations

**Definition 4.2.1** (Multiplicative character). Let $G$ be a finite group and $V$ be a one-dimensional vector space over a field $\mathbb{F}$. A representation $\rho : G \to GL(V) = \mathbb{F}^\times$ is a (multiplicative) character of $G$.

In terms of matrices, two matrix representations $\rho, \mu : G \to GL_n(\mathbb{F})$ are isomorphic if and only if there is a matrix $P \in GL_n(\mathbb{F})$ such that $\mu(g) = P\rho(g)P^{-1}$ for all $g$. In particular, if $\rho, \mu : G \to \mathbb{F}^\times$ are one-dimensional representations, then $\rho \cong \mu$ if and only if $\rho = \mu$.

Suppose $G$ is abelian of order $n$. Then $G$ has $n$ conjugacy classes and the dimensions satisfy $d_1^2 + \cdots + d_n^2 = n$, so $d_i = 1$ for all $i$. This shows that all irreducible representations of an abelian group are one-dimensional, i.e. $|\text{Hom}(G, \mathbb{F}^\times)| = n$. In fact, $\text{Hom}(G, \mathbb{F}^\times) \cong G$, but we will not show this.

Now consider a general finite group $G$ and let $\rho : G \to \mathbb{F}^\times$ be a one-dimensional representation. Then $\rho$ factors through $G/G'$, the abelianization of $G$. Hence there are exactly $|G/G'|$ one-dimensional representations of $G$.

**Example 4.2.2.** Unless otherwise specified, the representations are assumed to be complex representations.

1. The group $S_4$ has order 24, and it has 5 conjugacy classes. Its derived subgroup is $A_4$, so there are two one-dimensional representations, i.e. $d_1 = d_2 = 1$ if the dimensions $d_i$ are listed in increasing order. These are the trivial representation and the sign representation which sends each permutation to $\pm 1$ depending on whether the permutation is even or odd. The dimensions $d_3, d_4, d_5$ satisfy $d_3^2 + d_4^2 + d_5^2 = 22$, so we must have $d_3 = 2$ and $d_4 = d_5 = 3$. 


2. Consider the group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, which has 5 conjugacy classes. The commutator subgroup is $\{\pm 1\}$, so there are four one-dimensional representations, which are defined by $i \mapsto \pm 1$ and $j \mapsto \pm 1$. The last irreducible representation must then have dimension 2, which is defined by

$$
i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

### 4.3 Characters

**Definition 4.3.1** (Character). Let $\rho : G \to GL(V)$ be a representation. The character of $\rho$ is the function $\chi_\rho : G \to F$ given by $\chi_\rho(g) = \text{tr} \rho(g)$.

**Example 4.3.2.** If $\dim \rho = 1$, then $\chi_\rho = \rho$.

Equivalently, if $V$ is a $G$-space, then we define $\chi_V : G \to F$ by $\chi_V(g) = \text{tr}(v \mapsto gv)$.

**Proposition 4.3.3.**

1. If $\rho \cong \mu$, then $\chi_\rho = \chi_\mu$.

2. $\chi_{\rho \oplus \mu} = \chi_\rho + \chi_\mu$.

3. $\chi_{\rho \circ \rho}(gh^{-1}) = \chi_\rho(g)$ for all $g, h \in G$.

4. $\chi_\rho(1) = \dim \rho$.

**Example 4.3.4** (Regular representation). Given a finite group $G$, we have a natural left $F[G]$-module structure on $V = F[G]$, and the corresponding representation is the regular representation of $G$. The elements of $G$ form a basis for $V$, and the matrix of the action of an element $g$ with respect to this basis is a permutation matrix. If $g \neq 1$, then $g$ fixes no basis element, so $\chi_{\text{reg}}(g) = 0$ for $g \neq 1$ and $\chi_{\text{reg}}(1) = |G|$.

The regular representation has the form $\rho_{\text{reg}} = \bigoplus_i \rho_i^{d_i}$, so $\chi_{\text{reg}} = \sum_i d_i \chi_{\rho_i}$.

A character $\chi_\rho$ can be extended to an $F$-linear map $\chi_\rho : F[G] \to F$, i.e. a linear functional on the vector space $F[G]$.

**Example 4.3.5.** For $G = Q_8$, we get a character table as shown.
\[ \begin{array}{ccccccc}
1 & -1 & i & -i & j & -j & k & -k \\
\chi_1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\chi_2 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
\chi_3 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\
\chi_4 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\
\chi_5 & 2 & -2 & 0 & 0 & 0 & 0 & 0 \\
\end{array} \]

(The last row can be computed directly or by using the regular representation.)

### 4.4 The main theorem

Let \( G \) be a finite group and \( F \) an algebraically closed field of characteristic zero. We know that

\[ F[G] = M_{d_1}(F) \times \cdots \times M_{d_k}(F) \]

for some \( d_1, \ldots, d_k \). We have idempotents \( e_i \) and simple modules \( M_i \), where \( M_i \) is the minimal left ideal in \( M_{d_i}(F) \). Given \( m \in M_i \), we have \( e_j m = m \) if \( j = i \) and \( e_j m = 0 \) if \( j \neq i \). If \( \chi_i \) is the character of the representation on \( M_i \), then \( \chi_i(a) = \mathrm{tr}(m \mapsto am) \), so in particular, \( \chi_i(ae_j) = \chi_i(a) \) if \( j = i \) and 0 otherwise.

Write \( e_i = \sum_g a_{i,g} g \in F[G] \). For \( g \in G \), we have \( \chi_{\mathrm{reg}}(g^{-1}e_i) = na_{i,g} \), where \( n = |G| \).

On the other hand, since \( \chi_{\mathrm{reg}} = \sum_i d_i \chi_i \), we get

\[ na_{i,g} = d_i \chi_i(g^{-1}) \]

after using the computation above, so

\[ e_i = \frac{d_i}{n} \sum_{g \in G} \chi_i(g^{-1}) g. \]

Write \( \mathrm{Ch}(G) \) for the vector space of functions \( G \to F \) which are constant on conjugacy classes. Then \( \dim \mathrm{Ch}(G) = k \) is the number of conjugacy classes, or equivalently the number of irreducible representations. Define \( B : \mathrm{Ch}(G) \times \mathrm{Ch}(G) \to F \) by

\[ (\chi, \eta) \mapsto B(\chi, \eta) = \langle \chi, \eta \rangle = \frac{1}{n} \sum_{g \in G} \chi(g^{-1}\eta)(g). \]

This is a bilinear form.
Proposition 4.4.1. The characters $\chi_1, \ldots, \chi_k$ form an orthonormal basis of $\text{Ch}(G)$ with respect to $B$.

Proof. We have

$$\langle \chi_i, \chi_j \rangle = d_i^{-1} \chi_j(e_i) = \delta_{ij}.$$

\[ \square \]

Theorem 4.4.2. Let $\rho_1, \ldots, \rho_k$ be the irreducible representations of a finite group $G$ over an algebraically closed field $F$ of characteristic zero, and let their characters be $\chi_1, \ldots, \chi_k$.

1. Every finite-dimensional representation $\rho$ is isomorphic to $\bigoplus_i \rho_i^{m_i}$, where $m_i = \langle \chi_\rho, \chi_i \rangle$.

2. Two representations $\rho$ and $\rho'$ are isomorphic if and only if $\chi_\rho = \chi_{\rho'}$.

3. A representation $\rho$ is irreducible if and only if $\langle \chi_\rho, \chi_\rho \rangle = 1$.

Example 4.4.3. 1. For $G = Q_8$, we can also see that the usual representation of dimension 2 is irreducible by computing $\langle \chi, \chi \rangle$.

2. If $G = S_n$, we have the standard representation on $F^n$ by permuting basis vectors. The kernel of the map $F^n \to F$ given by the sum of coordinates is an irreducible representation, so $F^n \cong V \oplus F$ as $G$-spaces, with the copy of $F$ being trivial.

4.5 Hurwitz’s theorem

We consider the question of when there exist $z_1, \ldots, z_n \in F[x_1, \ldots, x_n, y_1, \ldots, y_n]$ such that

$$\left( \sum_{i=1}^n x_i \right) \left( \sum_{j=1}^n y_j \right) = \sum_{k=1}^n z_k.$$}

Theorem 4.5.1 (Hurwitz). This can only happen for $n = 1, 2, 4, 8$.

Proof. If the $z_k$ exist, then they must be of the form

$$z_k = \sum_{i,j=1}^n a_{kij} x_i y_j.$$
Then
\[ \sum_{k=1}^{n} z_k^2 = \sum_{k=1}^{n} \left( \sum_{i,j} a_{kij} x_i y_j \right)^2 = \sum_{i,j,k=1}^{n} a_{kij}^2 x_i^2 y_j^2 + 2 \sum_{k=1}^{n} \sum_{i<j, j<j'} a_{kij} a_{kij'} x_i x'_i y_j y'_j. \]

We then require that
\[ \sum_{i,k=1}^{n} a_{kij}^2 x_i = \sum_{i=1}^{n} x_i^2, \quad \sum_{k=1}^{n} a_{kij} a_{kij'} = 0 \]
for all \( i \neq i' \) and \( j \neq j' \). If \( A \) is the matrix \( \sum_i a_{kij} x_i \), then writing \( A_i = (a_{kij})_{k,j} \), we require \( A_i^t A_i = I_n \) and \( A_i^t A_j + A_j^t A_i = 0 \) for \( i \neq j \). Letting \( B_i = A_i^t A_i \), we have \( B_i^t = -B_i \), and \( B_i^t B_j + B_j^t B_i = 0 \) when \( i \neq j \).

Consider the group \( G \) generated by \( a_1, \ldots, a_{n-1}, \varepsilon \) with relations \( a_i^2 = \varepsilon, a_i a_j = \varepsilon a_j a_i \) for \( i \neq j \), and \( \varepsilon^2 = 1 \). Then \( a_i \mapsto B_i \) and \( \varepsilon \mapsto -I_n \) is an \( n \)-dimensional representation of \( G \).

If \( n \) is odd, then \( Z(G) = \{1, \varepsilon\} \), and if \( n \) is even, then \( Z(G) = \{1, \varepsilon, a_1 \cdots a_{n-1}, \varepsilon a_1 \cdots a_{n-1}\} \). For \( g \in Z(G) \), the conjugacy class of \( g \) is \( C(g) = \{g, \varepsilon g\} \). Since \( |G| = 2^n \), the number of conjugacy classes is \( 2^{n-1} + 1 \) if \( n \) is odd and \( 2^{n-1} + 2 \) if \( n \) is even.

The commutator subgroup of \( G \) is \( \{1, \varepsilon\} \), so the number of one-dimensional representations is \( 2^{n-1} \). If \( n \) is odd, then the dimension of the last irreducible representation is \( 2^{(n-1)/2} \). If \( n \) is even, then (by descent / modular arithmetic), the dimensions of the other two irreducible representations are both \( 2^{n/2-1} \). If \( \rho \) is a 1-dimensional representation of \( G \), then \( \rho(\varepsilon) = 1 \), so the representation we constructed cannot have any 1-dimensional irreducibles in its decomposition. Hence \( n \) is a multiple of \( 2^{(n-1)/2} \) if \( n \) is odd and a multiple of \( 2^{n/2-1} \) if \( n \) is even. From this, we deduce that \( n \in \{1, 2, 4, 8\} \).

This proof also constructs the 8-dimensional Cayley algebra (or octonions).

### 4.6 More properties of representations

Let \( F \) be an algebraically closed field of characteristic zero.

**Proposition 4.6.1.** Let \( \chi \) be the character of a representation of a finite group \( G \) over \( F \) and let \( g \in G \). Then
1. $\chi(g)$ is an algebraic integer.

2. $|\chi(g)| \leq \dim \rho$.

3. $|\chi(g)| = \dim \rho$ if and only if $\rho(g)$ is a scalar matrix.

**Proof.**

1. Every eigenvalue of $\rho(g)$ is a root of unity, hence an algebraic integer, so their sum (with multiplicity) is an algebraic integer.

2. Every root of unity has magnitude 1, so the bound follows from the triangle inequality.

3. Equality holds if and only if the roots of unity in the sum are all positive real scalar multiples of each other, hence equal.

**Proposition 4.6.2.** Let $\chi$ be the character of an irreducible representation of dimension $d$ of a finite group $G$ over $F$, and let $g \in G$. Then $|C(g)|\chi(g)/d$ is an algebraic integer.

**Proof.** Let the corresponding matrix representation be $\rho : G \to GL_d(F)$, which extends to a homomorphism $F[G] \to M_d(F)$. We can then restrict to $Z(F[G]) \to \text{End}_G(F^d)$. By Schur’s lemma, $\text{End}_G(F^d) \cong F$, so anything in $Z(F[G])$ acts by scalar multiplication. In particular, $\alpha = \sum_{h \in C(g)} h$ maps to a scalar matrix $\lambda I_d$, so $\chi(\alpha) = |C(g)|\chi(g) = d\lambda$. Note that $\alpha \in Z(Z[G])$, which has a ring homomorphism to $F$ with $\lambda$ in its image. If $R$ is the image, then it is a subring of $F$ which is finitely generated as a $\mathbb{Z}$-module. Since it is a domain, it is a faithful $\mathbb{Z}[\lambda]$-module. Therefore, $\lambda$ is integral over $\mathbb{Z}$. \qed

**Theorem 4.6.3.** If $d$ is the dimension of an irreducible representation of a finite group $G$ over $F$, then $d \mid |G|$.

**Proof.** Let $n = |G|$ and $\chi$ be the character of an irreducible representation. Then if $C_1, \ldots, C_k$ are the conjugacy classes and $g_i \in C_i$ are representatives,

$$1 = \frac{1}{n} \sum_{g \in G} \chi(g^{-1})\chi(g) = \frac{1}{n} \sum_{i=1}^k |C_i|\chi(g_i^{-1})\chi(g_i),$$

so

$$\frac{n}{d} = \sum_{i=1}^k \frac{|C_i|\chi(g_i)}{d} \chi(g_i^{-1})$$

is an algebraic integer and a rational number, hence an integer. \qed
4.7 Tensor products

**Definition 4.7.1** (Bilinear map). Let $R$ be a ring, $M$ be a right $R$-module, $N$ be a left $R$-module, and $A$ be an abelian group, written additively. A bilinear map on $M \times N$ with values in $A$ is a map $B : M \times N \to A$ such that

(i) $B(m + m', n) = B(m, n) + B(m', n)$;

(ii) $B(m, n + n') = B(m, n) + B(m, n')$;

(iii) $B(mr, n) = B(m, rn)$.

The bilinear maps $M \times N \to A$ form an abelian group $\text{Bil}(M, N; A) = \text{Hom}_R(M, \text{Hom}_{\text{Ab}}(N, A))$, where the equality comes from noting that $\text{Hom}_{\text{Ab}}(N, A)$ has the structure of a right $R$-module.

For fixed $M, N$, this gives us a functor $\text{Ab} \to \text{Ab}$ by $A \mapsto \text{Bil}(M, N; A)$.

**Theorem 4.7.2.** The functor $A \mapsto \text{Bil}(M, N; A)$ is representable by an abelian group.

*Proof.* Let $F$ be the free abelian group with basis the symbols $m \otimes n$ for $m \in M$ and $n \in N$, then quotient by the subgroup generated by

$$(m + m') \otimes n - m \otimes n - m' \otimes n, \quad m \otimes (n + n') - m \otimes n - m \otimes n', \quad (mr) \otimes n - m \otimes (rn).$$

This gives an abelian group which represents the functor. \hfill $\Box$

**Definition 4.7.3** (Tensor product). The representing abelian group is the tensor product $M \otimes_R N$.

In particular, $\text{Bil}(M, N; M \otimes_R N) \cong \text{Hom}(M \otimes_R N, M \otimes_R N)$, so the identity map on $M \otimes_R N$ induces a “universal” bilinear map $B_{\text{uni}}(m, n) = m \otimes n$.

**Theorem 4.7.4** (Universal property of tensor products). For any bilinear map $B : M \times N \to A$, there is a unique abelian group homomorphism $f : M \otimes_R N \to A$ such that $f(m \otimes n) = B(m, n)$.

Let $g : M \to M'$ be a homomorphism of right $R$-modules and $h : N \to N'$ be a homomorphism of left $R$-modules. Then $B : M \times N \to M' \otimes_R N'$ given by $(m, n) \mapsto g(m) \otimes h(n)$ is a bilinear map, so there is a unique homomorphism $g \otimes h : M \otimes_R N \to M' \otimes_R N'$ such that $(g \otimes h)(m \otimes n) = g(m) \otimes h(n)$.

This shows that the tensor product is a functor $(\text{Mod-}R) \times (\text{R-Mod}) \to \text{Ab}$. 
Proposition 4.7.5. 1. $R \otimes_R N \cong N$ and $M \otimes_R R \cong M$.

2. $(\bigoplus_i M_i) \otimes_R N \cong \bigoplus_i (M_i \otimes_R N)$.

3. If $M$ is free with basis $\{m_i\}$, then every element of $M \otimes_R N$ can be written $\sum_i m_i \otimes n_i$ for unique $n_i \in N$, almost all zero.

If $M$ is both a right $R$-module and a left $S$-module such that $(sm)r = s(mr)$, then left multiplication by $S$ is an endomorphism $M \to M$ of right $R$-modules. Thus $m \otimes n \mapsto sm \otimes n$ gives a left $S$-module structure on $M \otimes_R N$. In particular, if $R$ is commutative, then we can take $S = R$, and so $M \otimes_R N$ has the structure of an $R$-module.

Supposing $R$ is commutative and $M, N$ are free $R$-modules, $M \otimes_R N$ is free, and if $\{m_i\}, \{n_j\}$ are bases, then $\{m_i \otimes n_j\}$ is a basis for $M \otimes_R N$. Thus $\text{rank}(M \otimes_R N) = \text{rank}(M) \cdot \text{rank}(N)$.

Suppose $M$ is a right $R$-module, $N$ is a left $R$-module and a right $S$-module with $(rm)s = r(ms)$, and $P$ is a left $S$-module. Then $(M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P)$, as they both represent the functor which sends an abelian group $A$ to trilinear maps $M \times N \times P \to A$.

If $R$ is commutative and $M, N$ are $R$-modules, then $M \otimes_R N \cong N \otimes_R M$.

Fix a right $R$-module $M$. The tensor product functor $R\text{-Mod} \to \text{Ab}$ sending $N$ to $M \otimes_R N$ is left exact.

4.8 Tensor products of representations

Let $\rho : G \to GL(V)$ and $\mu : H \to GL(W)$ be representations over a field $F$. Then $V \otimes_F W$ is a $(G \times H)$-space, or equivalently, we have a representation $\rho \otimes \mu : G \times H \to GL(V \otimes_F W)$. The corresponding character is $\chi_{\rho \otimes \mu}(g, h) = \chi_{\rho}(g) \chi_{\mu}(h)$. Moreover (assuming still that $F$ is algebraically closed of characteristic zero),

$$\langle \chi_{\rho_1 \otimes \mu_1}, \chi_{\rho_2 \otimes \mu_2} \rangle = \langle \chi_{\rho_1}, \chi_{\rho_2} \rangle \langle \chi_{\mu_1}, \chi_{\mu_2} \rangle.$$

Corollary 4.8.1. If $\rho$ and $\mu$ are irreducible, then $\rho \otimes \mu$ is irreducible.

Corollary 4.8.2. If $\rho_1, \ldots, \rho_k$ are the irreducible representations of $G$ and $\mu_1, \ldots, \mu_m$ are the irreducible representations of $H$, then $\rho_i \otimes \mu_j$ are the irreducible representations of $G \times H$.

If $G = H$, then we can restrict $\rho \otimes \mu$ to the diagonal $G \hookrightarrow G \times G$. However, the restriction may not be irreducible even if $\rho$ and $\mu$ are.
Theorem 4.8.3. Let $d$ be the dimension of an irreducible representation $\rho$ of a finite group $G$. Then $d \mid [G : Z]$.

Proof. Let $g \in Z$, so then $\rho(g)$ acts as a scalar. Let $\mu = \rho_{\otimes m} : G^m \to GL(W)$, where $W = V_{\otimes m}$. This is irreducible, so for $z_1, \ldots, z_m \in Z$, we have that $\mu(z_1, \ldots, z_m) = \prod \rho(z_i)$ acts as a scalar. Consider the central subgroup $H = \{(z_1, \ldots, z_m) \in Z^m \mid z_1 \cdots z_m = 1\} \leq G^m$ with $|H| = |Z|^{m-1}$. We have that $\mu(H) = 1$, so $\mu$ factors through $G^m/H \to GL(W)$ and is still irreducible. Hence $d^m = \dim W$ divides $|G^m/H| = |G|^m/|Z|^{m-1}$ for all $m$, so $d \mid [G : Z]$.

4.9 Burnside’s theorem

Lemma 4.9.1 (Homework C6 Problem 10). Let $\chi$ be the character of an irreducible representation of a finite group $G$ over $\mathbb{C}$ of dimension $d$. Let $C$ be a conjugacy class in $G$ such that $\gcd(|C|, d) = 1$. Then for every $g \in C$, either $\chi(g) = 0$ or $\rho(g)$ is a scalar matrix.

Proposition 4.9.2. Let $C$ be a conjugacy class of a finite group $G$ such that $|C| = p^a$ for some $p$ prime and $a > 0$. Then $G$ is not simple.

Proof. Let $\rho_1 = 1, \rho_2, \ldots, \rho_k$ be the irreducible representations of $G$ and $\chi_1, \ldots, \chi_k$ be the corresponding characters.

Suppose $p \nmid d_i = \dim \rho_i$ for some $i > 1$. Let $H = \{g \in G \mid \rho_i(g) \text{ is a scalar matrix}\} \leq G$. If $H = G$, then all matrices are scalar matrices, so $\rho_i(G)$ is abelian. Since $\rho_i \neq 1$, we have $\ker \rho_i \neq G$, but if $\ker \rho_i = 1$, then $G \cong \rho_i(G)$ is abelian, so $C$ cannot have size greater than 1, a contradiction. Therefore, $\ker \rho_i$ is a non-trivial proper normal subgroup of $G$, so $G$ is not simple.

If $H = 1$, then since $\gcd(|C|, d_i) = 1$, the lemma tells us that $\chi_i(g) = 0$ for all $g \in C$. Since $\chi_{\text{reg}} = \sum_i d_i \chi_i$, for $g \in C$, we get $-1/p = \sum_{i>1} (d_i/p) \chi_i(g)$ is an algebraic integer, since the only terms with $\chi_i(g) \neq 0$ have $p \mid d_i$. This is a contradiction, so $H$ must be a non-trivial proper normal subgroup of $G$.

Theorem 4.9.3 (Burnside’s $p^aq^b$-theorem). Let $p$ and $q$ be primes. Then every group of order $p^aq^b$ is solvable.

Proof. The theorem is already known if $a = 0$ or $b = 0$, so we can assume $a, b > 0$.
Let $Q \leq G$ be a Sylow $q$-subgroup, let $g \in Q$ be a non-trivial central element in $Q$, and let $H = Z_G(g) \leq G$. Then $Q \leq H$, so $|C(g)| = |G : H| \mid |G : Q| = p^a$. 

43
If $|C(g)| = 1$, then $g \in Z(G)$, so $Z(G) \leq G$ is non-trivial. If $Z(G) = G$, then $G$ is abelian and all abelian groups are solvable, and if $Z(G) \neq G$, then $G$ is not simple. If $|C(g)| > 1$, then by the proposition, $G$ is not simple.

In the cases where $G$ is not simple with non-trivial proper normal subgroup $H$, we obtain the result by induction applied to $H$ and $G/H$. 

\textbf{Theorem 4.9.4.} Let $|G| = pqr$ where $p, q, r$ are primes. Then $G$ is solvable.
5 Algebras

5.1 Definitions and basic properties

Let $R$ be a commutative ring.

**Definition 5.1.1** ($R$-algebra). An *$R$-algebra* is a ring $A$ such that $A$ has an $R$-module structure satisfying $r(xy) = (rx)y = x(ry)$.

If $A$ is an $R$-algebra, then there is a map $f : R \to A$ given by $r \mapsto r \cdot 1$.

**Proposition 5.1.2.** $f$ is a ring homomorphism with $f(R) \subset Z(A)$.

**Proposition 5.1.3.** Let $f : R \to A$ be a ring homomorphism with $\text{Im} f \subset Z(A)$. Then $A$ is an $R$-algebra with $r \cdot a = f(r)a$.

**Remark 5.1.4.** Let $A$ be an $R$-algebra. The product map $A \times A \to A$ is $R$-bilinear, and so we get a map $g : A \otimes_R A \to A$ with $g(x \otimes y) = xy$.

Conversely, if we have an $R$-module $A$ and an $R$-module homomorphism $g : A \otimes_R A \to A$, then we can define a product on $A$ by $xy = g(x \otimes y)$.

**Example 5.1.5.**

1. Every ring is a $\mathbb{Z}$-algebra.
2. Let $A$ be an $R$-algebra and $f : R \to A$ be the associated homomorphism. Then $A$ is an algebra over $R/ \text{Ker} f \hookrightarrow A$.
3. Every ring is an algebra over its center.
4. If $R \to S$ is a homomorphism of commutative rings and $A$ is an $S$-algebra, then $A$ can be given the structure of an $R$-algebra.
5. $R[x_1, \ldots, x_n]$ is an $R$-algebra.
6. If $M$ is an $R$-module, then $A = \text{End}_R(M)$ is an $R$-algebra.

**Definition 5.1.6** ($R$-algebra homomorphism). An *$R$-algebra homomorphism* is a ring homomorphism between two $R$-algebras that is simultaneously an $R$-module homomorphism.

**Proposition 5.1.7.** Let $A, B$ be $R$-algebras. Then $f : A \to B$ is an $R$-algebra homomorphism if and only if the following diagram of ring homomorphisms commutes.

$$
\begin{array}{ccc}
R & \xleftarrow{f} & B \\
\downarrow & & \downarrow \\
A & \xrightarrow{f} & B
\end{array}
$$
Denote by \( R\text{-Alg} \) the category of \( R \)-algebras whose morphisms are \( R \)-algebra homomorphisms. It has the subcategory \( R\text{-CAlg} \) of commutative algebras.

In \( R\text{-Alg} \), the Cartesian product coincides with the categorical product. In \( R\text{-CAlg} \), the tensor product \( A \otimes_R B \) coincides with the categorical coproduct of \( A \) and \( B \), where the multiplication on \( A \otimes_R B \) is given by \( (a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1a_2) \otimes (b_1b_2) \).

In \( R\text{-Alg} \) and \( R\text{-CAlg} \), the initial object is \( R \) and the terminal object is 0.

**Proposition 5.1.8.** Let \( A \) be an \( R \)-algebra and \( S \) be a commutative \( R \)-algebra. Then \( S \otimes_R A \) has the structure of an \( S \)-algebra.

This construction is referred to as extension of scalars.

Let \( f : A \rightarrow B \) be a homomorphism of \( R \)-algebras. Then \( 1_S \otimes f : S \otimes_R A \rightarrow S \otimes_R B \) is a homomorphism of \( S \)-algebras, so we have a functor \( R\text{-Alg} \rightarrow S\text{-Alg} \) given by \( A \mapsto S \otimes_R A \) and \( f \mapsto 1_S \otimes f \).

Given two \( R \)-algebras \( A, B \), we have

\[
(S \otimes_R A) \otimes_S (S \otimes_R B) = S \otimes_R (A \otimes_S S) \otimes_R B = S \otimes_R (A \otimes_R B),
\]

so the tensor product is respected by this functor.

### 5.2 Algebras over fields

Let \( F \) be a field. Then all short exact sequences are split, so the tensor product against a fixed vector space is an exact functor.

**Proposition 5.2.1.**

1. \( A \otimes_F M_n(F) \cong M_n(A) \) as \( F \)-algebras.

2. \( M_n(F) \otimes_F M_m(F) \cong M_{nm}(F) \).

Therefore,

\[
M_n(A) \otimes_F M_m(B) = M_n(F) \otimes_F A \otimes_F M_m(F) \otimes_F B = M_{nm}(A \otimes_F B).
\]

The canonical map \( F \rightarrow A \) is injective if \( A \neq 0 \), so we view \( F \) as a subalgebra of \( A \) with \( F \subset Z(A) \). Therefore, \( A \mapsto A \otimes_F B \) given by \( a \mapsto a \otimes 1_B \) is injective if \( B \neq 0 \).

**Proposition 5.2.2.** \( Z(A \otimes_F B) = Z(A) \otimes_F Z(B) \).
Proof. Let \( v \in Z(A \otimes_F B) \) and let \((a_i)\) be a basis for \( A \). Write \( v = \sum a_i \otimes b_i \) for unique \( b_i \in B \). Expanding \((1 \otimes b)v = v(1 \otimes b)\) gives us by uniqueness that \( b_ib = bb_i \) for all \( b \), so \( b_i \in Z(B) \). Therefore, \( v \in A \otimes Z(B) \). Let \((b_j)\) be a basis for \( Z(B) \), and write \( v = \sum a_j \otimes b_j \) for unique \( a_j \in A \). The same argument shows that \( a_j \in Z(A) \), so \( v \in Z(A) \otimes_F Z(B) \).

The other inclusion is clear. \( \square \)

**Corollary 5.2.3.** If both \( A \) and \( B \) are central \( F \)-algebras, then so is \( A \otimes_F B \).

**Example 5.2.4.** \( Z(M_n(A)) = Z(M_n(F) \otimes_F A) = Z(M_n(F)) \otimes_F Z(A) = F \otimes_F Z(A) \).

Recall that if \( A \) is an \( F \)-algebra and \( \dim_F A < \infty \), then the following are equivalent.

1. \( A \) is simple.
2. \( A \neq 0 \) is semisimple with unique simple \( A \)-module.
3. \( A \neq 0 \) and \( A \) has no non-trivial two-sided ideals.
4. \( A \cong M_n(D) \) for \( D \) a division \( F \)-algebra.

**Proposition 5.2.5.** Let \( f : A \to B \) be an \( F \)-algebra homomorphism. If \( A \) is simple and \( \dim_F A = \dim_F B \), then \( f \) is an isomorphism.

**Proof.** Let \( I = \ker f \subset A \). Then \( I = 0 \) or \( I = A \), but if \( I = A \), then \( B = 0 \), contradicting the dimension assumption. Hence \( I = 0 \), so \( f \) is an injective linear map, hence \( f \) is an isomorphism. \( \square \)

**Example 5.2.6.** Let \( L/F \) be a (finite) separable field extension and \( K/F \) be a field extension. Then \( L \) and \( K \) are simple \( F \)-algebras, and if \( L = F[x]/(f) \), then \( L \otimes_F K \cong K[x]/(f) \). If \( f = g_1 \cdots g_k \) with \( g_i \in K[x] \) irreducible (these are distinct by separability), then by the Chinese remainder theorem,

\[
L \otimes_F K \cong K[x]/(f) \cong \prod_{i=1}^k K[x]/(g_i) = \prod_{i=1}^k E_i,
\]

where \( E_i = K[x]/(g_i) \) is a finite separable extension of \( K \).

As a special case, if \( K \) is algebraically closed, then \( L \otimes_F K \cong K^{[L:F]} \).

**Proposition 5.2.7.** Let \( A \) and \( B \) be two simple \( F \)-algebras. If \( A \) is central, then \( A \otimes_F B \) is simple.
Proof. Let $I \subset A \otimes_F B$ be a non-zero two-sided ideal. Let $c \in I$ be non-zero and write $c = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ with $n$ as small as possible. Then $a_1 \neq 0$, so $Aa_1A = A$. Write $1 = y_1 a_1 z_1 + \cdots + y_m a_1 z_m$ for $y_j, z_j \in A$. We have that
\[
\sum_{j=1}^m (y_j \otimes 1_B) \cdot c \cdot (z_j \otimes 1_B) = \sum_{i,j} (y_j a_i z_j) \otimes b_i = \sum_{i=1}^n \left( \sum_{j=1}^m y_j a_i z_j \right) \otimes b_i = 1 \otimes b_1 + a_2' \otimes b_2 + \cdots + a_n' \otimes b_n
\]
is in $I$ and is non-zero. Hence we can suppose that $a_1 = 1$ in the original expression for $c$.

For $a \in A$, we have
\[
(a \otimes 1_B) c - c (a \otimes 1_B) = \sum_{i \geq 2} (aa_i - a_i a) \otimes b_i \in I.
\]
By minimality of $n$, this must be zero. Since the $b_i$ are linearly independent, $aa_i - a_i a = 0$ for all $i$ and for all $a \in A$. Hence $a_i \in Z(A) = F$ for all $i$, so $a_i \otimes b_i = 1 \otimes a_i b_i$ and $c = 1 \otimes b$ for some $b \neq 0$ in $B$.

Since $B$ is simple, $B b B = B$. Write $1 = \sum_k u_k b v_k$. Then
\[
\sum_k (1_A \otimes u_k) \cdot c \cdot (1_A \otimes v_k) = 1_A \otimes 1_B = 1_{A \otimes B} \in I.
\]

\[\square\]

Corollary 5.2.8. If $A$ and $B$ are central simple $F$-algebras, then so is $A \otimes_F B$.

5.3 The Brauer group

Let $F$ be a field, and consider the central simple $F$-algebras of finite dimension. These are of the form $M_n(D)$, where $D$ is a central division algebra of finite dimension over $F$. We say that $A \sim B$ if $M_k(A) \cong M_l(B)$ as $F$-algebras for some $k$ and $l$.

Proposition 5.3.1. This is an equivalence relation.

Proposition 5.3.2. Let $A_1 = M_{n_1}(D_1)$ and $A_2 = M_{n_2}(D_2)$ be two central simple $F$-algebras with $D_1, D_2$ division $F$-algebras. Then $A_1 \sim A_2$ if and only if $D_1 \cong D_2$.

Proof. If $A_1 \sim A_2$, then $M_{s_1}(A_1) \cong M_{s_2}(A_2)$, so $M_{s_1 n_1}(D_1) \cong M_{s_2 n_2}(D_2)$, hence $D_1 \cong D_2$.

Conversely, $M_{n_2}(A_1) \cong M_{n_1 n_2}(D_1) \cong M_{n_1 n_2}(D_2) \cong M_{n_2}(A_2)$, so $A_1 \sim A_2$. \[\square\]
Therefore, the class \([A]\) of \(A = M_n(D)\) is \(\{M_i(D)\}\) for \(i \geq 1\). In particular, \(D \in [A]\), so we have a correspondence between equivalence classes and central division \(F\)-algebras.

Write \(\text{Br}(F)\) for the set of equivalence classes with operation \([A][B] = [A \otimes_F B]\).

**Definition 5.3.3** (Brauer group). The abelian group \(\text{Br}(F)\) is the Brauer group of \(F\).

Note that \(\text{Br}(F) = 1\) if and only if every central division \(F\)-algebra of finite dimension is \(F\).

**Example 5.3.4.** If \(F\) is algebraically closed, then \(\text{Br}(F) = 1\).

**Theorem 5.3.5.** If \(F\) is a finite field, then \(\text{Br}(F) = 1\).

**Proof.** Let \(F = \mathbb{F}_q\) and let \(A\) be a division \(F\)-algebra of finite dimension. We show that \(A\) is commutative.

Suppose \(\text{dim}_F A = n\), so \(|A| = q^n\). Hence \(|A^\times| = q^n - 1\). For any \(a \in A\) non-zero, the centralizer \(C_A(a) \subseteq A\) is a subspace, so \(|C_A(a)| = q^k\) for some \(k\), hence \(|C_A^\times(a)| = q^k - 1\). Therefore, the conjugacy class of \(a\) in \(A^\times\) has \((q^n - 1)/(q^k - 1)\) elements. The elements of \(Z(A)^\times = F^\times\) have conjugacy classes of size 1, so there are exactly \(q - 1\) of them. The result then follows from the class equation and the fact that the cyclotomic polynomial \(\Phi_n(q)\) evaluated at \(q\) does not divide \(q - 1\) unless \(n = 1\).

**Example 5.3.6.** The quaternion algebra \(\mathbb{H}\) is a central \(\mathbb{R}\)-algebra of dimension 4, so \(\text{Br}(\mathbb{R}) \neq 1\).

Let \(F\) be a field with \(\text{char} F \neq 2\) and let \(a, b \in F^\times\). We can define a **generalized quaternion algebra** \((a, b)_F = F \cdot 1 \oplus F \cdot i \oplus F \cdot j \oplus F \cdot k\) by

\[
i^2 = a, \quad j^2 = b, \quad k = ij = -ji.
\]

This is a central simple \(F\)-algebra. We can write \((a, b)_F \cong M_n(D)\) with \(n^2 \dim_F D = 4\). If \(n = 1\), then \(D \cong (a, b)_F\) is a division algebra, or if \(n = 2\), then \((a, b)_F \cong M_2(F)\).

**Theorem 5.3.7** (Noether-Skolem). Let \(A\) be a finite-dimensional central simple algebra over \(F\) and let \(S, T \subseteq A\) be simple subalgebras. Let \(f : S \to T\) be an \(F\)-algebra isomorphism. Then there exists \(a \in A^\times\) such that \(f(s) = asa^{-1}\) for all \(s \in S\).
Proof. Regard $A$ as a right $(A^{op} \otimes_F S)$-module in two ways. First, we define $a \cdot (b^{op} \otimes s) = bas$. Second, we define $a \cdot (b^{op} \otimes s) = baf(s)$. Since $S$ is simple and $A^{op}$ is central simple, $A^{op} \otimes_F S$ is simple. Therefore, the two module structures are isomorphic.

Let $g : A \to A$ be an isomorphism, so that $g(bas) = bgaf(s)$ for all $a, b \in A$ and $s \in S$. For $a = s = 1$, we get $g(b) = bgf(1)$.

Remark 5.3.8. The condition that $A$ is central cannot be dropped. Otherwise, take $S = T = A$ to be a (non-trivial) Galois field extension of $F$. For $S = T = A$, we get $\text{Aut}(A) \cong A^×/F^×$ for the $F$-algebra automorphism group, with the action by conjugation. If $A = M_n(F)$, then $A^× = GL_n(F)$ and $\text{Aut}_F\text{-alg} = GL_n(F)/F^× = \text{PGL}_n(F)$.

Let $A$ be an $F$-algebra and let $S \subset A$ be a subalgebra. The centralizer of $S$ in $A$ is $C_A(S) = \{ a \in A \mid as = sa \text{ for all } s \in S \}$. This is a subalgebra of $A$.

Example 5.3.9. $C_A(F) = A$ and $C_A(A) = Z(A)$.

Lemma 5.3.10. Let $S \subset A$ and $T \subset B$ be two subalgebras. Then
\[ C_{A \otimes_F B}(S \otimes_F T) = C_A(S) \otimes_F C_B(T). \]

Proof. The same proof as for the special case of the tensor product of centers will work.

Corollary 5.3.11. $C_{A \otimes_F B}(A) = Z(A) \otimes_F B$ and $C_{A \otimes_F B}(B) = A \otimes_F Z(B)$.

Proof. Let $S = A$ and $T = F$.

Corollary 5.3.12. If $A$ and $B$ are central $F$-algebras, then $C_{A \otimes_F B}(A) = B$ and $C_{A \otimes_F B} = A$.

Example 5.3.13. Let $S$ be an $F$-algebra and $B = \text{End}_F(S)$. Then $S \subset B$ by left multiplication and $S^{op} \subset B$ by right multiplication. In fact, $S^{op} = C_B(S)$ and $S = C_B(S^{op})$.

Theorem 5.3.14 (Double centralizer theorem). Let $A$ be a central simple algebra over $F$ and let $S \subset A$ be a simple subalgebra.

1. $C_A(S)$ is simple with $Z(C_A(S)) = S \cap C_A(S) = Z(S)$.
2. \((\dim S)(\dim C_A(S)) = \dim A\).

3. \(C_A(C_A(S)) = S\).

Proof. 1. Let \(S \subset B = \text{End}_F(S)\). Then \(C_B(S) = S^{\text{op}}\). We have \(S \otimes_F A \subset A \otimes_F B\) and \(F \otimes_S \subset A \otimes_F B\). The first inclusion has \(C_{A \otimes B}(S \otimes F) = C_A(S) \otimes C_B(F) = C_A(S) \otimes B\), while the second inclusion has \(C_{A \otimes B}(F \otimes S) = C_A(F) \otimes C_B(S) = A \otimes S^{\text{op}}\), which is simple. By Noether-Skolem, \(S \otimes F\) and \(F \otimes B\) are conjugate, in particular isomorphic. Hence \(C_A(S) \otimes B \cong A \otimes S^{\text{op}}\) is simple. For the equalities, that \(Z(S) = S \cap C_A(S)\) is clear. By the third result, \(Z(C_A(S)) = C_A(S) \cap C_A(C_A(S)) = C_A(S) \cap S\).

2. We have \((\dim C_A(S))(\dim B) = (\dim A)(\dim S^{\text{op}})\), and the result follows from \(\dim B = (\dim S)^2\).

3. By the second result, \(\dim C_A(C_A(S)) = \dim S\) and \(S \subset C_A(C_A(S))\), so \(C_A(C_A(S)) = S\).

\[\square\]

Corollary 5.3.15. Let \(S\) be a central simple subalgebra of a central simple algebra \(A\). Then \(A = S \otimes_F C_A(S)\).

Proof. Consider the \(F\)-algebra homomorphism \(S \otimes_F C_A(S) \to A\) given by \(x \otimes y \mapsto xy\).  

\[\square\]

Let \(A\) be a central simple algebra over \(F\) and let \(L/F\) be a field extension. Then \(A_L = A \otimes_F L\) is a central simple \(L\)-algebra, as it is simple and \(Z(A \otimes_F L) = Z(A) \otimes_F Z(L) = F \otimes_F L = L\). Moreover, \(\dim_L A_L = \dim_F A\).

Suppose \(A \sim B\) over \(F\). Then \(M_n(A) \cong M_m(B)\) for some \(n\) and \(m\), so \(M_n(A)_L \cong M_m(B)_L\). Therefore, \(M_n(A_L) \cong M_m(B_L)\), so \(A_L \sim B_L\) over \(L\). Thus we have a group homomorphism \(\text{Br}(F) \to \text{Br}(L)\) given by extension of scalars \([A] \mapsto [A_L]\).

Proposition 5.3.16. If \(A\) is a central simple algebra over \(F\), then \(\dim_F A = n^2\) for some \(n\).

Proof. Let \(L\) be the algebraic closure of \(F\). Then \(A_L\) is a central simple algebra over \(L\), so \(A_L \cong M_n(L)\) for some \(n\). Then \(\dim_F A = \dim_L A_L = n^2\).  

\[\square\]
The value \( n \) is the degree of \( A \). Then \( \text{deg} M_k(A) = k \text{deg} A \).

Let \( A \) be a central simple algebra over \( F \) with \( A \cong M_k(D) \) for \( D \) some central division \( F \)-algebra. If \( m = \text{deg} D \) and \( n = \text{deg} A \), then \( n = km \). The value \( m \) is the index of \( A \), denoted \( \text{ind} A \). From the definition, \( \text{ind} A \mid \text{deg} A \), with equality if and only if \( A \) is a division algebra.

Suppose \( A \sim B \) with \( A = M_k(D) \) and \( B = M_l(d) \). Then \( \text{ind} A = \text{deg} D = \text{ind} B \), so we can define \( \text{ind}([A]) = \text{ind} A \). We have \([A] = 1\) if and only if \( \text{ind}([A]) = 1\).

**Example 5.3.17.** Let \( F \) be a field of characteristic zero and \( G \) be a finite group. Then \( F[G] \cong M_{d_1}(D_1) \times \cdots \times M_{d_r}(D_r) \) for division \( F \)-algebras \( D_1, \ldots, D_r \). Write \( Z_i = Z(D_i) \), \([Z_i : F] = m_i\), and \( \text{ind} D_i = s_i \). The simple \( F[G] \)-modules are then \( V_i = D_i^{d_i} \).

Let \( \rho : G \to GL(V) \) be a representation for \( V \) an \( F[G] \)-module. Let \( L \) be the algebraic closure of \( F \). Then \( V \otimes_F L \) is an \( L[G] \)-module. We have \( Z_i \otimes_L L = M_{s_i}(L) \) and \( D \otimes_{Z_i} L = M_{s_i}(L) \), so \( D_i \otimes_L L = D_i \otimes_{Z_i} (Z_i \otimes_L L) = (D \otimes_{Z_i} L)^{m_i} \).

Then \( M_{d_i}(D_i) \otimes_L L = M_{d_i}(L)^{m_i} \), so \( L[G] \cong \prod_i M_{d_i s_i}(L)^{m_i} \).

Take \( V = V_i = D_i^{d_i} \) and let \( \rho_{i_1}, \ldots, \rho_{i_m} \) be the irreducible representations of \( G \) over \( L \). Then \( \dim \rho_{i_j} = d_i s_i \) and \( V_i \otimes_L L \cong (M_{s_i}(L)^{d_i})^{m_i} \), so \( \dim M_{s_i}(L)^{d_i} = s_i^2 d_i \). If \( \rho_i : G \to GL(V_i) \) is the irreducible representation over \( F \), then

\[
\rho_i \otimes_F L \cong \bigoplus_{j=1}^{m_i} \rho_{i_j}^{s_i}.
\]

### 5.4 Maximal subfields

If \( A \) is a central simple algebra over \( F \), then \((\text{deg} A)^2 = \text{dim}_F A \). Writing \( A = M_s(D) \) for a central division \( F \)-algebra, the index of \( A \) is \( \text{ind} A = \text{deg} D \), so \( \text{deg} A = s \text{ ind} A \) and \( \text{deg} D = \text{ind} D \).

Let \( D \) be a central division algebra over \( F \) and let \( L \subset D \) be a subalgebra. Then \( L \) is a division subalgebra and \( L \) is a field extension of \( F \) if \( L \) is commutative. In the latter case, we will simply say that \( L \) is a subfield, with the containment of \( F \) understood.

**Proposition 5.4.1.** If \( L \subset D \) is a subfield, then \( L \) is maximal if and only if \( C_D(L) = L \).

**Proof.** \(( \implies \) Suppose \( \alpha \in C_D(L) \). Then \( L \subset L[\alpha] \subset D \) and \( L[\alpha] \) is a subfield of \( D \), so \( L[\alpha] = L \).
(⇐ ) Let \( L' \subset D \) be a subfield containing \( L \). Then \( L' \subset C_D(L) = L \), so \( L' = L \).

**Corollary 5.4.2.** Let \( L \) be a maximal subfield of a central division \( F \)-algebra \( D \). Then \([L : F] = \deg D \).

**Proof.** The double centralizer theorem gives \((\dim L)^2 = (\dim L)(\dim C_D(L)) = \dim D = (\deg D)^2\).

**Corollary 5.4.3.** Let \( L \) be a subfield of \( D \). Then \([L : F] \) divides \( \deg D \).

**Example 5.4.4.** Let \( D \) be a finite division ring. Then \( F = Z(D) \) is a finite field and \( D \) is central as an \( F \)-algebra. Let \( \alpha \in D^\times \) and let \( L \) be a maximal subfield of \( D \) containing \( F[\alpha] \). Then \([L : F] = \deg D \) is independent of \( \alpha \), so any two maximal subfields obtained in this way have the same degree over \( F \). As \( F \) is a finite field, these fields are isomorphic, hence conjugate by Noether-Skolem. It follows that \( D^\times = \bigcup_{\beta \in D^\times} \beta L^\times \beta^{-1} \), so since the groups are finite, \( L^\times = D^\times \). Hence \( L = D \). Computing dimensions, it follows that \( \deg D = 1 \).

Let \( A \) be a central simple algebra over \( F \) and let \( K/F \) be a field extension. Then \( A_K = A \otimes_F K \) is a central simple algebra over \( K \) and \( \deg_F A = \deg_K A_K \).

**Definition 5.4.5** (Splitting field). We say that \( K \) is a splitting field of \( A \) if \( A_K \cong M_n(K) \) for \( n = \deg A \).

Equivalently, \( A \) is split over \( K \) if \([A] \in \text{Ker}(\text{Br}(F) \to \text{Br}(K))\).

If \( K \) is an algebraic closure of \( F \), then \( \text{Br}(K) \) is trivial, so every central simple algebra is split over the algebraic closure.

**Remark 5.4.6.** If \( A \) is an \( F \)-algebra such that \( A_K = A \otimes_F K \cong M_n(K) \) for some \( n \), then \( A \) is a central simple algebra over \( F \) of degree \( n \). In fact, the central simple algebras over \( F \) are of this form for some \( K \). These are referred to as twisted forms of \( M_n(F) \), since \( A \otimes_F K \cong M_n(K) = M_n(F) \otimes_F K \).

**Proof.** Computing dimensions, \( \dim_F A = \dim_K A_K \). We have \( Z(A) \otimes_F K = Z(A \otimes_F K) = K = F \otimes_F K \) and \( F \subset Z(A) \), so computing dimensions, \( Z(A) = F \). Hence \( A \) is central. To see that \( A \) is simple, if \( I \subset A \) is a two-sided ideal, then \( I \otimes_F K \subset A \otimes_F K = M_n(K) \) is a two-sided ideal, so \( I \otimes_F K \) is 0 or \( A \otimes_F K \). Hence \( I \) is either 0 or \( A \).

**Theorem 5.4.7.** Let \( A \) be a central simple algebra over \( F \) with \( \deg A = n \). Let \( L \subset A \) be a subfield with \([L : F] = n \). Then \( L \) is a splitting field of \( A \).
Proof. Since $A \otimes_F L$ and $M_n(L)$ are central simple algebras of the same dimension, it suffices to find any homomorphism. Define $f : A \otimes_F L \to \text{End}_L(A) \cong M_n(L)$ with $A$ viewed as a right $L$-module by $f(a \otimes l)(m) = aml$.

**Corollary 5.4.8.** Every central simple algebra $A$ over $F$ has a splitting field $L$ such that $[L : F] = \text{ind } A$.

Proof. Write $A = M_s(D)$ for a central division algebra $D$ of degree $n = \text{ind } A$. Then a maximal subfield $L$ of $D$ is a splitting field for $D$, hence for $A$.

Let $D$ be a central division $F$-algebra and $\alpha \in D$. Then $F[\alpha] \subset D$ is a subfield, so $\alpha$ is algebraic over $F$.

**Lemma 5.4.9.** Let $D$ be a central division $F$-algebra with $D \neq F$. Then there exists $\alpha \in D \setminus F$ which is separable over $F$.

Proof. If $\text{char } F = 0$, then we are done. Otherwise, let $p = \text{char } F > 0$. Suppose all $\alpha \in D \setminus F$ are not separable. Pick $\alpha \in D \setminus F$. Then the maximal separable extension of $F$ contained in $F(\alpha)$ is $L$, so $L/F$ is purely inseparable. Therefore, $\alpha^{p^n} \in F$ for some $n$. Choose $n$ as small as possible and let $\beta = \alpha^{p^n-1}$, so $\beta^p \in F$. Define $f : D \to D$ by $f(a) = \beta a - a\beta$. Then $f \neq 0$ since $D$ is central and $D \neq F$, while $f^p(a) = \beta^p a - a\beta^p = 0$. Thus $f$ is nilpotent, so we can choose the smallest $k > 0$ with $f^k = 0$. Let $\gamma = f^{k-1}(\delta) \neq 0$ for some $\delta \in D$, so then $f(\gamma) = 0$. If $\varepsilon = f^{k-2}(\delta)$, then $\gamma = f(\varepsilon) = \beta \varepsilon - \varepsilon \beta$ and $\beta \gamma - \gamma \beta = 0$. Since $D$ is a division algebra, we can write $\gamma = \beta \zeta$ for some $\zeta \in D$. Then $\beta \zeta = \zeta \beta$, so

$$\beta = \beta \varepsilon \zeta^{-1} - \varepsilon \beta \zeta^{-1} = \beta \theta - \theta \beta$$

for $\theta = \varepsilon \zeta^{-1}$. Thus $1 + \beta^{-1} \theta \beta = \theta$, so $1 + \beta^{-1} \theta^{p^n} \beta = 1 + \theta^{p^n} = \theta^{p^n}$, a contradiction.

**Corollary 5.4.10.** Every central division $F$-algebra admits a maximal subfield which is separable over $F$.

Proof. Let $L \subset D$ be the maximal separable subfield extending $F$. Then $L \subset C_D(L)$, with equality if and only if $L$ is a maximal subfield of $D$. If $L \subsetneq C_D(L)$, then $C_D(L)$ is a central division $L$-algebra. By the lemma, there exists $\alpha \in C_D(L)$ such that $L(\alpha)/L$ is separable, but then $L(\alpha)/F$ is separable, contradicting maximality of $L$ as a separable extension.

**Corollary 5.4.11.** Every central simple $F$-algebra is split by a (finite) separable extension of $F$. 

54
Proof. Let $A$ be a central simple $F$-algebra and write $A = M_s(D)$ for $D$ a central division $F$-algebra. Let $L \subset D$ be a maximal subfield which is separable over $F$. Then $L$ is a splitting field for $D$, so also for $A$. \qed

Example 5.4.12. If $F$ is separably closed, i.e. it has no non-trivial separable extensions, then $\text{Br}(F) = 1$. One can construct the separable closure of a field by taking all separable elements in an algebraic closure.

Theorem 5.4.13. Let $A$ be a central simple $F$-algebra and $K/F$ be a finite field extension.

1. $\text{ind}(A_K) | \text{ind}(A)$ and $\text{ind}(A) | [K : F] \text{ind}(A_K)$.

2. If $A_K = M_s(D)$ for a central division $K$-algebra $D$, then $D \hookrightarrow M_p(A)$ for $p = [K : F] \text{ind}(A_K)/\text{ind}(A)$.

Proof. 1. Let $A = M_n(E)$ for a division algebra $E$, then $\text{ind}(A) = \deg(E)$. We have $A_K = M_n(E_K)$, so $\text{ind}(A_K) = \text{ind}(E_K) | \deg(E) = \text{ind}(A)$.

2. First suppose $A$ is a division algebra. Let $n = \deg A = \text{ind} A$ and write $A_K = M_s(D)$. If $m = \deg(D) = \text{ind}(D)$, then $n = sm$. Let $r = [K : F]$ and consider the embedding $K \hookrightarrow \text{End}_F(K) = M_r(F)$. Therefore, $A \hookrightarrow A_K \hookrightarrow M_r(A)$ (non-canonically). Let $C = C_{M_r(A)}(A)$. Since $A$ and $M_r(A)$ are central simple algebras, we have $A \otimes_F C \cong M_r(A) \cong A \otimes_F M_r(F)$. The fact that $A$ is simple then implies that $C \cong M_r(F)$. Since $K$ centralizes $A$, we have $K \subset C \cong M_r(F)$, so we have another embedding $A_K \hookrightarrow M_r(A)$ Hence $M_s(F) \subset M_s(D) \cong A_K \hookrightarrow M_r(A)$, so $M_s(B) \cong M_s(F) \otimes_F B \cong M_r(A)$ for $B = C_{M_r(A)}(M_s(F))$. The fact that $A$ is assumed a division algebra implies that $B \cong M_p(A)$ for $p$ as in the statement. Hence $n/m | r$, so $n | rm$, which is the required divisibility.

For the embedding, $D \subset M_s(D)$ commutes with $M_s(F)$, so $D \hookrightarrow B = M_p(A)$.

The general case follows from indices being Brauer invariant. \qed

Corollary 5.4.14. If a finite extension $K/F$ splits a central simple $F$-algebra $A$, then $\text{ind}(A) | [K : F]$.

Proof. The splitting implies that $\text{ind}(A_K) = 1$. \qed
Corollary 5.4.15. If $A$ is a central simple $F$-algebra of degree $r \text{ind}(A)$ and $K/F$ is a splitting field for $A$, then $K \hookrightarrow M_r(A)$. In particular, if $A$ is of degree $\text{ind}(A)$, then $K \hookrightarrow A$. If $A$ is a division algebra, then $K \cong M_r(A)$ for some $r > 0$. If $\text{char} F \neq 2$, then $A$ is a cyclic algebra.

Let $A$ be a division algebra of degree $\deg(A) = \text{ind}(A) = n$. If $K$ is a subfield of $A$, then $[K : F] | n$. On the other hand, if $K$ is a splitting field for $A$ which is finite over $F$, then $n | [K : F]$. The subfields which are splitting fields for $A$ are then the ones for which $[K : F] = n$, and hence maximal. Conversely, $A$ splits over any maximal subfield.

5.5 Cyclic algebras

Let $L/F$ be a cyclic field extension with Galois group $G = \text{Gal}(L/F)$ generated by $\sigma$. Let $n = [L : F]$ and $a \in F^\times$. The cyclic algebra $(L/F, \sigma, a)$ is the $F$-algebra given by

$$A = (L/F, \sigma, a) = \bigoplus_{i=0}^{n-1} Lu,$$

where $1, u, \ldots, u^{n-1}$ is a basis for $L/F$. The multiplication is defined by $u^n = a \cdot 1$ and extending the relations $(xu^i)(yu^j) = x\sigma^i(y)u^{i+j}$ for $x, y \in L$. In particular, $uyu^{-1} = \sigma(y)$.

Example 5.5.1. 1. Suppose $\text{char} F \neq 2$. Let $L = F(\sqrt{b}) = F[j]/(j^2 - b)$ for $b$ not a square. Then for $a \in F^\times$, we have

$$(L/F, \sigma, a) = (L \cdot 1) \oplus (L \cdot i) = (F \cdot 1) \oplus (F \cdot i) \oplus (F \cdot j) \oplus (F \cdot ij)$$

with $i^2 = a, j^2 = b, ij = -ji$. Hence $(L/F, \sigma, a) = (a, b)_F$ is the generalized quaternion algebra. The usual quaternions are $\mathbb{H} = (\mathbb{C}/\mathbb{R}, \text{conjugation}, -1)$.

2. If $\text{char} F = 2$, then polynomials $x^2 + x + a$ for $a \in F$ are separable. Let $L = F(\theta)$ for $\theta$ a root of $x^2 + x + a$ (assumed irreducible). Then $\sigma(\theta) = \theta + 1$, so $(L/F, \sigma, a)$ has basis $\{1, \theta, u, \theta u\}$ with relations $\theta^2 + \theta + a = 0, u^2 = a, u\theta = (\theta + 1)u$.

Proposition 5.5.2. $A = (L/F, \sigma, a)$ is a central simple algebra.

Proof. Suppose $s = \sum_i \alpha_i u^i \in Z(A)$ and let $\beta \in L$. Then $0 = \beta s - s\beta = \sum_i (\beta \alpha_i - \alpha_i \sigma^i(\beta))u^i$. If $i \neq 0$, then we can choose $\beta$ so that $\sigma^i(\beta) \neq \beta$, so then $\alpha_i = 0$. Hence
The degree of $M$ to know that $\deg(M)$ is a central simple algebra of degree $n$ over $F$. In particular, $L/F$ is a splitting field for $A$, so $[A] = \ker(\text{Br}(F) \to \text{Br}(L)) = \text{Br}(L/F)$ (the relative Brauer group). If $A$ is a division algebra, then $L$ is also a maximal subfield of $A$.

Hence $A$ is a central simple algebra of dimension $n^2$ containing $L$ as a subfield of dimension $n$ over $F$. It can be shown that $C(L/F, \sigma, a)$ and $C(L/F, \sigma^i, a^i)$ are isomorphic for $i$ coprime to $n$.

**Lemma 5.5.3.** Let $L/F$ be a cyclic field extension of degree $n$ and let $A$ be a central simple algebra of degree $n$ over $F$. If $L \hookrightarrow A$, then $A \cong C(L/F, \sigma, a)$ for some $\sigma$ generating $G = \text{Gal}(L/F)$ and $a \in F^\times$.

**Proof.** By Noether-Skolem, $\sigma : L \to L$ extends to an inner automorphism $\sigma(\alpha) = \beta \alpha \beta^{-1}$ for some $\beta \in A^\times$ and all $\alpha \in L$. Then $\alpha = \sigma^n(\alpha)$ shows that $\beta^n \in C_A(L) = L$. Since $\beta^n = \sigma(\beta^n)$, in fact $\beta^n \in F$. Take $a = \beta^n$, then define a map $C(L/F, \sigma, a) \to A$ by $\alpha \in L \mapsto \alpha \in L \subset A$ and $u \mapsto \beta$. It is easily checked that this is well-defined and a map of central simple algebras of the same dimension, hence an isomorphism. $\square$

**Proposition 5.5.4.** Let $L/F$ be a cyclic extension. Then $\text{Br}(L/F) = \{ [C(L/F, \sigma, a)] \mid a \in F^\times \}$.

**Proof.** Let $[A] \in \text{Br}(L/F)$ for $A$ a division algebra. Then $\deg(A) = \text{ind}(A) = m$. We know that $n = [L : F]$ is divisible by $m$, so $n = mk$ for some $k$ and $L \hookrightarrow M_k(A)$. The degree of $M_k(A)$ is $km = n$, so there is a cyclic algebra $C(L/F, \sigma, a)$ isomorphic to $M_k(A)$. $\square$

**Lemma 5.5.5.** $C(L/F, \sigma, 1) \cong M_n(F)$ for $n = [L : F]$.

**Proof.** Define an $F$-algebra isomorphism $C(L/F, \sigma, 1) \to \text{End}_F(L) = M_n(F)$ by $\alpha \in L \mapsto \alpha \in \text{End}_F(L)$ and $1 \mapsto \sigma$. $\square$

**Lemma 5.5.6.** Let $L/F$ be a cyclic extension of degree $n$, $\sigma \in \text{Gal}(L/F)$ be a generator, and $a, b \in F^\times$. Then $C(L/F, \sigma, a) \cong C(L/F, \sigma, b)$ if and only if $b/a \in N_{L/F}(L^\times)$.  

57
Proof. (\(\implies\)) Let \(f : C(L/F, \sigma, a) \to C(L/F, \sigma, b)\) be an isomorphism. Then \(f(L)\) and \(L\) are isomorphic subfields of \(C(L/F, \sigma, b)\), so by Noether-Skolem, we can modify \(f\) by conjugation to suppose \(f\) fixes \(L\). If \(u\) generates \(C(L/F, \sigma, a)\) and \(v\) generates \(C(L/F, \sigma, b)\), then \(f(u)\) and \(v\) act by conjugation in the same way on \(L \subset C(L/F, \sigma, b)\). Hence \(f(u)v^{-1}\) is in the centralizer of \(L\), which is \(L\) itself, so \(f(u) = \alpha^{-1}v\) for some \(\alpha \in L^\times\). It follows by computation that \(b = aN_{L/F}(\alpha)\).

(\(\Longleftrightarrow\)) Suppose \(b = aN_{L/F}(\alpha)\) for some \(\alpha \in L^\times\). Let \(u\) be a generator of \(C(L/F, \sigma, a)\) and \(v\) be a generator of \(C(L/F, \sigma, b)\). We can then define a homomorphism \(C(L/F, \sigma, a) \to C(L/F, \sigma, b)\) by fixing \(L^\times\) and mapping \(u \mapsto \alpha^{-1}v\). Since the two algebras are central simple algebras, the homomorphism is automatically an isomorphism.

\[\tag*{\text{Corollary 5.5.7.}} [C(L/F, \sigma, a)] = 1 \text{ if and only if } a \in N_{L/F}(L^\times).\]

\[\tag*{\text{Example 5.5.8.}} \text{Let } F = \mathbb{F}_q \text{ be a finite field. We have } Br(F) = \bigcup_{L/F} Br(L/F) \text{ with } L/F \text{ ranging over all finite extensions. Since } F \text{ is finite, } L/F \text{ is cyclic and } N_{L/F} : L^\times \to F^\times \text{ is surjective, so } Br(L/F) = 1.\]

Let \(L/F\) be cyclic and \(\sigma \in \text{Gal}(L/F)\) be a generator. Define \(f : F^\times \to Br(L/K)\) given by \(a \mapsto [C(L/F, \sigma, a)]\).

\[\tag*{\text{Theorem 5.5.9.}} \text{\(f\) is a surjective homomorphism and } \text{Ker } f = N_{L/F}(L^\times).\]

Consider \(p : L \otimes_F L \to L^n\) by \(p(x \otimes y) = (xy, x\sigma(y), \ldots, x\sigma^{n-1}y)\).

\[\tag*{\text{Proposition 5.5.10.}} \text{\(p\) is an } F\text{-algebra isomorphism.}\]

Proof. Write \(L = F(a) = F[t]/(f)\) with \(f(t) = (t - \alpha) \cdots (t - \sigma^{n-1}(\alpha)) \in L[t]\). Then \(L \otimes_F L = L[t]/(f)\) and the map \(p\) takes \(g \in L[t]/(f)\) to \((g(\alpha), \ldots, g(\sigma^{n-1}(\alpha)))\). This is an isomorphism by the Chinese remainder theorem.

If \(G = \text{Gal}(L/F)\), then \(G\) acts on \(L \otimes_F L\) by \(\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y)\). If \(G\) acts on \(L^n\) component-wise, then \(p\) respects the action of \(G\), so \((L \otimes_F L)^G \cong F^n.\)

\[\tag*{\text{Lemma 5.5.11.}} \text{Let } A \text{ be a central simple algebra of degree } n \text{ over } F. \text{ If } F^n \hookrightarrow A \text{ as a subalgebra, then } A \cong M_n(F).\]

Proof. We have \(A \cong \text{End}_D(V) \cong M_k(D)\) for some central division \(F\)-algebra \(D\) and \(V\) a \(D\)-module of rank \(k\). Let \(e_1, \ldots, e_n \in F^n\) be orthogonal idempotents. Then \(V = e_1(V) \oplus \cdots \oplus e_n(V)\) gives \(\text{rank}_D(V) \geq n\). On the other hand, if \(\deg(D) = m\), then \(n = km\), so \(\text{rank}_D(V) = k = n/m \geq n\), so \(m = 1\) and \(k = n\), so \(D = F.\)
Proposition 5.5.12. \([C(L/F,\sigma,a)][C(L/F,\sigma,b)] = [C(L/F,\sigma,ab)].\)

Proof. It suffices to show that \(C(L/F,\sigma,a) \otimes_F C(L/F,\sigma,b) \cong M_n(C(L/F,\sigma,ab)).\) To do this, we find an embedding of \(C(L/F,\sigma,ab)\) into the tensor product with centralizer \(M_n(F)\). Let \(A = C(L/F,\sigma,a) = \bigoplus L u_i\) and \(B = C(L/F,\sigma,b) = \bigoplus L v_i\). Then \(A \otimes_F B = \bigoplus (L \otimes_F L)(u^i \otimes v^i)\). If \(D = C(L/F,\sigma,ab) = \bigoplus L w_i\), then \(D \cong \bigoplus (L \otimes_F F)(u^i \otimes v^i)\) by \(u \otimes v \mapsto w\), which embeds in \(A \otimes_F B\). The centralizer of \(D\) contains \((L \otimes_F L)^G = F^n\), so the centralizer of \(D\) is \(M_n(F)\). \(\square\)