Contents

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 $M_n = M_{n+1} = \ldots$. □

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: $2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq \ldots$.

Proposition 1.1.5. *Let M be a (left) R-module and $N \subset N$ a submodule. Then M is noetherian (artinian) if and only if N and M/N are noetherian (artinian).*

Proof (noetherian case). ($\Longrightarrow$) Let $N_1 \subset N_2 \subset \cdots$ be submodules of N and hence of M. The sequence is stable since M is noetherian. Hence N is noetherian.

Let $f : M \to M/N$ be the natural surjection and let $P_1 \subset P_2 \subset \cdots$ be submodules of M/N. 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 M/N is noetherian.

($\Longleftarrow$) 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. $M_2 \simeq (M_1 \oplus M_2)/M_1$. Induct on n. □

Proposition 1.1.7. *Let $f : R \to S$ 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 $(\operatorname{Ker} f)M' = 0$, so M' can be realized as a module over $R/\operatorname{Ker} f \cong S$. Hence every R-submodule of M is also an S-submodule. □

Corollary 1.1.8. *Let $f : R \to S$ be a surjective ring homomorphism. If R is (left) noetherian (artinian), then S is noetherian (artinian).*

Proof. Since $S \cong R/\operatorname{Ker} f$, we have a short exact sequence $0 \to \operatorname{Ker} f \to R \to S \to 0$ 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 surjective homomorphism $0R^n \to M$ for some n. Since $R^n = R \oplus \cdots \oplus R$ is noetherian (artinian), so is M. □

Below we prove some properties of noetherian ring and modules.

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 $m_{i+1} \notin M_i = \operatorname{span}(m_1, \ldots, m_i)$. 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 $R[x_1, \ldots, x_n]$.*

Proof. It suffices to show that if R is left 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

$$M = R + Rx + Rx^2 + \cdots + Rx^{k-1} \subset R[x]$$

is the R-submodule of polynomials of degree $< k$, then M is finitely generated. As R is left noetherian, $I \cap M \subset M$ is a finitely generated R-module. Let $g_1, \ldots, g_m$ be the generators of $I \cap M$. We claim that $f_1, \ldots, f_s; g_1, \ldots, g_m$ generate I. Let I' be the left ideal in $R[x]$ generated by these polynomials. We show that $I = I'$. Clearly, $I' \subset I$.

To see that $I \subset I'$, we pick a polynomial $h \in I$ and prove by induction on $n = \deg h$ that $h \in I'$. If $\deg h < k$, then h is in the R-span of $g_1, \ldots, g_m$, so $h \in I'$. Otherwise, let $a \in R$ be the leading coefficient of h. Write a in the form $a = b_1 a_1 + \cdots + b_s a_s$ for some $b_1, \ldots, b_s \in R$ and consider the polynomial

$$h' = b_1 x^{n-k_1} f_1 + \cdots + b_s x^{n-k_s} f_s \in I'.$$

The polynomials h and h' have the same degree and the leading coefficients. Then $h - h' \in I$ has smaller degree, so $h - h' \in I'$ by the inductive hypothesis. Hence $h \in I'$. □

Let R be a subring of a commutative ring S. We say that the ring S is finitely generated over R if 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.

We can also view S as a module over R. If S is finitely generated as an R-module, then the ring S is finitely generated over R, but not conversely.

Corollary 1.1.14. *Let R be a subring of a commutative ring S. If the ring S is finitely generated over R and R is noetherian, then so is S.*

Proof. Let S be generated over R 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. □

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, the ring T is finitely generated over R, and T is finitely generated as an S-module. Then the ring S is finitely generated over R.*

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

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

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

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

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

We claim that $T = S_0 b_1 + \cdots + S_0 b_m$. To see this, we have

$$T = R[a_1, \dots, a_n] = S_0[b_1, \dots, b_m] = S_0 b_1 + \cdots + S_0 b_m,$$

where the last step follows from expressing quadratic monomials in terms of linear monomials with the coefficients β_{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, the ring S is finitely generated over R. □

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

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

In general, let $E = F[f_1, \dots, f_m]$ with $\{f_1, \dots, f_k\}$ be a maximal algebraically independent subset for some $k \leq m$. Then every element in E is algebraic over the field $F(f_1, \dots, f_k)$. As E finitely generated as a field over F, hence over $F(f_1, \dots, f_k)$, the field extension $E/F(f_1, \dots, f_k)$ is finite.

Note that $E_0 = F(f_1, \dots, f_k) \cong F(x_1, \dots, x_k)$ is the rational function field over F. Since E is finitely generated over F as a ring and E is finitely generated over E_0 as a module, by the lemma, E_0 is finitely generated over F as a ring. By the claim, $E_0 = F$, so E/F is a finite field extension. □

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

Theorem 1.2.3 (Hilbert Nullstellensatz, weak form)**.** *Let F be algebraically closed and $f_1, \dots, f_m \in F[x_1, \dots, x_n]$. TFAE:*

(1) *There is no $a \in F^n$ such that $f_i(a) = 0$ for all i.*

(2) *The polynomials $f_1, \dots, f_m$ generate the unit ideal in $F[x_1, \dots, x_n]$.*

Proof. (2) $\Rightarrow$ (1) Choose $g_1, \dots, g_m$ 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.

(1) $\Rightarrow$ (2) Let $I = (f_1, \dots, f_m)$ and suppose $I \neq F[x_1, \dots, x_n]$. Then I is contained in a maximal ideal M. The factor ring $F[x_1, \dots, x_n]/M$ is a field extension of F that is finitely generated over F as a ring. By the proposition, this field extension if finite, and hence it is trivial since F is algebraically closed. Let $a_i \in F$ be the pre-image of $x_i + M$ under the isomorphism $F \to F[x_1, \dots, x_n]/M$. Let $a := (a_1, \dots, a_n) \in F^n$. Since the image of $f_j(a)$ is $f_j(x) + M = M$ is trivial, we have $f_j(a) = 0$ in F for all j. $\square$

Remark 1.2.4. The statement of the weak form of HN is false if F is not algebraically closed. For example, take $F = \mathbb{R}$, $n = m = 1$, $f_1 = x^2 + 1$.

For any $a \in F^n$ consider a map $\varphi_a : F[x] = F[x_1, \dots, x_n] \to F$ taking a polynomial f to $f(a)$. Clearly, φ_a is a surjective the ring homomorphism. Set $M_a := \mathrm{Ker}(\varphi_a)$. Since $F[x]/M_a \simeq F$, M_a is a maximal ideal in $F[x]$.

Corollary 1.2.5. *Let F be algebraically closed. Then every maximal ideal of $F[x_1, \dots, x_n]$ is equal to M_a for a unique $a \in F^n$.*

Proof. Let $M \subset F[x_1, \dots, x_n]$ be a maximal ideal and $\{f_1, f_2, \dots f_m\}$ a set of generators of M. By the weak form of HN there is $a \in F^n$ such that $f_i(a) = 0$ for all i. Therefore, $M \subset M_a$ and since M is maximal, we have $M = M_a$. $\square$

Theorem 1.2.6 (Hilbert Nullstellensatz, strong form)**.** *Let F be algebraically closed and consider $f_1, \dots, f_m, g \in F[x_1, \dots, x_n]$. TFAE:*

(1) *Whenever $f_i(a) = 0$ for all i, we also have $g(a) = 0$.*

(2) *$g^k \in (f_1, \dots, f_m)$ for some k.*

Proof. (2) $\Rightarrow$ (1) Choose $g_1, \dots, g_m$ such that $f_1g_1 + \cdots + f_mg_m = g^k$ for some k. If $f_i(a) = 0$ for all i, we have $g(a)^k = 0$, hence $g(a) = 0$.

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

2 Dedekind Rings

Throughout, all rings are commutative.

2.1 Definitions and basic properties

Let R be an integral domain and A and B be two ideals of R. Denote by AB the set of all finite sums of the form $\sum a_i b_i$, where $a_i \in A$ and $b_i \in B$. Then AB is an ideal called the *product* of A and B. The product is commutative and associative.

Clearly $AB \subset A$ and $AB \subset B$. If $A = aR$ and $B = bR$ are principal ideals, the so is $AB = abR$.

Definition 2.1.1 (Divisibility of ideals)**.** Let $A, B \subset R$ be ideals with $B \neq 0$. We say that A is *divisible* by B (or B *divides* A) if there is an ideal $C \subset R$ such that $A = BC$. We write $B|A$.

If $B|A$, then $A \subset B$. The converse holds for principal ideals: if $aR \subset bR$ then b divides a, i.e., $a = bc$ for some $c \in R$ and hence $aR = (bR)(cR)$, i.e., $bR \mid aR$. But the converse does not hold in general.

Example 2.1.2. Let F be a field, $R = F[x, y]$, $A = xR$ and $B = xR + yR$. We claim that B does not divide A. Suppose the opposite: $A = BC$ for some ideal C. For any $c \in C$ we have $yc \in BC = A = xR$, i.e., x divides yc, hence x divides c. It follows that $C \subset xR$. We have $xR = A = BC \subset BxR = xB$, hence $R \subset B$, a contradiction.

Definition 2.1.3 (Dedekind domain)**.** An integral domain R is a *Dedekind domain* if for any two ideals $A \subset B \neq 0$, we have that B divides 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 $a \in A$ be non-zero, so then $aR \subset A$. 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 $A \subset R$ be an ideal. If $A = 0$, then we are done. Otherwise, let $a \in A$ be non-zero, so then $aR = AB$ for some ideal $B \subset R$. Write $a = x_1y_1 + \cdots + x_ny_n$ for $x_i \in A$ and $y_i \in B$. Define $f : R^n \to A$ by $f(r_1, \ldots, r_n) = r_1x_1 + \cdots + r_nx_n \in A$ and $g : A \to R^n$ by $g(z) = (zy_i/a)_i \in R^n$. Then $f \circ g = \mathrm{id}_A$, 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 $P_0 \subsetneq \cdots \subsetneq P_n$ in R.

Example 2.1.10. 1. $\dim F = 0$ for any field F.

2. $\dim \mathbb{Z} = 1$.

Proposition 2.1.11. *Let R be a domain. Then $\dim R \le 1$ if and only if every non-zero prime ideal is maximal.*

Theorem 2.1.12. *If R is a Dedekind domain, then $\dim R \le 1$.*

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 $A \subsetneq R$ 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 $\mathcal{A}$ be the set of all non-zero proper ideals that have no such factorization. If $\mathcal{A}$ is non-empty, then since R is noetherian, $\mathcal{A}$ 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 $A \ne B$. By maximality of $A \in \mathcal{A}$, 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 $\dim R \le 1$, 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

$$P_1 = (2, 1+\sqrt{-5}), \qquad P_2 = (3, 1+\sqrt{-5}), \qquad P_3 = (3, 1-\sqrt{-5}).$$

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

$$(2) = P_1^2, \qquad (3) = P_2 P_3, \qquad (1+\sqrt{-5}) = P_1 P_2, \qquad (1-\sqrt{-5}) = P_1 P_3.$$

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 $R \to \operatorname{End} M$ 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) α 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 $1, x, \dots, x^{n-1}$.

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

(3) $\implies$ (1) Suppose M is generated by $m_1, \dots, m_n$ 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 $X = (m_1, m_2, \dots, m_n)^t$. Multiplying through by $\operatorname{adj}(\alpha I - A)$, 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 α, so α is integral over R. □

Corollary 2.2.5. *Let $R \subset S$ be rings such that S is a finitely generated R-module. Then every $\alpha \in S$ is integral over R.*

Proof. Let $\alpha \in S$. Then S is a faithful $R[\alpha]$-module and hence s is integral over R. □

Corollary 2.2.6. *Let $R \subset S$ be rings and $\alpha_1, \dots, \alpha_n \in S$ be integral over R. Then $R[\alpha_1, \dots, \alpha_n]$ is finitely generated as an R-module.*

Corollary 2.2.7. *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. By the corollary, any $\gamma \in R[\alpha, \beta]$ is integral over R. In particular, $\alpha + \beta$ and $\alpha\beta$ are integral over R. □

Definition 2.2.8 (Integral closure)**.** Let $R \subset S$ be rings. The ring of elements of S which are integral over R is the *integral closure* of R in S.

If the integral closure of R in S is S, we say that S is *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 *integrally closed* in S.

Definition 2.2.9 (Normal ring)**.** Let R be a domain and F be its quotient field. We say that R is *normal* (or *integrally closed*) if R is integrally closed in F.

Example 2.2.10. 1) Every UFD is normal.
2) The ring $R = \mathbb{Z}[\sqrt{5}]$ is not normal. The element $\alpha = (1 + \sqrt{5})/2$ is in the quotient field of R but not in R. It is a root of $x^2 - x - 1$, hence α is integral over R.

Proposition 2.2.11. *Let $R \subset S \subset T$ be rings with S/R integral. If $\alpha \in T$ is integral over S, then α is integral over R.*

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

Corollary 2.2.12. *Let $R \subset S \subset T$ be rings with S/R integral. If T/S is integral, then T/R is integral.*

Corollary 2.2.13. *Let S^{int} be the integral closure of R in S. Then S^{int} is integrally closed in S.*

Example 2.2.14. 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 $\alpha^n + \beta_i \alpha^{n-1} + \cdots + \beta_n = 0$ 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 2.2.15. *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 α is integral over R if and only if the minimal polynomial of α in $F[x]$ is in fact contained in $R[x]$.*

Proof. If the minimal polynomial m of α is contained in $R[x]$, then α is integral over R as m is monic. Conversely, if α 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. $\square$

Theorem 2.2.16. *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, $aA = bAB$ for some ideal $B \subset R$. Then $aR = bB$, so $\alpha \in (a/b)R \subset B \subset R$. $\square$

Lemma 2.2.17. *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 α is integral over R, i.e. $\alpha \in R$. $\square$

Theorem 2.2.18. *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 2.2.19. *Let $A \subsetneq R$ 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,

$$A \subsetneq A + aR \supset P_1 \cdots P_n,$$
$$A \subsetneq A + bR \supset Q_1 \cdots Q_m,$$

but then

$$A \supset (A + aR)(A + bR) \supset P_1 \cdots P_n Q_1 \cdots Q_m. \qquad \square$$

Lemma 2.2.20. *Let $B \subsetneq R$ be a nonzero ideal. Let F be the quotient field of R. Then there exists $\alpha \in F \backslash R$ with $\alpha B \subset R$.*

Proof. Let $b \in B$ be non-zero. By lemma, there exist primes such that $P_1 \cdots P_k \subset bR$; choose these primes so that k is as small as possible. Let P be a prime ideal containing B. Then $P_i \subset P$ for some i, wlog $i = 1$, so since $\dim(R) \leq 1$, $P_1 = P$. By minimality of k, we have $P_2 \cdots P_k \not\subset bR$, so there exists $c \in P_2 \cdots P_k$ with $c \notin bR$. Then $cB \subset cP = cP_1 \subset P_1 \cdots P_k \subset bR$, so we can choose $\alpha = c/b$. $\square$

Now suppose that $A \subset B$ are ideals with $B \neq 0$. To show that $A = BC$ for some ideal C, we use noetherian induction on B. We may assume that $A \neq 0$.

If $B = R$, then take $C = A$, so assume that $B \neq R$. Let $\alpha \in F \backslash R$ be as in the second lemma. Since $\alpha \notin R$, we have $\alpha B \not\subset B$ (since R is normal), but $\alpha B \subset R$. Letting $B' = B + \alpha B$, we have $A \subset B \subsetneq B' \subset R$, so by induction, there exists C' such that $A = B'C'$. Let $C = (R + \alpha R)C' \subset F$. Then

$$BC = B(R + \alpha R)C' = B'C' = A.$$

To see that $C \subset R$, let $c \in C$. Then $cB \subset B'C' = A \subset B$, so $c \in R$ as R is normal. $\square$

Theorem 2.2.21. *Let 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 R in K, then S is a Dedekind domain.*

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

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

Let $\alpha_1, \ldots, \alpha_n \in K$ be a basis over F. From the proof that K is the quotient field of S, there exists $a \in R$ non-zero such that $b_i = a\alpha_i \in S$. Let $f : K \to F^n$ be given by $f(x)_i = \mathrm{tr}(xb_i)$. 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 tr is non-zero as a function, there exists $\beta \in K$ such that $\mathrm{tr}\,\beta \neq 0$. Write $\beta/\alpha = \sum \gamma_i b_i$ for $\gamma_i \in F$. Then $\beta = \sum \gamma_i \alpha b_i$, so for some i, we have $\mathrm{tr}(\alpha b_i) \neq 0$. 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 $P = Q \cap R$, so then P is prime in R. If $\alpha \in Q$ is non-zero, then α is a root of some $x^m + a_{m-1}x^{m-1} + \cdots + a_m = 0$ with $a_i \in R$ and $a_m \neq 0$. Then $\alpha^m + \cdots + a_1\alpha \in Q \cap R = P$ and is non-zero, so $P \neq 0$. Since $\dim(R) \leq 1$, the ideal P is maximal. The inclusion $R \hookrightarrow S$ 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 $\dim S = 1$.

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

Example 2.2.22. 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.

We have

$$\boxed{\text{UFD}} \cap \boxed{\text{Dedekind rings}} = \boxed{\text{PID}}$$

Indeed, If R is a Dedekind ring that is a UFD and $P \subset R$ is a nonzero prime ideal, choose a nonzero $a \in P$. Factor aR as a product of principal prime ideals $p_1R, \ldots, p_nR$. Since $aR \subset P$ we have $p_iR \subset P$ for some i. As R is a Dedekind ring we must have $P = p_iR$, i.e., all prime ideals of R are principal. Since every ideal is a product of primes, every ideal in R is principal.

2.3 Discrete valuations

Definition 2.3.1 (Discrete valuation)**.** Let F be a field. A *discrete valuation* on F is a map $\nu : F^\times \to \mathbb{Z}$ 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 ν 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 $aR = P^nA$ 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 nonzero 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 ν 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 $M \subset \{a \in F \mid \nu(a) > 0\}$.*

Proof. That R_ν is a ring and M is an ideal follows from $\nu(ab) = \nu(a) + \nu(b)$ and $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$. That M is the unique maximal ideal follows from using $\nu(a^{-1}) = -\nu(a)$ to show that $R_\nu \backslash M = R_\nu^\times$. $\square$

Definition 2.3.6 (Discrete valuation ring)**.** The ring R_ν is the *valuation ring* of ν.

A domain R is a *discrete valuation ring* (DVR) if $R = R_\nu$ for some discrete valuation ν (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) $\Longrightarrow$ (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 $A = \pi^n R$. For $a \in A$, we have $\nu(a/\pi^n) \geq 0$, so $a/\pi^n \in R$. Hence $a \in \pi^n R$, so $A \subset \pi^n R$. 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 $\pi^n R \subset A$.

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

(3) $\Longrightarrow$ (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 ν. 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 $a/b = c \in R$. □

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 αA 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* $\mathrm{Frac}(R)$ *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. $\mathrm{Frac}(R)$ *is a free abelian group with basis the set of all non-zero prime ideals of R.*

Proof. Let $F \in \mathrm{Frac}(R)$ 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 $\mathrm{Frac}(R)$ 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* $\mathrm{PFrac}(R)$ *of* $\mathrm{Frac}(R)$*.*

Definition 2.4.7 (Class group)**.** The *class group* is $\mathrm{Cl}(R) = \mathrm{Frac}(R)/\,\mathrm{PFrac}(R)$.

Proposition 2.4.8. *The sequence*

$$1 \longrightarrow R^\times \hookrightarrow F^\times \xrightarrow{\alpha \mapsto \alpha R} \mathrm{Frac}(R) \twoheadrightarrow \mathrm{Cl}(R) \longrightarrow 1$$

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. $\mathrm{Cl}(R) = 1$.

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 $\mathrm{Frac}(R)$ are not finitely generated, while results from algebraic number theory state that $\mathrm{Cl}(R)$ is finite and $R^\times$ is finitely generated. However, the structure of $\mathrm{Cl}(R)$ 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 $s \in S := R \backslash P$. 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. □

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 $R_P/P^nR_P \simeq R/P^n$ 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*

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

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 $S = R\backslash\{0\}$. 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 $M \cong aM \subset R^n$. □

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*

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

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 $M \twoheadrightarrow f(M)$ 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. □

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_{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_{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 fractional ideals. For $x \in BA^{-1}$, the "multiplication by x" map $l_x : m \mapsto xm$ is an R-module homomorphism $A \to B$.

Proposition 2.5.7. *Every homomorphism $A \to B$ is of the form l_x for some $x \in BA^{-1}$. Moreover, the choice of x is unique, so* $\operatorname{Hom}_R(A, B) = BA^{-1}$.

Proof. Uniqueness is clear, so we must show existence. Let $f : A \to B$, 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 $x \in xR = xAA^{-1} \subset BA^{-1}$. □

Remark 2.5.8. The composition map $\operatorname{Hom}(B, C) \times \operatorname{Hom}(A, B) \to \operatorname{Hom}(A, C)$ coincides with the product map $CB^{-1} \times BA^{-1} \to CA^{-1}$.

Corollary 2.5.9. *If $A, B \subset R$ are fractional 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 $A \cong B$. □

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

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 $f : \bigoplus_j A_j \to \bigoplus_i B_i$ be an isomorphism represented by the matrix $C = (c_{ij})$, where $c_{ij} \in \operatorname{Hom}(A_j, B_i) = B_i A_j^{-1} \subset F$. We claim that if $a_j \in A_j$, then

$$\det(C) a_1 \cdots a_n \subset B_1 \cdots B_n.$$

Indeed, let $D = C \cdot \operatorname{diag}(a_1, \ldots, a_n)$, 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. □

Remark 2.5.11. If $f : \bigoplus_j A_j \to \bigoplus_i B_i$ is a homomorphism represented by the matrix C, then for every fractional ideal K the matrix C also represents a homomorphism $g : \bigoplus_j (A_j K) \to \bigoplus_i (B_i K)$. In particular, if $f$is an isomorphism, then so is g.

Definition 2.5.12 (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

$$\det(M) = [A_1 \cdots A_n] \in \mathrm{Cl}(R).$$

Proposition 2.5.13. *1.* $\det(M \oplus N) = \det(M)\det(N)$.

2. If $A \subset R$ *is a fractional ideal, then* $\det(A) = [A]$.

Lemma 2.5.14. *Let* A *and* B *be fractional ideals of* R *and* $P \subset R$ *a nonzero prime ideal. Then* $A \oplus PB \simeq AP \oplus B$.

Proof. First consider the case $B = R$. Since $AA^{-1} = R$, there are elements $a_i \in A$ and $x_i \in A^{-1}$ for $i = 1, \dots, n$, such that $\sum a_i x_i = 1$. It follows that there is i such that $a_i x_i \notin P$. Consider the R-module homomorphism $f : A \oplus P \to R$ defined by $f(a, p) = ax_i + p$. Since the image of f properly contains P, it coincides with R, $\mathrm{Im}(f) = R$, hence f is split. It follows that if $C = \mathrm{Ker}(f)$, then $A \oplus P \simeq C \oplus R$. Localizing w.r.t $S = R \setminus \{0\}$ we see that $S^{-1}C \simeq F$. Since C is torsion free, C is an R-submodule of F, i.e., C is a fractional ideal. Taking determinants, we get $[AP] = \det(A \oplus P) = \det(C \oplus R) = [C]$. By Corollary 2.5.9, $C \simeq AP$.

In general, applying the first part of the proof to the ideal AB^{-1} in place of A, we get an isomorphism $AB^{-1}P \oplus R \simeq AB^{-1} \oplus P$. Multiplying with B (see Remark 2.5.11) we get an isomorphism $AP \oplus B \simeq A \oplus PB$. □

Corollary 2.5.15. *Let* A *and* B *be nonzero ideals of* R*. Then* $A \oplus B \simeq AB \oplus R$.

Proof. Write B as a product of n prime ideals and apply the lemma n times. □

An induction yields the following statement.

Corollary 2.5.16. *Let* $A_1, A_2, \dots, A_n$ *be nonzero ideals of* R*. Then* $A_1 \oplus A_2 \oplus \cdots \oplus A_n \simeq A_1 A_2 \cdots A_n \oplus R^{n-1}$.

Recall that the rank of a finitely generated R-module M is the dimension of the F-vector space $S^{-1}M$, where $S = R \setminus \{0\}$.

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* $A \oplus R^{n-1}$*, 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 $\mathrm{Pic}(R)$ of rank 1 projective R-modules with the tensor product over R as the group operation.

Proposition 2.5.19. *For Dedekind domains,* $\mathrm{Pic}(R) \cong \mathrm{Cl}(R)$*.*

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 $M \cong R/\operatorname{Ker} f$, and by the correspondence of submodules, it follows that $\operatorname{Ker} f$ is maximal as a left ideal. Conversely, the correspondence tells us that R/I is simple whenever I is a maximal left ideal. □

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 $S^\times = GL_n(D)$ acts transitively on $M\backslash 0$, where $M = D^n$. It follows that $M = D^n$ is a simple S-module. Note that S as an S-module is a direct sum of n left ideals, each of them is isomorphic to D^n.
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 $\operatorname{Ker} f \neq M$, so $\operatorname{Ker} f = 0$. □

Corollary 3.1.7. *If M is a simple R-module, then $\operatorname{End}_R(M)$ is a division ring.*

Let $A_i \subset R$ be (left) ideals such that $R \simeq \coprod_i A_i$ as (left) R-modules. Then there exist $e_i \in A_i$, all but finitely many zero, such that $1 = \sum_i e_i$. Hence $a = \sum_i ae_i$ for all $a \in R$, so if Δ is the set of indices with $e_i \neq 0$, then $R = \coprod_{i\in\Delta} A_i$. If $a \in A_j$ we have $a = ae_j$ and $ae_i = 0$ if $i \neq 0$. It follows that $A_i = Re_i$ and

1) (Idempotents) $e_i^2 = e_i$;

2) (Orthogonality) $e_ie_j = 0$ if $i \neq j$;

3) (Partition of the identity) $\sum_{i\in\Delta} e_i$.

Conversely, suppose we have a finitely many elements $e_i \in R$ satisfying 1), 2) and 3). Set $A_i = Re_i$. Then $R \simeq \coprod_i A_i$. Indeed, every $a \in R$ is equal to $\sum_i ae_i$ and $ae_i \in A_i$. If $\sum_i b_i = 0$, where $b_i \in A_i$, then for any j, we have $b_j = b_j e_j = (\sum_i b_i)e_j = 0$.

Note that the conditions 1), 2) and 3) are left/right symmetric. Hence we have a decomposition $R \simeq \coprod_i e_i R$ into a direct sum of right ideals $e_i R$.

Proposition 3.1.8. *Let R be a left semisimple ring with $R = \coprod_i Re_i$ with Re_i minimal left ideals. Then the right ideal $e_i R$ is minimal for all i and $R = \coprod_i e_i R$, so R is a right semisimple ring.*

Proof. That $R = \coprod_i e_i R$ 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 $a \in eR$ be non-zero. We must show that $aR = eR$. The inclusion $aR \subset eR$ is clear.

Since $a \in eR$ 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 $f(abe) = abeae_j = abae_j = ae_j$, so $e = abe \in aR$, hence $eR \subset aR$. ☐

Definition 3.1.9 (Semisimple module)**.** A (left) R-module M is *semisimple* if there is a family of simple submodules M_i such that $M = \coprod_i M_i$.

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

Definition 3.1.10 (Semisimple ring)**.** We say that a ring R is *semisimple* if R is left semisimple = right semisimple as R-module.

Remark 3.1.11. The zero module is semisimple but not simple. The zero ring is semisimple.

Lemma 3.1.12. *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

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

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

Lemma 3.1.13. *Let R be a semisimple ring and write $R = \coprod_{i=1}^n L_i$ for L_i minimal left ideals. Then any simple left R-module is isomorphic to L_i for some i. In particular, every minimal (left) ideal is isomorphic to L_i for some i.*

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

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

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

Theorem 3.1.14. *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 $R = \coprod_{i=1}^{n} L_i$ and let M be a left R-module. Then

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

is a sum of simple modules, hence semisimple.

(2) $\implies$ (3) In particular, R is semisimple, so $R = \coprod_{i=1}^{n} L_i$. 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 $J \hookrightarrow R \to R/M$ is an isomorphism. Then $J \cap M = 0$ and J is simple, hence a minimal left ideal, contradicting the choice of M.

□

Example 3.1.15. 1. 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. $M = D^n$ is the only simple (left) R-module.

Similarly, R is isomorphic to the direct sum of n right ideals, each of them is isomorphic to the modules D^n of rows.

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

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.

Theorem 3.1.16 (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 $L_1, \dots, L_k$ be non-isomorphic minimal 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 $R \cong \mathrm{End}_R(R)$ as right R-modules, where $r \in R$ corresponds to left multiplication by r in $\mathrm{End}_R(R)$. On the other hand, $\mathrm{End}_R(R)$ is the ring of matrices (s_{ij}) with $s_{ij} \in S_{ij} = \mathrm{Hom}_R(N_j, N_i)$. By Schur's lemma, we have $\mathrm{Hom}_R(L_j, L_i) = 0$ if $i \neq j$ and $\mathrm{Hom}_R(L_j, L_i) = D_i = \mathrm{End}_R(L_i)$ if $i = j$. Therefore,

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

The result follows. □

Remark 3.1.17.

1. The central orthogonal idempotents $e_1, \dots, e_k \in R$ 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 $D_i = \mathrm{End}_R(L_i)$ and $n_i = \dim_{D_i}(\mathrm{Hom}_R(L_i, R))$.

More generally, let M be a right R-module with $M \cong L_1^{a_1} \oplus \cdots \oplus L_k^{a_k}$. Then $a_i = \dim_{D_i}(\mathrm{Hom}_R(L_i, M))$.

Remark 3.1.18. (Morita equivalence) Let R be a ring and P a right R-module. Set $S = \mathrm{End}_R(P)$. Then P is also a left S-module: ${}_S P_R$. If M is a left R-module, the tensor product $P \otimes_R M$ is a left S-module, and we have a functor

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

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

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

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

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

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

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

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

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

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

$$R\textbf{-Mod} \cong D_1\textbf{-Mod} \times \cdots \times D_k\textbf{-Mod}.$$

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 $\operatorname{rad}_R(M)$, is the intersection of all maximal submodules of M.

Example 3.2.2.

1. $\operatorname{rad}(\mathbb{Z}) = 0$;
2. $\operatorname{rad}_{\mathbb{Z}}(\mathbb{Q}) = \mathbb{Q}$ since there is no maximal submodule;
3. $\operatorname{rad}_R[M/\operatorname{rad}_R(M)] = 0$.

Proposition 3.2.3. *Let M be a left R-module.*

1. *If M is semisimple, then $\operatorname{rad}_R(M) = 0$.*
2. *If M is artinian and $\operatorname{rad}_R(M) = 0$, 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 $\operatorname{rad}_R(M) = 0$, 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. □

Lemma 3.2.4. $\operatorname{rad}(R)$ *is the set of all elements $a \in R$ such that $1 - ba$ has a left inverse for all $b \in R$.*

Proof. If $a \in \operatorname{rad}(R)$ 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. □

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

Proof. If $c(1-ab) = 1$, then $c(1-ab)a = a$, or equivalently, $ca(1-ba) = a$. Therefore, $bca(1-ba) = ba$, and

$$(bca + 1)(1 - ba) = bca(1 - ba) + (1 - ba) = ba + (1 - ba) = 1. \qquad \square$$

Proposition 3.2.6. $\mathrm{rad}(R)$ *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 $a \in \mathrm{rad}(R)$.

Conversely, if $a \in \mathrm{rad}(R)$, then $1 - cba$ is left invertible for all $c, b \in R$ by Lemma 3.2.4, so then $1 - bac$ is left invertible by Lemma 3.2.5, i.e., $d(1 - bac) = 1$ for some $d \in R$. In particular, d is right invertible. By Lemma 3.2.4, $1 + cdba$ is left invertible, hence $d = 1 + dbac$ is left invertible in view of Lemma 3.2.5. Hence d is left and right invertible, so $d \in R^\times$ and $d^{-1} = 1 - bac \in R^\times$. $\square$

Corollary 3.2.7. $\mathrm{rad}(R)$ *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 $J(R) = \mathrm{rad}(R)$.

There is another characterization of the Jacobson radical.

Proposition 3.2.9. *$J(R)$ coincides with the set of all elements $x \in R$ such that $xM = 0$ for all left simple R-modules M.*

Proof. Suppose that $x \in R$ such that $xM = 0$ for all left simple R-modules M. Let $I \subset R$ be a maximal left ideal. Then $M := R/I$ is a simple left R-module. Since $xM = 0$, we have $x \in I$ for all I, i.e., $x \in J(R)$.

Conversely, let $x \in J(R)$ and M a simple left R-module. Then $M \simeq R/I$ for a maximal left ideal I. Since $J(R)$ is a two-sided ideal, we have $xR \subset J(R) \subset I$, i.e., $xM = x(R/I) = 0$. $\square$

Theorem 3.2.10. *A ring R is semisimple if and only if R is (left) 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 and $M_n(D)$ is a finite sum of simple (minimal) left ideals. Note that simple modules are artinian. $\square$

Definition 3.2.11 (Simple ring)**.** A non-zero ring R is *simple* if R has no non-trivial two-sided ideals.

Example 3.2.12. If D is a division ring, then $R = M_n(D)$ is simple. Indeed, let $I \subset R$ be a nonzero 2-sided ideal and $x = \sum_{i,j} x_{ij} e_{ij} \in I$ a nonzero element. Then $x_{st} \neq 0$ for some s and t. Then for every k the element $e_{ks} x e_{tk} = e_{kk} x_{st}$ is in I. Then I contains the invertible element $x_{st} = \sum_k e_{kk} x_{st}$, hence $I = R$.

Theorem 3.2.13. *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. □

Theorem 3.2.14 (Nakayama Lemma). *Let M be a finitely generated left R-module. If $J(R)M = M$, then $M = 0$.*

Proof. Let $\{m_1, m_2, \ldots, m_n\}$ be a generating set for M with the smallest n. We show that $n = 0$. Suppose $n > 0$. Write $m_n = \sum_{i=1}^{n} x_i m_i$ with $x_i \in J(R)$. Therefore,

$$(1 - x_n)m_n = \sum_{i=1}^{n-1} x_i m_i \in M' := \sum_{i=1}^{n-1} Rm_i.$$

The element $1 - x_n$ in R is invertible, hence $m_n \in M'$ and therefore, $M = M'$ is generated by $n - 1$ elements, a contradiction. □

Proposition 3.2.15. *Let R be a nonzero ring and $I = R \setminus R^{\times}$. TFAE:*

(1) *I is closed under addition;*

(2) *I is a (left) ideal;*

(3) *$I = J(R)$;*

(4) *There is a unique maximal (left) ideal in R;*

(5) *$J(R)$ is a maximal (left) ideal.*

Proof. (1) ⇒ (2): Suppose $a \in I$ and $r \in R$ are such that $ra \notin I$, i.e., ra is invertible: $rav = vra = 1$ for some $v \in R$. Let $u := vr$, so $ua = 1$.

We claim that u is not invertible, i.e., $u \in I$. Indeed, if $u \in R^{\times}$, then $a = u^{-1} \in R^{\times}$, a contradiction since $a \in I$. As u is right invertible, it follows from the claim that u is not left invertible, i.e., $Ru \neq R$. Since $Ru \cap R^{\times} = \emptyset$, we have $Ru \subset I$. In particular, $au \in I$. But $(1 - au)a = 0$ and $a \neq 0$, hence $1 - au$ is not invertible $1 - au \in I$. By assumption $1 = au + (1 - au) \in I$ since both au and $1 - au$ are in I. This is a contradiction.

(2) ⇒ (4): Every proper (left) ideal in R is disjoint with $R^{\times}$, hence it is contained in $I = R \setminus R^{\times}$, hence I is a unique maximal (left) ideal.

(4) ⇒ (3): Let I be a unique maximal left ideal. Hence $I = J(R)$, so I is a right ideal as well. Let $x \in R \setminus I$, we show that $x \in R^{\times}$.

We claim that if $a \in R \setminus I$, then a is left invertible. Indeed, as $a \notin I$, the left ideal Ra is not contained in I, hence $Ra = R$, i.e., a is left invertible. This proves the claim.

By the claim, there is $y \in R$ such that $yx = 1$. If $y \in I$, then $1 = yx \in I$ since I is a right ideal, a contradiction. Thus, $y \in R \setminus I$, and by the claim, there is $z \in R$ such that $zy = 1$. It follows that y is invertible and $y^{-1} = x = z$ and hence $x \in R^{\times}$. We have proved that $R \setminus J(R) = R \setminus I = R^{\times}$.

(3) ⇒ (2) ⇒ (1): trivial.

(4) ⇔ (5) is clear. □

Definition 3.2.16 (Local ring). The ring R is a *local ring* if the conditions (1) – (5) of the proposition hold.

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 ring)**.** Let G be a group and let R be a commutative ring. The *group ring* of G over R, denoted $R[G]$, is the free R-module generated by the set G, together with multiplication induced by the group law on the generators.

Example 4.1.5.

1. Let G be a cyclic group of order n. Then
$$\mathbb{Q}[G] = \mathbb{Q}[t]/(t^n - 1) \cong \prod_{d|n} \mathbb{Q}[t]/(\Phi_d(t)) \cong \prod_{d|n} \mathbb{Q}(\zeta_d).$$
2. Let F be a field with $\operatorname{char} F = p > 0$ and let G be a cyclic group of order p. Then
$$F[G] = F[t]/(t^p - 1) = F[s]/(s^p).$$
3. Let S be an R-algebra. Then there is a natural isomorphism
$$\operatorname{Hom}_{R-Alg}(R[G], S) \simeq \operatorname{Hom}(G, S^{\times}).$$

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 isomorphic categories for representation theory.

Objects	**Morphisms**
G-spaces V	F-linear maps $f : V \to W$ such that $f(gv) = gf(v)$
Representations $\rho : G \to GL(V)$	F-linear maps $f : V \to W$ such that $f(\rho(g)(v)) = \mu(g)(f(v))$
$F[G]$-modules	$F[G]$-module homomorphisms

In particular, the categories of G-spaces and representations of G are abelian.

Two representations $\rho : G \to GL(V)$ and $\mu : G \to GL(W)$ are isomorphic iff there is an isomorphism $f : V \xrightarrow{\sim} W$ such that $f(\rho(g)(v)) = \mu(g)(f(v))$.

Two matrix representations $\rho : G \to GL_n(F)$ and $\mu : G \to GL_m(F)$ are isomorphic iff $n = m$ and there is an invertible matrix $c \in GL_n(F)$ such that $\mu(g) = c \cdot \rho(g) \cdot c^{-1}$ for all $g \in G$. Such representations ρ and μ are also called *equivalent* or *similar*.

Example 4.1.6. If V is a G-space, then the dual space $V^* = \mathrm{Hom}_F(V, F)$ is also a G-space via $(g\varphi)(v) = \varphi(g^{-1}v)$. A map of G-spaces $V \to V^*$ is given by a G-invariant bilinear form $B : V \times V \to F$, that is $B(gv, gw) = B(v, w)$ for all $g \in G$ and $v, w \in V$. In particular, the G-spaces V and V^* are isomorphic if and only if there is a non-degenerate G-invariant bilinear form $B : V \times V \to F$.

Example 4.1.7. If V is a G-space, we write

$$V^G := \{v \in V \mid gv = v \quad \text{for all} \quad g \in G, v \in V\}$$

for the subspace of G-fixed elements. Let V and W be two G-spaces. The space $\mathrm{Hom}_F(V, W)$ of all F-linear homomorphisms $V \to W$ has structure of a G-space via $(g\varphi)(v) = g\varphi(g^{-1}v)$. Then

$$\mathrm{Hom}_F(V, W)^G = \mathrm{Hom}_G(V, W).$$

Direct sums of $F[G]$-modules correspond to the direct sums of G-spaces and representations of G.

The G-spaces and representations corresponding to simple $F[G]$-modules are called *irreducible*.

Theorem 4.1.8. *Let G be a finite group and F be a field. Then $F[G]$ is semisimple if and only if $\mathrm{char}\, F$ does not divide $|G|$.*

Proof. ($\Longrightarrow$) 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 $I = \mathrm{Ker}\, \varepsilon$, 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 $f \circ \varepsilon = \mathrm{id}_F$. If $f(1) = u$, then $gu = u$ for all $g \in G$, so then $u = a \sum_g g$ for some $a \in F$. Applying ε, we get $a|G| = 1$.

($\Longleftarrow$) 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 $f \circ h = \mathrm{id}_P$.

Note that the vector space $\mathrm{Hom}_F(P, N)$ is a G-space via $(gh)(p) = g(h(g^{-1}p))$. We have h a map of G-spaces if and only if $gh = h$ for all $g \in G$.

Consider the linear map $h' : P \to N$:

$$h' = \frac{1}{|G|} \sum_{g \in G} gh.$$

Then

$$f \circ h' = \frac{1}{|G|} \sum_{g \in G} (f \circ gh) = \frac{1}{|G|} \sum_{g \in G} (gf \circ gh) = \frac{1}{|G|} \sum_{g \in G} (g\, \mathrm{id}_F) = \mathrm{id}_F$$

and $gh' = h'$ for all $g \in G$, i.e., h' is a map of G-spaces. $\square$

It follows from the theorem that if $\mathrm{char}(F) = 0$, then:

1. Every G-space is a direct sum of irreducible G-spaces that are unique up to permutation and isomorphisms.

2. Every $F[G]$-module is a direct sum of simple $F[G]$-modules that are unique up to permutation and isomorphisms.

3. Every representation of G is isomorphic to a direct sum of irreducible representations that are unique up to permutation and isomorphisms.

Proposition 4.1.9. *Let F be an algebraically closed field and let D be a finite-dimensional F-algebra which is also a division ring. 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, $a \in F$. $\square$

As a corollary, the Artin-Wedderburn theorem tells us that

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

Then $M_i \cong F^{d_i}$ is a simple left $M_{d_i}(F)$-module of dimension d_i for all $i = 1, 2, \ldots, k$. We view M_i as left $F[G]$-modules via the projection $F[G] \to M_{d_i}(F)$. The modules M_i are all non-isomorphic simple left $F[G]$-modules.

Every left $F[G]$-module is a direct sum of the M_i's.

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 $\rho \cong \bigoplus_i \rho_i^{a_i}$.

Consider the center $Z(F[G])$. The condition that $\alpha \in Z(F[G])$ is equivalent to the condition that α 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 $Z(F[G])$. In particular, $\dim(Z(F[G]))$ is the number of conjugacy classes of G.

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

Remark 4.1.10. If $\alpha : H \to G$ is a group homomorphism and $\rho : G \to GL(V)$ is a representation of G, then the composition $\rho \circ \alpha : H \to GL(V)$ is a representation of H, called the *pull-back* of ρ. If α is surjective and ρ is irreducible, then the pull-back of ρ is also irreducible.

4.2 One-dimensional representations

We assume that F is an algebraically closed field of characteristic zero.

Definition 4.2.1. A *(multiplicative) character* of a group G is a group homomorphism $G \to F^\times$.

If V is a one-dimensional vector space over a field F then $GL(V) = F^\times$. Hence a 1-dimensional representation of a group G is a character of G.

In terms of matrices, two matrix representations $\rho, \mu : G \to GL_n(F)$ are isomorphic if and only if there is a matrix $c \in GL_n(F)$ such that $\mu(g) = c\rho(g)c^{-1}$ for all g. In particular, if $\rho, \mu : G \to F^\times$ 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. $|\mathrm{Hom}(G, F^\times)| = n$. In fact, $\mathrm{Hom}(G, F^\times) \cong G$, but we will not show this.

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

Example 4.2.2.

1. A finite abelian group G has exactly $|G|$ irreducible representations, all one-dimensional. Conversely, if all irreducible representations of a finite group G are one-dimensional, then G is abelian.

2. The group S_3 has order 6, and it has 3 conjugacy classes. Its derived subgroup is A_3, so there are two one-dimensional representations, i.e. $d_1 = d_2 = 1$. Then $d_3 = 2$ as $d_1^2 + d_2^2 + d_3^2 = 6$. The 2-dimensional irreducible S_3-space is $\mathrm{Ker}(F^3 \to F)$, where $(a, b, c) \mapsto a + b + c$. This is irreducible since the derived subgroup acts nontrivially.

3. The group A_4 has order 12, and it has 4 conjugacy classes. We have A_4 is a semidirect product of $N = \mathbb{Z}/2 \times \mathbb{Z}/2$ and C_3. Hence A_4/A_4' is cyclic of order 3, so there are 3 one-dimensional representations, i.e. $d_1 = d_2 = d_3 = 1$. We have $d_4 = 3$ as $d_1^2 + d_2^2 + d_3^2 + d_4^2 = 12$. The 3-dimensional irreducible representation is $\mathrm{Ker}(F^4 \to F)$. This is irreducible because the commutator subgroup acts nontrivially.

4. 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 ± 1 depending on whether the permutation is even or odd. The dimensions d_i satisfy
$$d_1^2 + d_2^2 + d_3^2 + d_4^2 + d_5^2 = 24,$$
so we must have $d_3 = 2$ and $d_4 = d_5 = 3$. The 2-dimensional representation is the pull-back of the irreducible 2-dimensional representation of S_3 under surjection $S_4 \to S_3$. One of the 3-dimensional representations is $\mathrm{Ker}(F^4 \to F)$. The other one is the twist of this by the only nontrivial 1-dimensional representation.

5. 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
$$-1 \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$
This is irreducible because the commutator $-1 = [i, j]$ is not the identity.

4.3 Characters

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

Example 4.3.2. If $\dim \rho = 1$, then $\chi_\rho = \rho$. If ρ is trivial 1-dimensional representation, then $\chi_\rho = 1$.

Equivalently, if V is a G-space, then we define $\chi_V : G \to F$ by

$$\chi_V(g) = \operatorname{tr}(v \mapsto gv).$$

The character χ_ρ of a representation $\rho : G \to GL(V)$ can be extended to an F-linear map $\chi_\rho : F[G] \to F$, i.e. a linear functional on the vector space $F[G]$. We have $\chi_\rho(s) = \operatorname{tr}(v \mapsto sv)$, the trace of the left multiplication $s : V \to V$.

Proposition 4.3.3. *1. If $\rho \cong \mu$, then $\chi_\rho = \chi_\mu$.*

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

3. $\chi_\rho(hgh^{-1}) = \chi_\rho(g)$ for all $g, h \in G$, i.e., χ_ρ is constant on conjugacy classes.

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

$$\rho_{\text{reg}} = \bigoplus_i \rho_i^{d_i}, \quad \text{so} \quad \chi_{\text{reg}} = \sum_i d_i \chi_{\rho_i}.$$

(Recall that $\rho_1, \ldots, \rho_k$ are all irreducible representations of G and $d_i = \dim(\rho_i)$.)

Example 4.3.5. For $G = Q_8$, we get a character table as shown.

	1	-1	i	$-i$	j	$-j$	k	$-k$
χ_1	1	1	1	1	1	1	1	1
χ_2	1	1	1	1	-1	-1	-1	-1
χ_3	1	1	-1	-1	1	1	-1	-1
χ_4	1	1	-1	-1	-1	-1	1	1
χ_5	2	-2	0	0	0	0	0	0

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

Example 4.3.6. Let $G = S_3 = \{1, (12), (13), (23), (123), (132)\}$.

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Example 4.3.7. Let $G = S_n$. Let ρ_{st} be the *standard* representation in the space F^n given by permutations of the components. We have

$$\chi_{st}(\sigma) = \mathrm{Fix}(\sigma),$$

where $\mathrm{Fix}(\sigma)$ is the number of symbols $i = 1, \ldots, n$ fixed by σ. The subspace of F^n spanned by $(1, \ldots, 1)$ is a trivial 1-dimensional G-space. Hence $\rho_{taut} = 1 \oplus \rho'_{taut}$. We have $\rho'_{st}(\sigma) = \mathrm{Fix}(\sigma) - 1$.

Example 4.3.8. For $G = S_4$. The conjugacy classes are represented by $1, (12), (123), (12)(34), (1234)$.

	1	(12)	(123)	(12)(34)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	-1	1

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 central idempotents e_i and simple modules M_i, where M_i is the minimal left ideal in $M_{d_i}(F)$, $i = 1, \ldots, k$.
Given $m \in M_i$, we have $e_j m = m$ if $j = i$ and $e_j m = 0$ if $j \neq i$. If χ_i is the character of the representation on M_i, then $\chi_i(a) = \mathrm{tr}(m \mapsto am)$ for $a \in F[G]$, so in particular,

$$\chi_i(ae_j) = \begin{cases} \chi_i(a), & \text{if } j = i; \\ 0, & \text{otherwise.} \end{cases}$$

In particular, $\chi_i(e_j) = d_i \delta_{i,j}$.
Write $e_i = \sum_h a_{i,h} h \in F[G]$. For $g \in G$, we have

$$\chi_{\mathrm{reg}}(g^{-1}e_i) = \chi_{\mathrm{reg}}\Big(g^{-1} \sum_{h \in G} a_{i,h} h\Big) = \sum_{h \in G} a_{i,h} \chi_{\mathrm{reg}}(g^{-1}h) = n a_{i,g},$$

where $n = |G|$. On the other hand, since $\chi_{\mathrm{reg}} = \sum_j d_j\chi_j$, we get

$$na_{i,g} = \sum_j d_j\chi_j(g^{-1}e_i) = d_i\chi_i(g^{-1})$$

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. In particular, the characters of representations of G are in $\mathrm{Ch}(G)$. 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 symmetric bilinear form.

Proposition 4.4.1. *The characters $\chi_1, \dots, \chi_k$ form an orthonormal basis of $\mathrm{Ch}(G)$ with respect to B.*

Proof. We have

$$\langle \chi_i, \chi_j\rangle = \frac{1}{n}\sum_{g\in G}\chi_i(g^{-1})\chi_j(g) = \frac{1}{d_i}\chi_j\Big(\frac{d_i}{n}\sum_{g\in G}\chi_i(g^{-1})g\Big) = \frac{1}{d_i}\chi_j(e_i) = \delta_{ij}. \qquad \square$$

Thus,

$$\Big\langle \sum_i a_i\chi_i, \sum_i b_i\chi_i\Big\rangle = \sum_i a_ib_i.$$

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

1. *Every finite-dimensional representation ρ is isomorphic to $\bigoplus_i \rho_i^{\oplus m_i}$, where $m_i = \langle\chi_\rho, \chi_i\rangle$.*
2. *Two representations ρ and μ are isomorphic if and only if $\chi_\rho = \chi_\mu$.*
3. *A representation ρ is irreducible if and only if $\langle\chi_\rho, \chi_\rho\rangle = 1$.*

Proof. 1. Write $\rho \simeq \bigoplus_j \rho_j^{\oplus m_j}$ for some $m_j \geq 0$, hence $\chi_\rho = \sum_j m_j\chi_j$, and therefore,

$$\langle\chi_\rho, \chi_i\rangle = \sum_j m_j\langle\chi_j, \chi_i\rangle = m_i.$$

2. Write $\rho \simeq \bigoplus_j \rho_j^{\oplus m_j}$ and $\mu \simeq \bigoplus_j \rho_j^{\oplus n_j}$. If $\chi_\rho = \chi_\mu$, then $m_i = \langle\chi_\rho, \chi_i\rangle = \langle\chi_\mu, \chi_i\rangle = n_i$, hence $\rho \simeq \mu$.

3. Write $\rho \simeq \bigoplus_j \rho_j^{\oplus m_j}$. We have $\langle\chi_\rho, \chi_\rho\rangle = \sum_j m_j^2$. This integer is equal to 1 if and only if there is i such that $m_i = 1$ and $m_j = 0$ for all $j \neq i$, i.e., if $\rho \simeq \rho_i$ is irreducible. $\square$

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 $\rho_{st} = 1 \oplus \rho'_{st}$. One can show that the S_n-representation ρ'_{st} is irreducible if $n > 1$. It follows that

$$\langle 1, \chi_{st} \rangle = \langle 1, 1 \rangle + \langle 1, \chi'_{st} \rangle = 1 + 0 = 1.$$

Recall that $\chi_{st}(\sigma) = \mathrm{Fix}(\sigma)$. Then

$$\frac{1}{n!} \sum_{\sigma \in S_n} \mathrm{Fix}(\sigma) = 1,$$

i.e., the average value of $\mathrm{Fix}(\sigma)$ over all $\sigma \in S_n$ is equal to 1!

We have $\mathrm{Fix}(\sigma^{-1}) = \mathrm{Fix}(\sigma)$ and if $n \geq 2$,

$$\langle \chi_{st}, \chi_{st} \rangle = \langle 1, 1 \rangle + \langle \chi'_{st}, \chi'_{st} \rangle = 1 + 1 = 2.$$

Hence

$$\frac{1}{n!} \sum_{\sigma \in S_n} \mathrm{Fix}(\sigma)^2 = \frac{1}{n!} \sum_{\sigma \in S_n} \mathrm{Fix}(\sigma^{-1}) \, \mathrm{Fix}(\sigma) = \langle \chi_{st}, \chi_{st} \rangle = 2,$$

i.e., the average value of $\mathrm{Fix}(\sigma)^2$ over all $\sigma \in S_n$ is equal to 2! It follows that the variance of Fix is equal to $2 - 1^2 = 1$.

In general, the average value of $\mathrm{Fix}(\sigma)^m$ over all $\sigma \in S_n$ is equal to the number of partitions of the set $[1, m] = \{1, 2, \ldots, m\}$ into disjoint union of $\leq n$ subsets. If $n \geq m$, this is equal to the number of all partitions of the set $[1, m]$ into disjoint union of subsets. This number depends only on m, denoted B_m and called the *Bell number*.

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

$$\left(\sum_{i=1}^{n} x_i^2 \right) \left(\sum_{j=1}^{n} y_j^2 \right) = \sum_{k=1}^{n} z_k^2.$$

Example 4.5.1. 1. $x_1^2 y_1^2 = (x_1 y_1)^2$

2. Use the norm map for the quadratic field extension $F(\sqrt{-1})/F$:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 - x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2.$$

3. Use the reduced norm map for the Hamilton quaternion algebra:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = &(x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4)^2 + \\ &(x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3)^2 + \\ &(x_1 y_3 - x_2 y_4 + x_3 y_1 + x_4 y_2)^2 + \\ &(x_1 y_4 + x_2 y_3 - x_3 y_2 + x_4 y_1)^2\end{aligned}$$

4. Use the norm map for the Cayley algebra:

$$\begin{aligned}
&(x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2)(y_1^2+y_2^2+y_3^2+y_4^2+y_5^2+y_6^2+y_7^2+y_8^2) =\\
&(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8)^2+\\
&(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7)^2+\\
&(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6)^2+\\
&(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_5)^2+\\
&(x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4)^2+\\
&(x_1y_6 + x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3)^2+\\
&(x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2)^2+\\
&(x_1y_8 - x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1)^2.
\end{aligned}$$

Theorem 4.5.2 (Hurwitz)**.** *This can only happen for $n = 1, 2, 4, 8$.*

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

$$z_k = \sum_{i,j=1}^{n} a_{kij} x_i y_j.$$

We can write the equality in the matrix form as follows. Consider the $n \times n$-matrix

$$A = A_1x_1 + A_2x_2 + \ldots + A_nx_n$$

over $F[x_1, x_2, \ldots, x_n]$, where $A_i = (a_{kij})_{k,j}$ is $n \times n$ matrix over F and $z = (z_1, z_2, \ldots, z_n)^t$ and $y = (y_1, y_2, \ldots, y_n)^t$ are columns of variables. Then the equality above reads:

$$z = Ay$$

and hence

$$y^t\Big(\sum_{i=1}^{n} x_i^2 \cdot I_n\Big)y = \Big(\sum_{i=1}^{n} x_i^2\Big)\cdot\Big(\sum_{i=1}^{n} y_i^2\Big) = \sum_{i=1}^{n} z_i^2 = z^t z = (Ay)^t(Ay) = y^t(A^tA)y,$$

It follows that

$$\sum_{i=1}^{n} x_i^2 \cdot I_n = A^tA = \sum_{i=1} A_i^tA_i x_i^2 + \sum_{i<j}(A_i^tA_j + A_j^tA_i)x_ix_j,$$

and hence

$$A_i^tA_i = I_n \quad \text{and} \quad A_i^tA_j + A_j^tA_i = 0.$$

Letting $B_i = A_n^tA_i$, we have for $i = 1, 2, \ldots, n-1$,

$$B_i^2 = (A_n^tA_i)(A_n^tA_i) = -(A_n^tA_i)(A_i^tA_n) = -A_n^t(A_iA_i^t)A_n = -A_n^tA_n = -I_n,$$

and for $i \neq j$,

$$B_iB_j = (A_n^tA_i)(A_n^tA_j) = -(A_n^tA_i)(A_j^tA_n) = (A_n^tA_j)(A_i^tA_n) = -(A_n^tA_j)(A_n^tA_i) = -B_jB_i.$$

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 μ of G. Note that $\mu(\varepsilon)$ is multiplication by -1. The order of G is 2^n.

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 $g \notin Z(G)$, 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 the dimensions d_1 and d_2 of the other two irreducible representations satisfy $d_1^2 + d_2^2 = 2^{n-1}$. Considering the largest powers of 2 dividing d_1 and d_2 we see that d_1 and d_2 are both equal to $2^{(n-2)/2}$.

If ρ is a 1-dimensional representation of G, then $\rho(\varepsilon) = 1$, but $\mu(\varepsilon)$ is multiplication by -1, so the representation μ cannot have any 1-dimensional irreducibles in its decomposition. Hence the integer $\dim(\mu) = n$ is a multiple of $2^{(n-1)/2}$ if n is odd and a multiple of $2^{(n-2)/2}$ if n is even. From this, we deduce that $n \in \{1, 2, 4, 8\}$. □

4.6 More properties of representations

Let F be the field of complex numbers.

Proposition 4.6.1. *Let χ be the character of a representation ρ 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 multiple of the identity.*

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 χ 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. (Here $C(g)$ is the conjugacy class of g.)*

Proof. The irreducible representation $\rho : G \to GL(V)$ extends to an F-algebra homomorphism $F[G] \to \mathrm{End}(V)$. We can then restrict to a ring homomorphism

$$Z(F[G]) \to \mathrm{End}_G(V),$$

over F, where $Z(F[G])$ is the center of $F[G]$. By Schur's lemma, $\mathrm{End}_G(V) \cong F$, so anything in $Z(F[G])$ acts by scalar multiplication. In particular, $\alpha = \sum_{h \in C(g)} h$ maps to $\lambda 1_V$, so

$$\chi(\alpha) = |C(g)|\chi(g) = d\lambda.$$

Note that $\alpha \in Z(\mathbb{Z}[G])$, which has a ring homomorphism to F with λ in its image. If R is the image, then it is a subring of F which is finitely generated as a $\mathbb{Z}$-module. Therefore, λ is integral over $\mathbb{Z}$. □

Remark 4.6.3. We have proved that every central element in $F[G]$ acts on a simple $F[G]$-module by scalar multiplication.

Theorem 4.6.4. *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 χ be the character of an irreducible representation. Then if $C_1, \dots, C_k$ 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. □

Remark 4.6.5. The statement of the theorem holds over any algebraically closed field of characteristic zero. Indeed, let L be a field extension of the field of complex numbers F. Applying the functor $-\otimes_F L$ to the ring isomorphism $F[G] \simeq \prod_{i=1}^{r} M_{d_i}(F)$ we get an isomorphism

$$L[G] \simeq F[G] \otimes_F L \simeq \prod_{i=1}^{r} M_{d_i}(L).$$

Hence, dimensions of irreducible representations of G over L are the same as over L. Now, let K be an algebraically closed field of characteristic zero. Choose a field L that is an extension of both fields F and K. (Take the factor ring of $F \otimes_{\mathbb{Z}} K$ by a maximal ideal.) By the above, dimensions of irreducible representations of G over F, L and K are the same.

Let $H \subset G$ be a subgroup. If V is a G-space, then V can be be viewed as an H-space, called the *restriction* of V to H and denoted by $\operatorname{Res}_H^G(V)$. We have $\dim \operatorname{Res}_H^G(V) = \dim V$.

Conversely, let W be an H-space. Let $\widetilde{W}$ be the set of all maps $f : G \to W$ such that $f(hg) = hf(g)$ for all $h \in H$ and $g \in G$. Then $\widetilde{W}$ has structure of a G-space by $(gf)(x) = f(xg)$ where $g, x \in G$ and $f \in \widetilde{W}$. We call $\widetilde{W}$ the G-space *induced from* W and denote by $\operatorname{Ind}_H^G(W)$. We have $\dim \operatorname{Ind}_H^G(W) = [G : H] \cdot \dim W$.

Example 4.6.6. Let V be a G-space such that there is a basis X for V stable under G. (Such G-space is called a *permutation* G-space.) Suppose G acts transitively on X and H is the stabilizer of a point $x_0 \in X$. Then $V \simeq \operatorname{Ind}_H^G(1)$. Indeed, every H-invariant map $f : G \to F$ (viewed as an element of $\operatorname{Ind}_H^G(1)$) is constant on the left cosets Hg. Take a point $x \in X$ and write $x = g^{-1}x_0$ for some $g \in G$. The left coset Hg is well defined by x. Let $f_x : G \to F$ be a map such that f_x is equal to 1 on Hg and zero otherwise. Then $g(f_x) = f_{gx}$, i.e., $(f_x)_{x\in X}$ is a permutation basis for $\operatorname{Ind}_H^G(1)$ that is isomorphic to X as a G-set. Thus, $V \simeq \operatorname{Ind}_H^G(1)$.

If V is a G-space and W is an H-space, there is a natural isomorphism of vector spaces

$$\mathrm{Hom}_G\left(\mathrm{Ind}_H^G(W), V\right) \simeq \mathrm{Hom}_H\left(W, \mathrm{Res}_H^G(V)\right).$$

In other words, the functor $\mathrm{Ind}_H^G : H\text{-}Rep \to G\text{-}Rep$ is a left adjoint to the functor $\mathrm{Res}_H^G : G\text{-}Rep \to H\text{-}Rep$.

Let W and W' be two G-spaces. Write $W = \bigoplus_i V_i^{\oplus n_i}$ and $W' = \bigoplus_i V_i^{\oplus m_i}$, where V_i are irreducible G-spaces. Recall that $\mathrm{Hom}_G(V_i, V_j)$ is zero if $i \neq j$ and is equal to F if $i = j$. It follows that

$$\dim \mathrm{Hom}_G(W, W') = \sum_i n_i m_i = \langle \chi_W, \chi_{W'} \rangle.$$

Example 4.6.7. Let V be a G-space and W an H-space. Then

$$\langle \chi_{\mathrm{Ind}_H^G(W)}, \chi_V \rangle_G = \langle \chi_W, \chi_{\mathrm{Res}_H^G(V)} \rangle_H.$$

4.7 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,

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

We assume that F is algebraically closed of characteristic zero.

Corollary 4.7.1. *If ρ and μ are irreducible, then $\rho \otimes \mu$ is irreducible.*

Corollary 4.7.2. *If $\rho_1, \ldots, \rho_k$ are all irreducible representations of G and $\mu_1, \ldots, \mu_m$ are all irreducible representations of H, then $\rho_i \otimes \mu_j$ are all irreducible representations of $G \times H$.*

If $G = H$, then we can restrict $\rho \otimes \mu$ to the diagonal $G \hookrightarrow G \times G$. We have $\chi_{\rho\otimes\mu}(g) = \chi_\rho(g) \cdot \chi_\mu(g)$. However, the restriction may not be irreducible even if ρ and μ are.

Theorem 4.7.3. *Let d be the dimension of an irreducible representation ρ of a finite group G. Then $d \mid [G : Z]$, where Z is the center of G.*

Proof. Let $g \in Z$, so then $\rho(g)$ acts as a scalar as the representation is irreducible. 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

$$H = \{(z_1, \ldots, z_m) \in Z^m \mid z_1 \cdots z_m = 1\} \trianglelefteq G^m$$

with $|H| = |Z|^{m-1}$. We have that $\mu(H) = 1$, so μ 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 $d \mid |G|/|H| = [G : Z]$. $\square$

4.8 Burnside's theorem

Theorem 4.8.1 (Burnside's pq-theorem)**.** *Let p and q be primes. Then every group of order $p^a q^b$ is solvable.*

Lemma 4.8.2. *Let χ be the character of an irreducible representation ρ of dimension d of a finite group G. Let C be a conjugacy class in G such that $\gcd(|G|, d) = 1$. Then for every $g \in C$, either $\chi(g) = 0$ or $\rho(g)$ is a multiple of the identity.*

Proof. Since $|C(g)|\chi(g)/d$ is an algebraic integer and $\gcd(|G|, d) = 1$, the fraction $\alpha := \chi(g)/d$ is an algebraic integer.

Let $K/\mathbb{Q}$ be a finite cyclotomic field extension containing all roots of unity of degree $|G|$. In particular, $\alpha \in K$. For every $\sigma \in \Gamma = Gal(K/\mathbb{Q})$, $\sigma(\chi(g))$ is the sum of d roots of unity, hence $|\sigma(\chi(g))| \leq d$ and $|\sigma(\alpha)| \leq 1$. Therefore,

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{\sigma\in\Gamma} |\sigma(\alpha)| \leq 1.$$

But $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ as α is an algebraic integer. Hence $|N_{K/\mathbb{Q}}(\alpha)|$ is either equal to 0 or 1. If $|N_{K/\mathbb{Q}}(\alpha)| = 0$, then $\chi(g) = 0$. If $|N_{K/\mathbb{Q}}(\alpha)| = 1$, then $|\alpha| = |\chi(g)/d| = 1$ and we have already proved that this implies $\rho(g)$ is a multiple of the identity. □

Proposition 4.8.3. *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 all 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

$$H = \{g \in G \mid \rho_i(g) \text{ is a multiple of the identity}\} \trianglelefteq G.$$

If $H = G$, then all $\rho_i(g)$ commute, so $\rho_i(G)$ is abelian. Since $\rho_i \neq 1$, we have $\operatorname{Ker}\rho_i \neq G$, but if $\operatorname{Ker}\rho_i = 1$, then $G \cong \rho_i(G)$ is abelian, so C cannot have size greater than 1, a contradiction. Therefore, $\operatorname{Ker}\rho_i$ 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 $\chi_{\text{reg}} = \sum_i d_i\chi_i$ and $\chi_{\text{reg}}(g) = 0$ 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. □

Proof. (of Burnside's pq-theorem) We induct on $|G|$. The statement is already known if $p = q$ or $a = 0$ or $b = 0$, so we can assume that $p \neq q$ and $a, b > 0$.

Let $Q \subset G$ be a Sylow q-subgroup, let $g \in Q$ be a non-trivial central element in Q, and let $H = Z_G(g) \subset G$. Then $Q \subset H$, so $|C(g)| = [G : H] \mid [G : Q] = p^a$, so $|C(g)|$ is a power of p.

If $|C(g)| = 1$, then $g \in Z(G)$, so $Z(G) \subset G$ is non-trivial. By induction, the group $G/Z(G)$ is solvable, so is G.

If $|C(g)| > 1$, then by the proposition, G is not simple, hence there is a proper normal subgroup N in G. By induction the groups N and G/N are solvable, so is G. $\square$

5 Algebras

5.1 Definitions

Let R be a commutative ring. Let S be a set together with the three operations:
Addition: $S \times S \to S, \quad (x, y) \mapsto x + y,$
Multiplication: $S \times S \to S, \quad (x, y) \mapsto x \cdot y,$
Scalar multiplication: $R \times S \to S, \quad (a, x) \mapsto ax.$
We say that S is an *R-algebra* if $(S, +, \cdot)$ is a ring, $(S, +, \ )$ is an R-module and
$a(x \cdot y) = (ax) \cdot y = x \cdot (ay)$ for all $a \in R$ and $x, y \in S$.
Let S be an R-algebra. We define a map

$$\varphi : R \to S, \quad \varphi(a) = a1_S.$$

Claim: φ is a ring homomorphism and $\mathrm{Im}(\varphi)$ is contained in the center of S.

Proof. We have $\varphi(a + b) = (a + b)1_S = a1_S + b1_S = \varphi(a) + \varphi(b)$ by distributivity,
$\varphi(a \cdot b) = (a \cdot b)1_S = a(b1_S) = a(1_S \cdot b1_S) = (a1_S) \cdot (b1_S) = \varphi(a) \cdot \varphi(b)$
and $\varphi(1_R) = 1_R 1_S = 1_S$, so φ is a ring homomorphism.
Let $a \in R$ and $x \in S$. We have
$x \cdot (a1_S) = (ax) \cdot 1_S = ax = a(1_S \cdot x) = (a1_S) \cdot x.$
Conversely, let $\varphi : R \to S$ be a ring homomorphism such that $\mathrm{Im}(\varphi)$ is contained in the center of S. We make S an R-algebra as follows. If $a \in R$ and $x \in S$, we set $ax := \varphi(a) \cdot x$. Clearly, S is an R-module. We have
$a(x \cdot y) = \varphi(a) \cdot (x \cdot y) = (\varphi(a) \cdot x) \cdot y = (ax) \cdot y$ and
$(ax) \cdot y = (\varphi(a) \cdot x) \cdot y = (x \cdot \varphi(a)) \cdot y = x \cdot (\varphi(a) \cdot y) = x \cdot (ay).$ □

Example 5.1.1. 1. Every ring is a $\mathbb{Z}$-algebra is a unique way.

2. Every ring is an algebra over its center.

3. The polynomial ring $R[x]$ is an R-algebra.

4. The matrix ring $M_n(R)$ is an R-algebra.

5. If G is a group, the group ring $R[G]$ is an R-algebra.

An *R-algebra homomorphism* is a map of R-algebras that is a ring and R-module homomorphism.

Denote by R-**Alg** the category of R-algebras whose morphisms are R-algebra homomorphisms. It has the full subcategory R-**CAlg** of commutative algebras. In R-**Alg** and R-**CAlg**, the initial object is R and the terminal object is 0. In R-**Alg** and R-**CAlg**, the Cartesian product coincides with the categorical product.

If A and B are two R-algebras, we define an R-algebra structure on the tensor product $A \otimes_R B$ of R-modules given by $(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2)$.

Here are some basic properties of the tensor product:

1. The R-algebras $A \otimes_R B$ and $B \otimes_R A$ are canonically isomorphic.
2. $(A \otimes_R B) \otimes_R C \simeq A \otimes_R (B \otimes_R C)$.
3. $A \otimes_R R \simeq A \simeq R \otimes_R A$.
4. $M_n(R) \otimes_R A \simeq M_n(A)$.
5. $M_n(R) \otimes_R M_m(R) \simeq M_{nm}(R)$.

In R-**CAlg**, the tensor product $A \otimes_R B$ coincides with the categorical coproduct of A and B.

Proposition 5.1.2. *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 $f : A \to B$ be a homomorphism of R-algebras. Then $1_S \otimes f : S \otimes_R A \to S \otimes_R B$ is a homomorphism of S-algebras, so we have a functor R-**Alg** $\to S$-**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. Recall that $A \otimes_F M_n(F) \cong M_n(A)$ as F-algebras and $M_n(F) \otimes_F M_m(F) \cong M_{nm}(F)$. 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 $F \to A$ 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 $B \neq 0$ and $B \mapsto A \otimes_F B$ given by $b \mapsto 1_A \otimes b$ is injective if $B \neq 0$. Note that the images of A and B in $A \otimes_F B$ commute element-wise.

If $A' \subset A$ and $B' \subset B$ are F-subalgebras, then $A' \otimes_F B'$ is a subalgebra of $A \otimes_F B$.

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 5.2.1. $C_A(F) = A$ and $C_A(A) = Z(A)$.

Lemma 5.2.2. *Let $S \subset A$ and $T \subset B$ be two subalgebras. Then*

$$C_{A \otimes_F B}(S \otimes_F T) = C_A(S) \otimes_F C_B(T) \quad \textit{in} \quad A \otimes_F B.$$

Proof. Let $x = \sum a_i \otimes b_i \in C_{A\otimes_F B}(S \otimes_F T)$, where $\{b_i\}$ is a basis for B. For every $s \in S$ we have

$$0 = (s \otimes 1)x - x(s \otimes 1) = \sum (sa_i - a_i s) \otimes b_i,$$

hence $sa_i = a_i s$ for all i and $s \in S$. Therefore, $a_i \in C_A(S)$ and hence $x \in C_A(S) \otimes_F B$. Rewriting x we may assume that the a_i's are linearly independent. For every $t \in T$ we have

$$0 = (1 \otimes t)x - x(1 \otimes t) = \sum a_i \otimes (tb_i - b_i t).$$

Then $tb_i = b_i t$ for all i and $t \in T$, therefore, $b_i \in C_B(T)$, hence $x \in C_A(S) \otimes_F C_B(T)$. The other inclusion is clear. $\square$

Corollary 5.2.3. *$C_{A\otimes_F B}(A) = Z(A) \otimes_F B$ and $C_{A\otimes_F B}(B) = A \otimes_F Z(B)$.*

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

Corollary 5.2.4. *If A and B are central F-algebras, then $C_{A\otimes_F B}(A) = B$ and $C_{A\otimes_F B}(B) = A$.*

Corollary 5.2.5. *$Z(A \otimes_F B) = Z(A) \otimes_F Z(B)$. If both A and B are central F-algebras, then so is $A \otimes_F B$.*

Example 5.2.6. $Z(M_n(A)) = Z(M_n(F) \otimes_F A) = Z(M_n(F)) \otimes_F Z(A) = F \otimes_F A = Z(A)$.

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 5.2.7. *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 $I = \operatorname{Ker} f \subset A$. 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. $\square$

Proposition 5.2.8. *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. Write a non-zero element $c \in I$ in the form $c = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ with n as small as possible. Note that the b_i's are linearly independent. 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 the element

$$\sum_{j=1}^{m} (y_j \otimes 1_B) \cdot c \cdot (z_j \otimes 1_B) = \sum_{i,j} (y_j a_i z_j) \otimes b_i =$$

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} y_j a_i z_j\right) \otimes b_i = 1 \otimes b_1 + a_2' \otimes b_2 + \cdots + a_n' \otimes b_n$$

is in I and is non-zero (since the b_i's are linearly independent). Hence we can suppose that $a_1 = 1$ in the original expression for c.

For $a \in A$, we have

$$(a \otimes 1_B)c - c(a \otimes 1_B) = \sum_{i \geq 2}^{n} (aa_i - a_i a) \otimes b_i \in I.$$

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, $BbB = B$. Write $1 = \sum_k u_k b v_k$. Then

$$\sum_k (1_A \otimes u_k) \cdot c \cdot (1_A \otimes v_k) = 1_A \otimes 1_B = 1_{A \otimes B} \in I.$$ □

Corollary 5.2.9. *If A and B are central simple F-algebras, then so is $A \otimes_F B$.*

Example 5.2.10. If A is a central (simple) F-algebra, then so in the *opposite* algebra A^{op}.

5.3 Representations over non-closed fields

If F is a field and K/F a field extension. If V is a vector space over F, then the tensor product $V_K := V \otimes_F K$ is a vector space over K, moreover, $\dim_K(V_K) = \dim_F(V)$. If $W \subset V$ is a subspace over F, then $W_K \subset V_K$ is a subspace over K since tensor product functor over a field is exact.

If A is an F-algebra, then A_K is a K-algebra. If M is a (left) A-module, then M_K is a (left) A_K-module.

Lemma 5.3.1. *Let G be a finite group and let V be a G-space. Then $(V^G)_K = (V_K)^G$ as subspaces of V_K.*

Proof. We have an exact sequence

$$0 \to V^G \to V \to \prod_{g \in G} V,$$

where the last map takes v to the tuple $(gv - v)_{g \in G}$. Tensoring with K over F, we get an exact sequence

$$0 \to (V^G)_K \to V_K \to \prod_{g \in G} V_K,$$

hence $(V^G)_K = (V_K)^G$. □

Example 5.3.2. Let L/F be a finite separable field extension and K/F be a field extension. We can write $L = F[x]/(f)$, where f is an irreducible separable polynomial over 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 $L \otimes_F K \cong K^{[L:F]}$.

Lemma 5.3.3. *Let V and W be two G-spaces and K/F a field extension. Then the natural homomorphism*

$$\mathrm{Hom}_G(V, W)_K \to \mathrm{Hom}_G(V_K, W_K)$$

is an isomorphism.

Proof. The natural map $\mathrm{Hom}_F(V, W)_K \to \mathrm{Hom}_K(V_K, W_K)$ is an isomorphism, hence

$$\mathrm{Hom}_G(V, W)_K = (\mathrm{Hom}_F(V, W)_K)^G \simeq \mathrm{Hom}_K(V_K, W_K)^G = \mathrm{Hom}_G(V_K, W_K).$$

□

Note that for a G-space V over F, the characters of V and V_K coincide.

Corollary 5.3.4. *Let V and W be two G-spaces. Then*

$$\dim \mathrm{Hom}_G(V, W) = \langle \chi_V, \chi_W \rangle.$$

Proof. By the lemma we may assume that the base field is algebraically closed. By additivity we may assume that V and W are irreducible. The result follows by Schur's Lemma. □

Let D be division finite dimensional F-algebra. We view F as a subring of the center Z of A. Then Z is a field of finite degree over F and we can view D as an algebra over Z.

Let G be a finite group and let F be a field of characteristic zero. Recall that the group algebra $F[G]$ is semisimple and

$$F[G] \simeq M_{k_1}(D_1) \times M_{k_2}(D_2) \times \ldots \times M_{k_m}(D_m),$$

where D_i are division finite dimensional F-algebras. It follows that there are m simple G-spaces $W_1, W_2, \ldots, W_m$ over F with $W_i = (D_i)^{\oplus k_i}$. Recall that we view W_i as a G-space over F (equivalently, an $F[G]$-module) via the projection $F[G] \to M_{k_i}(D_i)$.

Take one of the simple G-spaces $W = W_i$ over F. Recall that $D := D_i = \mathrm{End}_G(W)$. Let Z be the center of D, so Z/F is a finite field extension. The degree $t := [Z : F] \geq 1$ is called the *decomposition index* of W. The decomposition index is equal to 1 is and only if $Z = F$, i.e., the algebra D is central.

Let K be an algebraically closed field containing Z. Since D is central over Z, $D \otimes_Z K$ is a simple K-algebra, hence $D \otimes_Z K \simeq M_s(K)$ for some $s \geq 1$. In fact, $s^2 = \dim_Z(D)$. We call the integer s the *Schur index* of W. The Schur index is equal to 1 if and only if D is commutative.

Proposition 5.3.5. *Let W be a simple G-space over F and K/F a field extension with K algebraically closed. Then*

$$W_K \simeq V_1^{\oplus s} \oplus V_2^{\oplus s} \oplus \ldots \oplus V_t^{\oplus s}$$

for some pairwise non-isomorphic simple G-spaces $V_1, V_2, \ldots, V_t$ over F of the same dimension, where t and s are decomposition and Schur indices of W respectively.

Proof. Let Z be the center of $D = \mathrm{End}_G(W)$. We may assume that $Z \subset K$. By Example, $Z \otimes_F K \simeq K^t$, where $t = [Z : F]$. We have

$$D \otimes_F K = D \otimes_Z (Z \otimes_F K) = (D \otimes_Z K)^t = M_s(K)^t.$$

As $M_k(D)$ is a direct factor of $F[G]$ for some k, the K-algebra

$$M_{ks}(K)^t = M_k(D) \otimes_F K$$

is a direct factor of $K[G]$. Each copy of $M_{ks}(K)$ corresponds to a simple G-space V_j, $j = 1, 2, \ldots t$, of dimension ks. Moreover, $(V_j)^{\oplus ks} \simeq M_{ks}(K)$ as G-spaces. As $W^{\oplus k} \simeq M_k(D)$, we have

$$W_K^{\oplus k} \simeq M_k(D) \otimes_F K \simeq M_{ks}(K)^t \simeq \bigoplus V_j^{\oplus ks}$$

and the result follows by cancellation. □

Remark 5.3.6. It follows from the proof that the simple components V_i of W_K for distinct simple $F[G]$-modules W are distinct. It follows that if W and W' are G-spaces over F such that $W_K \simeq W'_K$, then $W \simeq W'$. Moreover, every simple G-module V over K is a direct summand of W_K for a (unique) simple G-space W.

Example 5.3.7. Let G be a cyclic group of order n and $F = \mathbb{Q}$. We know that

$$\mathbb{Q}[G] \cong \prod_{d|n} \mathbb{Q}[t]/(\Phi_d(t)) \cong \prod_{d|n} \mathbb{Q}(\zeta_d).$$

Each field $\mathbb{Q}(\zeta_d)$ can be viewed as a simple G-space, where the generator of G acts via multiplication by ζ_d. The decomposition index is equal to $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \varphi(d)$ and Schur index is 1.

Example 5.3.8. Let $G = Q_8 = \{1, \varepsilon, i, \varepsilon i, j, \varepsilon j, ij, \varepsilon ij\}$, where ε is in the center and $F = \mathbb{R}$. Consider the central idempotent $e = \frac{1}{2}(1 + \varepsilon)$. We have $F[G] = eF[G] \times fF[G]$ with $f = 1 - e$. The map

$$F[G] \to eF[G] \simeq F[G/(\varepsilon)] = F \times F \times F \times F$$

is trivial on $fF[G]$ and an isomorphism on $fF[G]$.

Let $\mathbb{H}$ be the classical division Hamilton quaternion algebra with basis $\{1, I, J, IJ\}$. The inclusion of G into $\mathbb{H}^\times$ taking i to I, j to J and ε to -1 yields a map $F[G] \to \mathbb{H}$ that takes $eF[G]$ to zero and it is an isomorphism on $fF[G]$. Hence

$$F[G] \simeq F \times F \times F \times F \times \mathbb{H}.$$

Therefore, $\mathbb{H}$ is a simple G-space over F of dimension 4 with decomposition index 1 and Schur index 2, so $\mathbb{H}_\mathbb{C} \simeq V \oplus V$ where V is (the only) 2-dimensional simple G-space over $\mathbb{C}$. The same holds over any subfield $F \subset \mathbb{R}$, for example, over $\mathbb{Q}$.

Proposition 5.3.9. *Let W be a simple G-space over F and K/F a field extension with K algebraically closed and let V be a simple direct summand of W_K over K. Then the following are equivalent:*

(1) *The decomposition index of W is equal to* 1 *(i.e., $W_K \simeq V^{\oplus s}$);*

(2) *All values of the character of V are contained in F;*

Proof. (1) ⇒ (2) If $W_K \simeq V^{\oplus s}$, then $\chi_W = \chi_{W_K} = s \cdot \chi_V$ has values in F, hence χ_V has values in F.

(2) ⇒ (1) Let

$$e = \frac{d}{n} \sum_{g \in G} \chi_V(g^{-1}) g \in F[G] \subset K[G],$$

where $d = \dim(V)$. We know that V is a simple $eK[G]$-module, hence e is a central idempotent of $K[G]$ and V is a $K[G]$-module via the projection $K[G] \to eK[G]$.

As K is algebraically closed, $eK[G] \simeq M_d(K)$ is a central simple algebra. Since $(eF[G])_K = eK[G]$, the F-algebra $eF[G]$ is also simple. Let W' be a simple G-space over F via the projection $F[G] \to eF[G]$. In particular, $eF[G] \simeq M_p(D)$ for some p, where $D = \operatorname{End}_G(W')$ is a division F-algebra. Since $M_p(D)_K \simeq (eF[G])_K = eK[G] \simeq M_d(K)$ is central, the F-algebra D is central, i.e., the decomposition index of W' is 1. It follows that $W'_K \simeq V^{\oplus s}$ for some s. Since V is the common simple direct summand of both W_K and W'_K over K, by the remark above, $W \simeq W'$, hence the decomposition index of W is equal to 1. □

Definition 5.3.10. Let K/F be a field extension and V a G-space over K. We say that V *is defined over* F if there is a G-space W over F such that $V \simeq W_K$. An an irreducible G-space W over F is called *absolutely irreducible* if W_K is irreducible for every field extension K/F.

Example 5.3.11.

1. One-dimensional representations are absolutely irreducible.
2. Let V be (the only)simple 2-dimensional Q_8-space over $\mathbb{C}$. Then $V \oplus V$ is defined over $\mathbb{R}$ but V is not defined over $\mathbb{R}$.

Proposition 5.3.12. *Let G be a finite group and F a field of characteristic zero. The following are equivalent.*

(1) *Every irreducible representation of G is absolutely irreducible;*

(2) *For every irreducible G-space V, the F-algebra $\operatorname{End}_G(V)$ is equal to F;*

(3) *For every irreducible representation of G we have $t = 1 = s$;*

(4) *For any field extension L/F every representation of G over L is defined over F;*

(4′) *For any algebraically closed field extension K/F every representation of G over K is defined over F;*

(5) $F[G] = M_{d_1}(F) \times \cdots \times M_{d_r}(F)$ *for some $d_i \geq 1$.*

Proof. (1) ⇒ (2) Let V be an irreducible G-space and $D = \operatorname{End}_G(V)$. Let K/F be a field extension with K algebraically closed. Since V_K is irreducible, by Schur's Lemma,

$$D_K \simeq \operatorname{End}_G(V_K) = K.$$

It follows that $D = F$.

(2) $\Rightarrow$ (3) Let V be an irreducible G-space. Then $\mathrm{End}_G(V) = F$ and hence $t = 1 = s$.

(3) $\Rightarrow$ (4) It suffices to show that every irreducible G-space U over L is defined over F. Let K be a field extension of L that is algebraically closed. Let V be an irreducible direct summand of $U_K = U \otimes_L K$. Let W be an irreducible G-space over F such that V is a direct summand of $W_K = W \otimes_F K$. As $t = 1 = s$ for W, we have $W_K = M$. It follows that W_L is irreducible. Thus, W_L and U are two irreducible G-spaces over L that have the same irreducible direct summand V over K. It follows that $W_L \simeq U$, i.e., U is defined over F.

(4) $\Rightarrow$ (4′) is trivial.

(4′) $\Rightarrow$ (1) Let W be an irreducible G-space over F and K/F a field extension. We want to prove that W_K is irreducible. We can change K by a larger field, so we may assume that K is algebraically closed.

Let V be an irreducible direct summand of W_K. As V is defined over F, there is a G-space W' over F such that $W'_K \simeq V$. Clearly W' is irreducible. As $\mathrm{Hom}_G(W, W') \otimes_F K = \mathrm{Hom}_G(W_K, W'_K) = \mathrm{Hom}_G(W_K, V) \neq 0$, we have $\mathrm{Hom}_G(W, W') \neq 0$ and hence by Schur's Lemma, $W \simeq W'$ and therefore, $W_K \simeq W'_K \simeq V$ is irreducible.

(5) $\Rightarrow$ (1) All irreducible G-spaces are F^{d_i}. As for any field extension K/F, we have $K[G] = F[G] \otimes_F K = M_{d_1}(K) \times \cdots \times M_{d_r}(K)$, all irreducible G-spaces over K are $K^{d_i} = F^{d_i} \otimes_F K$, hence the G-spaces F^{d_i} are absolutely irreducible.

(3) $\Rightarrow$ (5) Write $F[G] \simeq M_{k_1}(D_1) \times M_{k_2}(D_2) \times \ldots \times M_{k_m}(D_m)$. Let Z_i be the center of D_i. By assumption $[Z_i : F] = t_i = 1$ and $\dim_{Z_i}(D_i) = s_i^2 = 1$, hence $D_i = F$ for all i. □

Definition 5.3.13. Let G be a finite group. A field F of characteristic 0 is called a *splitting field of* G or G *is split over* F if the equivalent conditions (1) − (5) of the proposition hold.

Example 5.3.14.

1. Algebraically closed fields are splitting fields of any finite group G.
2. Let $G = Q_8$ over $\mathbb{Q}$. Then the field $\mathbb{Q}(i)$ is a splitting field of G.
3. Let G be a finite group and F a field of characteristic 0. Then there is a finite field extension K/F such that G is split over K. Indeed, we can take the field generated by the entries of all irreducible matrix representations over an algebraic closure of F.
4. Symmetric groups S_n are split over $\mathbb{Q}$.
5. If m is the exponent of G (the smallest positive integer such that $g^m = 1$ for all $g \in G$), the cyclotomic field extension F_m/F is a splitting field of G.

Let $Rep_F(G)$ be the representation ring of a finite group G over a field F of characteristic zero. For a representation ρ of G over F write $[\rho]$ its class in $Rep_F(G)$. The ring operations are defined by $[\rho] + [\mu] = [\rho \oplus \mu]$ and $[\rho] \cdot [\mu] = [\rho \otimes \mu]$.

As a group, $Rep_F(G)$ is a free abelian group with basis the set of isomorphism classes of irreducible representations of G over F. We can identify $Rep_F(G)$ with the subgroup of $\mathrm{Ch}(G)$ generated by the characters of representations of G over F. Note that $\rho \simeq \mu$ if and only if $[\rho] = [\mu]$.

Let K/F be a field extension. We have a ring homomorphism $Rep_F(G) \to Rep_K(G)$ taking $[\rho]$ to $[\rho_K]$. Recall that if K is algebraically closed and ρ is an irreducible representation of G over F, then

$\rho_K = \rho_1^{\oplus s} \oplus \ldots \oplus \rho_d^{\oplus s}$, where ρ_i are irreducible representations of G over K. Moreover, the sets of ρ_i for different irreducible ρ don't intersect. It follows that the homomorphism $Rep_F(G) \to Rep_K(G)$ is injective. Moreover, the map $Rep_F(G) \to Rep_K(G)$ is an isomorphism if and only if $d = 1 = s$ for all ρ if and only if G is split over F by the proposition above.

We will use the following theorem.

Theorem 5.3.15. *(Brauer) Let G be a finite group and F an algebraically closed field of characteristic zero. Then the group $Rep_F(G)$ is generated by the classes of induced representations $Ind_H^G(\chi)$ over all subgroups $H \subset G$ and one-dimensional representations χ of H.*

Suppose F contains all roots of unity of degree m the exponent of G. Choose an algebraically closed field extension K/F. We will show that G is split over F by proving that the map $Rep_F(G) \to Rep_K(G)$ is an isomorphism.

By Brauer's theorem, $Rep_K(G)$ is generated by the classes of $Ind_H^G(\chi)$, where χ is one-dimensional, i.e., $\chi : H \to K^\times$ is a homomorphism. By assumption on the roots of unity, the image of χ is contained in $F^\times$, hence χ is defined over F, hence the map $Rep_F(G) \to Rep_K(G)$ is surjective.

5.4 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 5.4.1. *This is an equivalence relation.*

Proposition 5.4.2. *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, $M_{n_2}(A_1) \cong M_{n_1 n_2}(D_1) \cong M_{n_1 n_2}(D_2) \cong M_{n_1}(A_2)$, so $A_1 \sim A_2$. □

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 $\mathrm{Br}(F)$ for the set of equivalence classes with operation $[A][B] = [A \otimes_F B]$. The operation is well defined: if $A_1 \sim A_2$, i.e., $M_{s_1}(A_1) \cong M_{s_2}(A_2)$ and $B_1 \sim B_2$, i.e., $M_{t_1}(B_1) \cong M_{t_2}(B_2)$, then

$$M_{s_1 t_1}(A_1 \otimes_F B_1) \cong M_{s_1}(A_1) \otimes_F M_{t_1}(B_1) \cong M_{s_2}(A_2) \otimes_F M_{t_2}(B_2) \cong M_{s_2 t_2}(A_2 \otimes_F B_2),$$

i.e., $A_1 \otimes_F B_1 \sim A_2 \otimes_F B_2$.

Theorem 5.4.3. *The set $\mathrm{Br}(F)$ is an abelian group.*

Proof. The operation is obviously commutative and associative. The class $[F]$ is the identity. Let A be a central simple algebra of finite dimension over F. We show that $[A]^{-1} = [A^{op}]$. Consider a map

$$f : A \otimes_F A^{op} \to \mathrm{End}_F(A), \quad f(x \otimes y^{op})(a) = xay.$$

This is a homomorphism of simple F-algebras of the same dimension, hence f is an isomorphism. It follows that $[A][A^{op}] = [\mathrm{End}_F(A)] = [F] = 1$. □

Definition 5.4.4 (Brauer group)**.** The abelian group $\mathrm{Br}(F)$ is the *Brauer group* of F.

Remark 5.4.5. Every class $[A]$ in $\mathrm{Br}(F)$ contains a central division algebra that is unique up to isomorphism. Thus, we have a bijection between the set $\mathrm{Br}(F)$ and the set of isomorphism classes of central division F-algebras of finite dimension. It follows that two central simple F-algebras A and B are isomorphic if and only if $[A] = [B]$ in $\mathrm{Br}(F)$ and $\dim(A) = \dim(B)$.

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

Example 5.4.6. If F is algebraically closed, then $\mathrm{Br}(F) = 1$.

Theorem 5.4.7. *If F is a finite field, then* $\mathrm{Br}(F) = 1$.

Proof. Let $F = \mathbb{F}_q$ and let A be a central division F-algebra of finite dimension. We show that $A = F$.

Suppose $\dim_F A = n$, so $|A| = q^n$. Hence $|A^\times| = q^n - 1$. For any $a \in A$ non-zero, the centralizer $C_A(a) \subset A$ is a subspace, so $|C_A(a)| = q^k$ for some k, hence $|C_{A^\times}(a)| = q^k - 1$. Note that k divide n as $\frac{n}{k}$ is the rank of A as a module over the division algebra $C_A(a)$. 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. As $A^\times$ is the disjoint union of conjugacy classes, we have

$$q^n - 1 = \sum_{k<n} \frac{q^n - 1}{q^k - 1} + (q - 1).$$

If k divides n and $k < n$, the polynomial $\frac{x^n-1}{x^k-1}$ is divisible by the cyclotomic polynomial $\Phi_n(x)$, hence $\Phi_n(q)$ divides $\frac{q^n-1}{q^k-1}$. It follows that $\Phi_n(q)$ divides $q - 1$, hence $|\Phi_n(q)| \leq q - 1$.

On the other hand $\Phi_n(x) = \prod(x - \xi)$, where the product is taken over all primitive n-th roots of unity ξ, hence $\Phi_n(q) = \prod(q - \xi)$. As $|q - \xi| \geq q - 1 \geq 1$, we must have $n = 1$. □

Example 5.4.8. The quaternion algebra $\mathbb{H}$ is a central $\mathbb{R}$-algebra of dimension 4, so $\mathrm{Br}(\mathbb{R}) \neq 1$. If F is a field of characteristic not 2 and $a, b \in F^\times$. The F-algebra $(a, b)_F$ with basis $\{1, i, j, k\}$ and multiplication table $i^2 = a$, $j^2 = b$ and $k = ij = -ji$ is called the *(generalized) quaternion algebra*. We will see that $(a, b)_F$ is a central simple algebra over F.

Example 5.4.9. An *anti-automorphism* of an F-algebra A is a linear automorphism $\sigma : A \to A$ such that $\sigma(x+y) = \sigma(x)+\sigma(y)$ and $\sigma(xy) = \sigma(y)\sigma(x)$ for all $x, y \in A$. An anti-automorphism σ can be viewed as an isomorphism between A and A^{op}. If an anti-automorphism σ satisfies $\sigma \circ \sigma = Id_A$, we say that σ is an *involution*.

If A is a central simple F-algebra that admits an anti-automorphism, then $A \simeq A^{op}$ and hence $[A]^{-1} = [A]$ in $\mathrm{Br}(F)$.

Theorem 5.4.10 (Noether-Skolem)**.** *Let A be a finite-dimensional central simple algebra over F and let $S, T \subset A$ 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 $(A^{\mathrm{op}} \otimes_F S)$-module in two ways. First, we define

$$a \cdot (b^{\mathrm{op}} \otimes s) = bas.$$

Second, we define
$$a \star (b^{\mathrm{op}} \otimes s) = baf(s).$$
Since S is simple and A^{op} is central simple, $A^{\mathrm{op}} \otimes_F S$ is simple. Over a simple algebra every two right modules of the same dimension are isomorphic. Therefore, the two module structures are isomorphic. Let $g : A \to A$ be an isomorphism, so that
$$g(bas) = bg(a)f(s)$$
for all $a, b \in A$ and $s \in S$. For $a = s = 1$, we get $g(b) = bg(1)$. As g is an isomorphism, this implies $g(1)$ is left invertible, hence right invertible since A has finite dimension over F. For $a = b = 1$, we get $sg(1) = g(s) = g(1)f(s)$, so $f(s) = g(1)^{-1}sg(1)$, as required. $\square$

Remark 5.4.11. 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 $\mathrm{Aut}_{F\text{-alg}}(A) \cong A^\times/F^\times$ for the F-algebra automorphism group, with the action by conjugation. If $A = M_n(F)$, then $A^\times = GL_n(F)$ and $\mathrm{Aut}_{F\text{-alg}}(M_n(F)) = GL_n(F)/F^\times = PGL_n(F)$.

Example 5.4.12. Let S be an F-algebra and $B = \mathrm{End}_F(S)$. Then $S \subset B$ by left multiplication and $S^{\mathrm{op}} \subset B$ by right multiplication. In fact, $S^{\mathrm{op}} = C_B(S)$ and $S = C_B(S^{\mathrm{op}})$. Indeed, $f \in C_B(S)$ if and only if $f(ax) = af(x)$ for all $a, x \in A$. Plugging $x = 1$, we get $f(a) = af(1)$, i.e., f is right multiplication by $f(1)$. Conversely, if $f(a) = ab$ for some $b \in A$, then $f(ax) = (ax)b = a(xb) = af(x)$, i.e., $f \in C_B(S)$.

Theorem 5.4.13 (Double centralizer theorem)**.** *Let A be a central simple algebra over F and let $S \subset A$ be a simple subalgebra. Then*

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 $S \subset B = \mathrm{End}_F(S)$. Then $C_B(S) = S^{\mathrm{op}}$. We have
$$S = S \otimes F \subset A \otimes_F B \quad \text{and} \quad S = F \otimes_F S \subset A \otimes_F B.$$
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
$$C_{A\otimes B}(F \otimes S) = C_A(F) \otimes C_B(S) = A \otimes S^{\mathrm{op}},$$
which is simple. By Noether-Skolem, $S \otimes F$ and $F \otimes S$ are conjugate. Hence their centralizers $C_A(S) \otimes B$ and $A \otimes S^{\mathrm{op}}$ are conjugate, hence isomorphic. As $A \otimes S^{\mathrm{op}}$ is simple, so is $C_A(S) \otimes B$ and hence $C_A(S)$ 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 $(\dim C_A(S))(\dim B) = (\dim A)(\dim S^{\mathrm{op}})$, 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 5.4.14. *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 $f : S \otimes_F C_A(S) \to A$ given by $f(x \otimes y) = xy$. By the theorem, $S \otimes_F C_A(S)$ is a simple F-algebra of the same dimension as A. Hence f is an isomorphism. $\square$

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 $\mathrm{Br}(F) \to \mathrm{Br}(L)$ given by extension of scalars $[A] \mapsto [A_L]$.

Proposition 5.4.15. *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 $\deg M_k(A) = k \deg A$. If L/F is a field extension, $\deg A_L = deg A$.

Let A be a central simple algebra over F with $A \cong M_k(D)$ for D some central division F-algebra. If $m = \deg D$ and $n = \deg A$, then $n = km$. The value m is the *(Schur) index* of A, denoted $\operatorname{ind} A$. From the definition, $\operatorname{ind} A \mid \deg A$, 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 $\operatorname{ind} A = \deg D = \operatorname{ind} B$, so we can define $\operatorname{ind}([A]) = \operatorname{ind} A$. We have $[A] = 1$ if and only if $\operatorname{ind}([A]) = 1$.

5.5 Maximal subfields

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

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

Proof. ($\Longrightarrow$) Suppose $\alpha \in C_D(L)$. Then $L \subset L[\alpha] \subset D$ and $L[\alpha]$ is a subfield of D, so $L[\alpha] = L$.

($\Longleftarrow$) Let $L' \subset D$ be a subfield containing L. Then $L' \subset C_D(L) = L$, so $L' = L$. $\square$

Corollary 5.5.2. *Let L be a maximal subfield of a central division F-algebra D. Then $[L : F] = \deg D$.*

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

Corollary 5.5.3. *Let L be a subfield of D. Then $[L : F]$ divides $\deg D$.*

Proof. There is a maximal subfield L' of D containing L. Hence $[L : F]$ divides $[L' : F] = \deg D$. $\square$

Example 5.5.4. Let D be a finite division ring. Then $F = Z(D)$ is a finite field and D is central as an F-algebra. Let L be a maximal subfield of D. Let $\alpha \in D^\times$ and L' a maximal subfield of D containing α. Then $[L : F] = \deg D = [L' : F]$. As F is a finite field, the fields L and L' are isomorphic over F, hence conjugate by Noether-Skolem. It follows that $\alpha \in \beta L^\times \beta^{-1}$ for some $\beta \in D^\times$.

We have proved 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 5.5.5 (Splitting field)**.** A central simple F-algebra A is *split over* F if $A \cong M_n(F)$ for $n = \deg A$. Let A be a central simple F-algebra and K/F a field extension. We say that K is a *splitting field* of A (or A *is split over* K) if A_K is split over K.

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

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

Remark 5.5.6. 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. $\square$

Theorem 5.5.7. *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 $f : A \otimes_F L \to \operatorname{End}_L(A) \cong M_n(L)$ with A viewed as a right L-module by $f(a \otimes l)(m) = aml$. $\square$

Corollary 5.5.8. *Every maximal subfield of a central division algebra D is a splitting field of D.*

Corollary 5.5.9. *Every central simple algebra A over F has a splitting field L such that $[L : F] = \operatorname{ind} A$.*

Proof. Write $A = M_s(D)$ for a central division algebra D of degree $n = \operatorname{ind} A$. 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 and $[F[\alpha] : F] < \infty$, so α is algebraic over F.

Lemma 5.5.10. *Let D be a central division F-algebra with $D \neq F$. Then there exists $\alpha \in D \backslash F$ which is separable over F.*

Proof. If F is perfect, then we are done.

Otherwise F is infinite and $p = \operatorname{char} F > 0$. Suppose all $\alpha \in D\backslash F$ are not separable. Pick a maximal subfield $L \subset D$ containing α, so L/F is purely inseparable. Then

$$\alpha^{p^n} \in L^{p^n} \subset F,$$

where $p^n = [L : F] = \deg D$. It follows that $D^{p^n} \subset F$.

Choose a basis $\{d_1 = 1, d_2, \ldots, d_m\}$ for D over F. Let $x = (x_1, x_2, \ldots, x_m)$ be variables. We have

$$\Big(\sum_{i=1}^{m} d_i x_i\Big)^{p^n} = \sum_{i=1}^{m} d_i f_i(x)$$

for (unique) polynomials $f_1, f_2, \ldots, f_m \in F[x]$.

Let $a = (a_1, a_2, \ldots, a_m) \in F^m$. Plugging in $x_i = a_i$ we have $f_i(a) = 0$ for all $i > 1$ since $d_1 = 1$ and $D^{p^n} \subset F$. Since F is infinite, $f_i = 0$ for all $i > 1$.

Let L/F be field extension and $b = (b_1, b_2, \ldots, b_m) \in L^m$. Plugging in $x_i = b_i$ we get

$$\Big(\sum_{i=1}^{m} d_i b_i\Big)^{p^n} = d_1 f_1(b) = f_1(b) \in L.$$

(We view D and L as subalgebras in D_L.) It follows that $(D_L)^{p^n} \subset L$.

Now take for L a splitting field for D, so that $D_L \simeq M_k(L)$ for some $k > 1$. But $(e_{1,1})^{p^n} = e_{1,1}$ is not a scalar matrix, so it is not contained in L, a contradiction. □

Corollary 5.5.11. *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 $L \neq C_D(L)$, since $C_D(L)$ is a central division L-algebra, by the lemma, there exists $\alpha \in C_D(L) \setminus L$ such that $L(\alpha)/L$ is nontrivial and separable, but then $L(\alpha)/F$ is separable, contradicting maximality of L as a separable extension. □

Corollary 5.5.12. *Every central simple F-algebra is split by a (finite) separable extension of F.*

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. $\square$

Example 5.5.13. If F is separably closed, i.e. it has no non-trivial separable extensions, then $\mathrm{Br}(F) = 1$. One can construct the separable closure of a field by taking all separable elements in an algebraic closure.

Theorem 5.5.14. *Let A be a central simple F-algebra and K/F be a field extension.*

1. $\operatorname{ind}(A_K) \mid \operatorname{ind}(A)$*;*

2. If K/F is a finite field extension, then $\operatorname{ind}(A) \mid [K : F] \cdot \operatorname{ind}(A_K)$*. Moreover, if $A_K = M_s(D)$ for a central division K-algebra D, then $D \hookrightarrow M_p(A)$ for*
$p = [K : F] \operatorname{ind}(A_K)/\operatorname{ind}(A)$*.*

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

2. First suppose A is a division algebra. Let $r = [K : F]$ and consider the embedding $K \hookrightarrow \mathrm{End}_F(K) = M_r(F)$ via left multiplications. Therefore,

$$M_s(F) \subset M_s(D) \simeq A_K = A \otimes K \hookrightarrow A \otimes M_r(F) = M_r(A).$$

Let $C = C_{M_r(A)}(M_s(F))$. Since $M_s(F)$ and $M_r(A)$ are central simple algebras, C is also central simple and we have

$$M_s(C) \simeq M_s(F) \otimes C \simeq M_r(A).$$

As A is a division algebra, we have $C \simeq M_p(A)$, where $p = r/s$. We have

$$s = \deg(A_K)/\deg(D) = \operatorname{ind}(A)/\operatorname{ind}(A_K),$$

hence

$$p = [K : F] \cdot \operatorname{ind}(A_K)/\operatorname{ind}(A),$$

i.e., $\operatorname{ind}(A)$ divides $[K : F] \operatorname{ind}(A_K)$. Note that $D \subset C \simeq M_p(A)$.

In the general case write $A = M_n(E)$ for a division algebra E. We have $\operatorname{ind}(E) = \operatorname{ind}(A)$ and $\operatorname{ind}(E_K) = \operatorname{ind}(A_K)$. Also, by the above, $D \hookrightarrow M_p(E) \subset M_p(A)$. $\square$

Corollary 5.5.15. *If a finite extension K/F splits a central simple F-algebra A, then* $\operatorname{ind}(A) \mid [K : F]$.

Corollary 5.5.16. *If A is a central simple F-algebra and K/F is a splitting field for A of degree $r \operatorname{ind}(A)$, then $K \hookrightarrow M_r(A)$. If A is a division algebra and $[K : F] = \operatorname{ind} D$, then K is isomorphic to a maximal subfield of A.*

Let D be a division algebra. Then

$$\boxed{\text{Subfields of } D} \cap \boxed{\text{Splitting fields of } D} = \boxed{\text{Maximal subfields of } D}$$

5.6 Cyclic algebras

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

$$A = (L/F, \sigma, a) = \bigoplus_{i=0}^{n-1} L \cdot u = (L \cdot 1) \oplus (L \cdot u) \oplus (L \cdot u^2) \oplus \ldots \oplus (L \cdot u^{n-1}),$$

where $1, u, \ldots, u^{n-1}$ is a basis for L/F. In particular, $\dim_F(A) = n^2$. 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, $uyu^{-1} = \sigma(y)$. Note that $L = L \cdot 1$ is a subfield of A of degree n over F.

Example 5.6.1.

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

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

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

Proposition 5.6.2. *$A = (L/F, \sigma, a)$ is a central simple algebra.*

Proof. Suppose $s = \sum_i \alpha_i u^i \in Z(A)$, where $\alpha_i \in L$ and let $\beta \in L$. Then

$$0 = \beta s - s\beta = \sum_i (\alpha_i \beta - \alpha_i \sigma^i(\beta)) u^i,$$

hence $\alpha_i(\beta - \sigma^i(\beta)) = 0$ for all i. If $i \neq 0$, then we can choose β so that $\sigma^i(\beta) \neq \beta$, so then $\alpha_i = 0$. Hence $s = \alpha_0 \cdot 1$, so $C_A(L) = L$. From $us = su$, we get $\sigma(\alpha_0) = \alpha_0$. This shows that $\alpha_0 \in F$, so $Z(A) = F$.

Let $0 \neq I \subset A$ be an ideal. We must show that $1 \in I$. Let $s = \sum_i \alpha_i u^i \in I \neq 0$ have the smallest number of non-zero terms. By replacing s with su^k for some k, we can suppose $\alpha_0 \neq 0$. For $\beta \in L$, we have $\beta s - s\beta = \sum_i \alpha_i(\beta - \sigma^i(\beta))u^i \in I$. For $i = 0$, we get 0, so $\beta s - s\beta = 0$. Therefore, $\alpha_i = 0$ for $i \neq 0$, so $s = \alpha_0 \cdot 1$ for $\alpha_0 \in L$ non-zero. Hence $\alpha_0^{-1} s = 1 \in I$. $\square$

Hence A is a central simple algebra of dimension n^2 containing L as a subfield of dimension n over F. In particular, L/F is a splitting field for A, so

$$[A] = \mathrm{Ker}(\mathrm{Br}(F) \to \mathrm{Br}(L)) =: \mathrm{Br}(L/F)$$

(the relative Brauer group). If A is a division algebra, then L is also a maximal subfield of A.

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 5.6.3. *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 σ generating $G = \mathrm{Gal}(L/F)$ 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

$$C(L/F, \sigma, a) \to A \qquad \alpha \in L \mapsto \alpha \in L \subset A$$

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. □

Proposition 5.6.4. *Let L/F be a cyclic extension. Then*

$$\mathrm{Br}(L/F) = \{[C(L/F, \sigma, a)] \mid a \in F^\times\}.$$

Proof. Let $[A] \in \mathrm{Br}(L/F)$ for A a division algebra. Then $\deg(A) = \mathrm{ind}(A) = m$. 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 $M_k(A)$, hence $[A] = [C(L/F, \sigma, a)]$. □

Lemma 5.6.5. $C(L/F, \sigma, 1) \cong M_n(F)$ *for* $n = [L : F]$.

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

Lemma 5.6.6. *Let L/F be a cyclic extension of degree n, $\sigma \in \mathrm{Gal}(L/F)$ 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*
$b/a \in N_{L/F}(L^\times)$.

Proof. ($\Longrightarrow$) 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 $b = aN_{L/F}(\alpha)$.

($\Longleftarrow$) 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. □

Corollary 5.6.7. $[C(L/F, \sigma, a)] = 1$ *if and only if* $a \in N_{L/F}(L^\times)$.

Example 5.6.8. Let $F = \mathbb{F}_q$ be a finite field. We have $\mathrm{Br}(F) = \bigcup_{L/F} \mathrm{Br}(L/F)$ with L/F ranging over all finite extensions. Since F is finite, L/F is cyclic and $N_{L/F} : L^\times \to F^\times$ is surjective, so $\mathrm{Br}(L/F) = 1$.

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

Theorem 5.6.9. *If L/F is a cyclic field extension, f is a surjective homomorphism and* $\mathrm{Ker}\, f = N_{L/F}(L^\times)$. *In particular,*

$$\mathrm{Br}(L/F) \simeq F^\times / N_{L/F}(L^\times).$$

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

Proposition 5.6.10. *p is an F-algebra isomorphism.*

Proof. Write $L = F(\alpha) = F[t]/(f)$ 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 $G = \mathrm{Gal}(L/F)$, 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 $(L \otimes_F L)^G \cong F^n$.

Lemma 5.6.11. *Let A be a central simple algebra of degree n over F. If $F^n \hookrightarrow A$ as a subalgebra, then $A \cong M_n(F)$.*

Proof. We have $A \cong \mathrm{End}_D(V) \cong M_k(D)$ 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 $\mathrm{rank}_D(V) \geq n$. On the other hand, if $\deg(D) = m$, then $n = km$, so $\mathrm{rank}_D(V) = k = n/m \geq n$, so $m = 1$ and $k = n$, so $D = F$. □

Proposition 5.6.12. $[C(L/F, \sigma, a)] \cdot [C(L/F, \sigma, b)] = [C(L/F, \sigma, ab)] \in \mathrm{Br}(L/F)$.

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

$$A = C(L/F, \sigma, a) = \bigoplus Lu^i \quad \text{and} \quad B = C(L/F, \sigma, b) = \bigoplus Lv^i.$$

Then $A \otimes_F B = \bigoplus (L \otimes_F L)(u^i \otimes v^j)$. If $D = C(L/F, \sigma, ab) = \bigoplus Lw^i$, then

$$\bigoplus (L \otimes_F F)(u^i \otimes v^i) \cong D \quad \text{by} \quad u \otimes v \mapsto w,$$

which embeds in $A \otimes_F B$. Note that the diagonal G-action on $L \otimes_F L = L^n$ coincides with the component-wise G-action. Hence the centralizer of D contains $(L \otimes_F L)^G = F^n$, so the centralizer of D is $M_n(F)$ by the lemma. □

Example 5.6.13. Let $F = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Then $\mathrm{Br}(L/F) \simeq \mathbb{Q}^\times / A$, where A is a subgroup of $\mathbb{Q}^\times$ of all nonzero rational numbers that are sums of two squares. This is a (multiplicatively written) vector space over $\mathbb{Z}/2\mathbb{Z}$ with (infinite) basis consisting of -1 and all primes p with $p \equiv 3$ modulo 4.