Noncommutative algebra

Luka Horjak (luka1.horjak@gmail.com)

February 25, 2024

Contents

Introduction

These are my lecture notes on the course Noncommutative algebra in the year 2023/24. The lecturer that year was prof. dr. Igor Klep.

The notes are not perfect. I did not write down most of the examples that help with understanding the course material. I also did not formally prove every theorem and may have labeled some as trivial or only wrote down the main ideas.

I have most likely made some mistakes when writing these notes – feel free to correct them.

1 Finite-dimensional algebras, Wedderburn's structure theory

"We can do the proof, because it's very simple – actually, it's semisimple."

– prof. dr. Igor Klep

1.1 Free algebras

Definition 1.1.1. Let $R = K\langle x, y\rangle$ be a free algebra and $F = \{xy - yx - 1\}$. The quotient

$$\mathcal{A}_1(K) = {}^{R}\!\Big/\!_{(F)}$$

is called the *first Weyl algebra*.

Remark 1.1.1.1. The first Weyl algebra is generated by elements $\overline{x}$ and $\overline{y}$ that satisfy $\overline{x} \cdot \overline{y} - \overline{y} \cdot \overline{x} - 1$.

Remark 1.1.1.2. The first Weyl algebra is the algebra of differential operators – for $D, L\colon K[y] \to K[y]$, defined as $D(p) = \frac{\partial p}{\partial y}$ and $L(p) = yp$, we have $DL - LD = I$.

Definition 1.1.2. Let R be a ring and $\sigma \in \mathrm{End}(R)$. The *skew polynomial ring* is the set

$$R[x, \sigma] = \left\{ \sum_{i=0}^{n} b_i x^i \;\middle|\; n \in \mathbb{N} \wedge b_i \in R \right\}$$

in which for all $b \in R$ the equality $xb = \sigma(b)x$ holds.

Definition 1.1.3. Let R be a ring and σ a derivation[1] on R. The *skew polynomial ring* is the set

$$R[x, \sigma] = \left\{ \sum_{i=0}^{n} b_i x^i \;\middle|\; n \in \mathbb{N} \wedge b_i \in R \right\}$$

in which for all $b \in R$ the equality $xb = bx + \sigma(b)$ holds.

[1] $\sigma(a + b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = a\sigma(b) + \sigma(a)b$.

1.2 Chain conditions

Definition 1.2.1. Let C be a set and $\{C_i \mid i \in I\}$ a set of subsets of C. The set $\{C_i \mid i \in I\}$ satisfies the *ascending chain condition* if there does not exist an infinite strictly increasing chain

$$C_{i_1} \subset C_{i_2} \subset C_{i_3} \subset \dots$$

The *descending chain condition* is defined analogously.

Definition 1.2.2. Let R be a ring and M an R-module.

i) M is *noetherian* if the set of submodules of M satisfies the ascending chain condition.

ii) M is *artinian* if the set of submodules of M satisfies the descending chain condition.

Proposition 1.2.3. The following statements are true:

i) A module M is noetherian if and only if each submodule of M is finitely generated.

ii) Let $N \leq M$ be a submodule. Then M is noetherian if and only if both N and M/N are noetherian.

iii) Let $N \leq M$ be a submodule. Then M is artinian if and only if both N and M/N are artinian.

Proof.

i) Suppose that each submodule of M is finitely generated and $M_1 \leq M_2 \leq \dots \leq M$. Define the submodule

$$N = \bigcup_{j \in \mathbb{N}} M_j.$$

By assumption, N is finitely generated. But then there exists some $j \in \mathbb{N}$ such that M_j contains all generators of N, so $M_j = N$. Therefore, the chain cannot be strictly increasing.

Now assume that M is noetherian and let $N \leq M$ be a submodule. Define

$$\mathcal{C} = \{S \leq N \mid S \text{ is finitely generated}\}.$$

This set must have some maximal element $N_0 \leq N$. Suppose $N_0 < N$ and consider some element $b \in N \backslash N_0$. The module $N + Rb$ is also finitely generated and contained in N, which is a contradiction as N_0 was maximal. Therefore we must have $N = N_0$ and N is finitely generated.

ii) Suppose that M is noetherian. Consider the following short exact sequence:

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} M/N \longrightarrow 0.$$

It is easy to see that N is also noetherian, as the inclusion of a chain in N is also a chain in M. As preimages of submodules are also submodules, the same conclusion follows for M/N.

Now suppose that both N and M/N are noetherian and consider a chain $M_1 \leq M_2 \leq \dots \leq M$ of submodules. As $f^{-1}(M_i)$ and $g(M_i)$ form increasing chains in

their respective modules, it follows that there exists some $n \in \mathbb{N}$ such that both $f^{-1}(M_i)$ and $g(M_i)$ are constant for all $i \geq n$. Now consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & f^{-1}(M_n) & \xrightarrow{f} & M_n & \xrightarrow{g} & g(M_n) & \longrightarrow & 0 \\ & & \downarrow \mathrm{id} & & \downarrow i & & \downarrow \mathrm{id} & & \\ 0 & \longrightarrow & f^{-1}(M_i) & \xrightarrow{f} & M_i & \xrightarrow{g} & g(M_i) & \longrightarrow & 0. \end{array}$$

By the short five lemma, i is an isomorphism, so $M_n = M_i$.

iii) Same as ii). □

Definition 1.2.4. A ring R is *left-noetherian* if it is noetherian as a left R-module. We analogously define *right-noetherian*, *left-artinian* and *right-artinian* rings.

A ring R is *noetherian*, if it is both left-noetherian and right-noetherian. We similarly define *artinian* rings.

Remark 1.2.4.1. A ring R is left-noetherian if and only if each left ideal of R is finitely generated.

Proposition 1.2.5. If R is a noetherian ring and M is a finitely generated R-module, M is noetherian.

Proof. As M is finitely generated, there exists an endomorphism $\varphi\colon R^n \to M$ for some $n \in \mathbb{N}$. Consider the short exact sequence

$$0 \longrightarrow R \longrightarrow R^n \longrightarrow R^{n-1} \longrightarrow 0.$$

By induction on n, R^n is noetherian. As M is a quotient of R^n, M is also noetherian. □

1.3 Simple modules

Definition 1.3.1. A non-trivial R-module M is *simple* if it has no proper non-trivial submodules. An R-module M is *cyclic* with generator $m \in M$ if $M = R \cdot m$.

Proposition 1.3.2. For R-modules M, the following are equivalent:

i) The module M is simple.

ii) The module M is cyclic and its every non-zero element is a generator.

iii) We have $M \cong {}^{R}/_{I}$ for some maximal left ideal $I \lhd R$.

Proof. Suppose that M is simple. Then for every $m \in M \setminus \{0\}$, $Rm \leq M$ is a non-trivial submodule. It follows that m is a generator.

Suppose now that every non-zero element is a generator. Define the homomorphism $\phi\colon R \to M$ with $\phi(r) = rm$. Set $I = \ker \phi = \operatorname{ann}(m)$. By the isomorphism theorem, we have $Rm = M \cong {}^{R}/_{I}$. There is bijective correspondence between ideals $I \lhd J \lhd R$ and submodules of M. As any element of a proper submodule cannot generate M, I must be maximal.

Suppose now that $M \cong {}^{R}/_{I}$ for some maximal $I \lhd R$ and suppose that $M' \leq M$ is a submodule. It follows that M' corresponds to a left ideal J such that $I \lhd J \lhd R$. Thus, $J = I$ or $J = R$, or equivalently, $M' = M$ or $M' = (0)$. □

Corollary 1.3.2.1. Let D be a division ring and V be an n-dimensional vector space over D. Let $R = \operatorname{End}_D(V)$. Then, V is a simple R-module.

Proof. For every $v \in V \setminus \{0\}$ we have $Rv = V$. □

Theorem 1.3.3 (Schur's lemma)**.** Let M and N be simple R-modules and $f\colon M \to N$ a homomorphism. Then f is either and isomorphism or the zero map. In particular, $\operatorname{End}_R(M)$ is a division ring.

Proof. Note that $\ker f \leq M$ and $\operatorname{im} f \leq N$. The conclusion follows. □

Proposition 1.3.4. Let D be a division ring and V a D-module. Then, $D \cong \operatorname{End}_R(V)$, where $R = \operatorname{End}_D(V)$.

Proof. Define a homomorphism $\Psi\colon D \to \operatorname{End}_R(V)$ as $\Psi(d) = (f \mapsto df)$. It is clear that Ψ is injective. Now let $T \in \operatorname{End}_R(V)$ be an arbitrary endomorphism. Choose a $v \in V \setminus \{0\}$. For any $w \in V$ there exists an endomorphism of V that sends w to v, therefore, $V = R \cdot v$. Every R-endomorphism is therefore determined by its image on v. To prove that Ψ is surjective, it is hence enough to show that $Tv = d \cdot v$ for some $d \in D$.

Let $p \in R$ be a projection onto Dv. It is easy to check that

$$Tv = T(p(v)) = p(T(v)) \in Dv.$$ □

Lemma 1.3.5. A finite dimensional division algebra D over an algebraically closed field k is k itself.

Proof. Note that, for $\alpha \in D$, $k(\alpha)\big/_k$ is a finite field extension, but as k is algebraically closed, $k(\alpha) = k$. □

1.4 Semisimple modules

Definition 1.4.1. A module is *semisimple* if it is a direct sum of simple modules.

Proposition 1.4.2. If an R-module M is a sum of simple submodules M_i for $i \in I$, then M is semisimple. Moreover, there exists a subset $I' \subseteq I$ such that

$$M = \bigoplus_{i \in I'} M_i.$$

Proof. Set

$$\mathcal{I} = \left\{ J \subseteq I \;\middle|\; (M_j)_{j \in J} \text{ is independent} \right\}.$$

As $\mathcal{I}$ is a non-empty set and every chain in M has an upper bound, we can apply Zorn's lemma. Let I' be a maximal element of $\mathcal{I}$. Note that

$$M' = \bigoplus_{i \in I'} M_i \leq M.$$

If $M' \cap M_i = \{0\}$ for some $i \in I$, the set I' is not maximal as we can take $I' \cup \{i\}$. Therefore, $M' \cap M_i = M_i$ for all i as M_i are simple modules. It follows that $M' = M$. □

Corollary 1.4.2.1. If M is semisimple, then so is every submodule and quotient of M. Furthermore, every submodule of M is a direct summand.

Proof. Let

$$M = \bigoplus_{i \in I} M_i$$

be a direct sum of simple modules and $M' \leq M$. The module M/M' is then generated by the images $\overline{M}_i$ of M_i under the quotient map. If $\overline{M}_i \neq \{0\}$, we have $\overline{M}_i \cong M_i$ since M_i is simple. Therefore, M/M' is a sum of modules M_i, and as such semisimple. As we can write

$$M = \left(\bigoplus_{i \in I'} M_i \right) \oplus M',$$

we can write

$$M' = \bigoplus_{i \in I \setminus I'} M_i.$$ □

Proposition 1.4.3. Let M be a module such that every submodule of M is a direct summand.[2] Then M is semisimple.

Proof. Let $M' \leq M$ be a non-zero cyclic submodule, say $M' = Rm$ for $m \neq 0$. Suppose M' is not simple. By Zorn's lemma, there exists a maximal submodule $M'' \leq M'$ with $m \notin M''$. The module M'/M'' is therefore simple. As M' also has the complement property, we can write $M' = M'' \oplus S$ for some $S \leq M'$. Since $S \cong M'/M''$, it is a simple submodule. In both cases, we have found a simple submodule of M.

Let M_1 be the sum of all simple submodules of M. Then there exists a submodule $M_2 \leq M$, such that $M = M_1 \oplus M_2$. If $M_2 \neq \{0\}$, by the same argument as above, M_2 has a simple submodule. This is of course not possible. □

[2] We call this the *complement property*.

1.5 Endomorphism ring of a semisimple module

Proposition 1.5.1. Let M be an R-module, $S = \mathrm{End}_R(M)$ and $p, m, n \in \mathbb{N}$. There is a canonical isomorphism of abelian groups

$$\mathrm{Hom}_R(M^n, M^m) \cong S^{m\times n},$$

such that the composition

$$\mathrm{Hom}_R(M^n, M^m) \times \mathrm{Hom}_R(M^p, M^n) \to \mathrm{Hom}_R(M^p, M^m)$$

corresponds to matrix multiplication. In particular, $\mathrm{End}_R(M^n) \cong S^{n\times n} = M_n(S)$ is an isomorphism of rings.

Proof. The isomorphism is given by the map $f \mapsto [\pi_i \circ f \circ \iota_j]_{i,j}$. □

Remark 1.5.1.1. For $r \in R$ the map $T_r \colon R \to R$ given by $T_r(x) = xr$ is R-linear. We can therefore define a homomorphism $\Phi \colon R \to \mathrm{End}_R(R)$ by $\Phi(r) = T_r$. As Φ is injective and $f = T_{f(1)}$, we have $\mathrm{End}_R(R) \cong R^{\mathsf{op}}$.

Corollary 1.5.1.2. For a division ring D, we have $\mathrm{End}_D(D^n) = M_n(D^{\mathsf{op}})$.

Definition 1.5.2. A semisimple module has *finite length* if it is a finite direct sum of simple modules.

Proposition 1.5.3. If M is a semisimple R-module of finite length, then $\mathrm{End}_R(M)$ is isomorphic to a finite product of matrix rings over division rings.

Proof. Let

$$M \cong \bigoplus_{i=1}^{k} M_i^{n_i}$$

for distinct simple modules M_i. By Schur's lemma, we can write

$$\mathrm{End}_R(M) = \mathrm{End}_R\left(\bigoplus_{i=1}^{k} M_i\right) = \prod_{i=1}^{k} \mathrm{End}_R\left(M_i^{n_i}\right) = \prod_{i=1}^{k} M_{n_i}\left(\mathrm{End}_R(M_i)\right). \qquad \square$$

1.6 Semisimple rings

Definition 1.6.1. A ring R is *semisimple* if it is a semisimple left R-module.

Theorem 1.6.2. Let R be a ring. The following statements are equivalent:

i) The ring R is semisimple.

ii) Every R-module is semisimple.

iii) Every short exact sequence of R-modules split.

Proof. Suppose that R is semisimple. As all R-modules are quotients of a free module R^I, which is semisimple, all R-modules are semisimple.

Suppose that every R-module is semisimple. As those have the complement property, every short exact sequence splits.

Suppose that every short exact sequence splits and let $I \leq R$ be a submodule over R. As

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

is a short exact sequence, it splits, so I is a direct summand of R. It follows that R has the complement property, therefore, it is semisimple. □

Corollary 1.6.2.1. Suppose that R is a semisimple ring. Then R as an R-module has finite length and any simple R-module is isomorphic to a simple component of R.

Proof. We can write

$$R = \bigoplus_{i \in I} M_i$$

for simple R-modules M_i. By considering $1 \in R$, we see that I is a finite set.

Let M be a simple R-module. As we have $M = R \cdot m$, there exist maps $M_i \to M$. As $R \to M$ is surjective, at least one of those maps is non-zero and therefore an isomorphism by Schur's lemma. □

Proposition 1.6.3. Let D be a division ring and V be an n-dimensional vector space over D. Then $R = \mathrm{End}_D(V)$ is semisimple.

Proof. The map $f \mapsto (f(e_1), f(e_2), \ldots, f(e_n))$ is an isomorphism of R-modules R and V^n. As V is simple by corollary 1.3.2.1, R is semisimple. □

1.7 Wedderburn structure theorem

Theorem 1.7.1 (Wedderburn)**.** Every semisimple ring R is isomorphic to a finite product of matrix rings over division rings. If R is also commutative, it is a finite direct products of fields.

Proof. By proposition 1.5.3, we can write

$$R^{\mathsf{op}} \cong \mathrm{End}_R(R) \cong \prod_{i=1}^{k} M_{n_i}(D_i).$$

It follows that

$$R \cong \left(\prod_{i=1}^{k} M_{n_i}(D_i)\right)^{\mathsf{op}} = \prod_{i=1}^{k} M_{n_i}\left(D_i^{\mathsf{op}}\right). \qquad \square$$

Definition 1.7.2. A ring is *simple* if it has no non-trivial proper two-sided ideals.

Remark 1.7.2.1. Simple rings are not necessarily semisimple.

Remark 1.7.2.2. Every semisimple ring R is isomorphic to a finite product of simple rings.

Proposition 1.7.3 (Uniqueness of the decomposition)**.** Suppose that

$$R = \prod_{i=1}^{n} R_i = \prod_{i=1}^{m} R_i'$$

for simple rings R_i and R_i'. Then, $n = m$ and R_i' are a permutation of R_i.

Proof. As $R_i \triangleleft R$, we have $R_i R = R_i$. It follows that

$$R_i = \prod_{j=1}^{m} R_i R_j'.$$

Take $R_i R_j' \triangleleft R_i$ to be a non-trivial ideal. It follows that $R_i R_j' = R_i$. Likewise, it follows that $R_i R_j' = R_j'$. $\square$

1.8 Jacobson radical

Definition 1.8.1. The *Jacobson radical* of a ring R is the set

$$\operatorname{rad} R = \bigcap \{I \lhd_L R \mid I \text{ is maximal in } R\}.$$

Lemma 1.8.2. For all $y \in R$ the following statements are equivalent:

i) We have $y \in \operatorname{rad} R$.

ii) For all $x \in R$ the element $(1 - xy)$ is left invertible.

iii) For all simple R-modules M we have $yM = (0)$.

Proof. Suppose that $y \in \operatorname{rad} R$. If there exists some $x \in R$ such that $(1 - xy)$ is not left invertible, the set $R(1 - xy)$ is a proper ideal of R. By Zorn's lemma, there exists some maximal ideal $M \lhd R$ such that $R(1 - xy) \leq M$. In particular, we have $1 - xy \in M$. As $y \in M$, we have $1 \in M$, which is of course not possible.

Suppose that $(1 - xy)$ is left invertible for all $x \in R$. If we have $ym \neq 0$ for an element $m \in M$ of a simple R-module, we get $R(ym) = M$. Therefore, there exists some $x \in R$ such that $xym = m$, or, equivalently, $(1 - xy) \cdot m = 0$. This is again a contradiction.

Suppose now that y annihilates all simple R-modules and let $M \lhd R$ be any maximal ideal. As R/M is a simple R-module, we get $y \cdot R/M = (0)$, therefore, $y \in M$. □

Definition 1.8.3. The *annihilator* of an R-module M is the set

$$\operatorname{ann}(M) = \{y \in R \mid y \cdot M = (0)\}.$$

Remark 1.8.3.1. We have $\operatorname{ann} M \lhd R$.

Corollary 1.8.3.2. We have

$$\operatorname{rad} R = \bigcap \{\operatorname{ann} M \mid M \text{ is a simple } R\text{-module}\}.$$

In particular, $\operatorname{rad} R \lhd R$.

Lemma 1.8.4. An element $y \in R$ is an element of the Jacobson radical if and only if $1 - xyz$ is invertible for all $x, z \in R$.

Proof. If $1 - xy \cdot 1$ is invertible, we have $y \in \operatorname{rad} R$.

Suppose now that $y \in \operatorname{rad} R$ and fix $x, z \in R$. As $yz \in \operatorname{rad} R$, the element $1 - xyz$ is left invertible with inverse $u \in R$. But as $xyz \in \operatorname{rad} R$, we also have that the element $1 + u \cdot (xyz) = u$ is left invertible. □

Proposition 1.8.5. The following statements are true:

i) The set $\operatorname{rad} R$ is the largest (left) ideal J satisfying $1 + J \subseteq R^{-1}$.

ii) The left radical is the same as the right radical.

iii) Suppose that $I \lhd R$ is an ideal with $I \subseteq \operatorname{rad} R$. Then

$$\operatorname{rad}\left(R/I\right) = \operatorname{rad} R/I.$$

Proof. Maximal left ideals in R/I correspond with maximal left ideals in R which contain I. □

Definition 1.8.6. A ring R is *J-semisimple* if $\operatorname{rad} R = (0)$.

Remark 1.8.6.1. For each ring R, the quotient $R/\operatorname{rad} R$ is J-semisimple.

Proposition 1.8.7. The following statements are true:

i) R and $R/\operatorname{rad} R$ have the same simple left modules.

ii) An element $x \in R$ is (left) invertible if and only if $x + \operatorname{rad} R$ is (left) invertible in $R/\operatorname{rad} R$.

Proof.

i) Follows from lemma 1.8.2.

ii) If x is invertible, then so is $x + \operatorname{rad} R$. Suppose now that for some $y \in R$ we have $(y + \operatorname{rad} R)(x + \operatorname{rad} R) = 1 + \operatorname{rad} R$. As $1 - yx \in \operatorname{rad} R$, we have that yx is invertible, so x has a left inverse. □

Definition 1.8.8. A one-sided or two-sided ideal $I \subseteq R$ is

i) *nil* if all its elements are nilpotent,

ii) *nilpotent* if $I^n = (0)$ for some $n \in \mathbb{N}$.

Lemma 1.8.9. If a left ideal $I \subseteq R$ is nil, then $I \subseteq \operatorname{rad} R$.

Proof. Fix an element $y \in I$. For all $x \in R$, the element $xy \in I$ is nilpotent, say $(xy)^n = 0$. As

$$(1 - xy) \cdot \sum_{k=0}^{n-1} (xy)^k = 1,$$

the element $1 - xy$ is invertible. Therefore, $y \in \operatorname{rad} R$. □

Theorem 1.8.10. Suppose that R is a left-artinian ring. Then $\operatorname{rad} R$ is the largest nilpotent left ideal.[3]

Proof. As every nilpotent ideal is contained in the radical, it suffices to show that $\operatorname{rad} R$ is nilpotent.

Consider the decreasing chain

$$R \supseteq \operatorname{rad} R \supseteq (\operatorname{rad} R)^2 \supseteq \dots$$

As R is artinian, this chain is eventually constant – call that ideal I. Assume that $I \neq (0)$. By the artinian property, there exists a minimal left ideal I_0 such that $I \cdot I_0 \neq 0$. Therefore, there exists some $a \in I_0$ such that $I \cdot a \neq (0)$. Then $I \cdot (Ia) = Ia \neq (0)$. It follows that $I \cdot a = I_0$. In particular, for some $y \in I$ we have $ya = a$, or $(1 - y)a = 0$. As $y \subseteq \operatorname{rad} R$, we get $a = 0$, which is a contradiction, therefore $I = (0)$. □

Theorem 1.8.11. For a ring R the following statements are equivalent:

[3] Also the *Wedderburn radical*.

i) The ring R is semisimple.

ii) The ring R is J-semisimple and left-artinian.

Proof. A semisimple ring is left-artinian by the Wedderburn theorem. Since R is semisimple, there exists a left R-module $I \leq R$ such that $R = \operatorname{rad} R \oplus I$. If $\operatorname{rad} R \neq (0)$, I is a proper ideal and therefore contained in a maximal ideal M. But as $\operatorname{rad} R$ is also contained in the same ideal M, it follows that $R \subseteq M$, which is impossible.

Now suppose that R is J-semisimple and left-artinian. By the artinian property, we can write $\operatorname{rad} R$ as a finite intersection of maximal submodules

$$(0) = \operatorname{rad} R = \bigcap_{i=1}^{n} M_i.$$

Consider the homomorphism

$$\varphi \colon R \to \bigoplus_{i=1}^{n} R/M_i$$

with

$$\varphi(x) = \prod_{i=1}^{n} (x + M_i).$$

As $\ker \varphi = (0)$, it is injective. We can therefore write

$$R \leq \bigoplus_{i=1}^{n} R/M_i \,,$$

so R is semisimple. □

Lemma 1.8.12 (Nakayama)**.** For a left ideal $J \leq R$ the following statements are equivalent:

i) $J \subseteq \operatorname{rad} R$

ii) The only finitely generated R-module M such that $JM = M$ is $M = (0)$.

iii) For all R-modules N and M such that $N \leq M$ and M/N is finitely generated, we have

$$N + JM = M \implies N = M.$$

Proof. Suppose that $J \subseteq \operatorname{rad} R$ and that $M \neq (0)$ is finitely generated with a minimal set of generators $\{x_1, \ldots, x_k\}$. Since $J \cdot M = M$, we can write

$$x_k = \sum_{i=1}^{k} a_i x_i$$

for some $a_i \in J$. But as $1 - a_k$ is invertible, we can express x_k as a linear combination of x_1, x_2, …, x_{k-1}, which is a contradiction.

Suppose that the second statement holds and let $N \leq M$ be modules. If $N \neq M$, it follows that $J \cdot M/N \neq M/N$, so $N + JM \neq M$.

No suppose that the third statement holds and let $y \in J \setminus \operatorname{rad} R$. Let M be a maximal submodule of R such that $y \notin M$. As $M + J = R$, it follows that $M = R$, which is a contradiction. □

1.9 Group rings and Maschke's theorem

Theorem 1.9.1 (Maschke)**.** Suppose that G is a finite group and k a field such that $\operatorname{char} k \nmid |G|$. Then kG is semisimple.

Proof. By Algebra 3, theorem 4.2.2, every submodule W of V is a direct summand, so kG has the complement property. □

Proposition 1.9.2. If k is a field and G is an infinite group, then kG is not semisimple.

Proof. Consider the map $\varepsilon\colon kG \to k$ such that $\varepsilon|_k = \mathrm{id}$ and $\varepsilon(g) = 1$ for all $g \in G$. Let $I = \ker \varepsilon$ and note that $I \lhd kG$.

Suppose that kG is semisimple. Therefore, there exists a submodule $J \leq kG$ such that $I \oplus J = kG$. Write $1 = e + f$ where $e \in I$ and $f \in J$. As $e = e^2 + ef$, it follows that $ef = 0$ and $e = e^2$. Similarly, we have $f = f^2$. Analogously, we get that $b = be$ for all $b \in I$, so $I = (kG)e$ and $J = (kG)f$.

Note that for all $g \in G$ we have $g - 1 \in I$, so $gf = f$. It is now clear that $f \neq 0$ must have the same non-zero coefficient in front of every element $g \in G$ in its linear combination of elements of G. This is not possible, as the linear combination is finite. □

Remark 1.9.2.1. The ring $\mathbb{C}G$ is always J-semisimple.

Remark 1.9.2.2. If G is a finite group and $\operatorname{char} k \mid |G|$, the ring kG is also not semisimple.

2 Primitive rings

"The word primitive often carries a negative connotation, but these are pretty cool."

– prof. dr. Igor Klep

2.1 Density theorem

Definition 2.1.1. A ring R is *primitive* if it has a faithful[4] simple module M.

Remark 2.1.1.1. Equivalently, the representation $R \to \mathrm{End}(M)$ is injective and irreducible.

Definition 2.1.2. Let V be a vector space over a division ring D, and let $R \subseteq \mathrm{End}_D(V)$ be a subring. The ring R is a *dense ring of linear transformations*[5] if for every finite set $\{v_1, \ldots, v_n\} \subseteq V$ of linearly independent vectors and any $\{w_1, \ldots, w_n\} \subseteq V$ there exists some $\phi \in R$ such that $\phi(v_i) = w_i$ for all $i \leq n$.

Theorem 2.1.3 (Density)**.** Let M be a semisimple module over a ring R. We denote $S = \mathrm{End}_R(M)$ and let $\phi \in \mathrm{End}_S(M)$. Then for any finite set $\{x_1, \ldots, x_n\} \subseteq M$ there exists an element $r \in R$ such that $\phi(x_i) = rx_i$ for all $i \leq n$.

Proof. For $n = 1$ we can write

$$M = Rx_1 \oplus M'$$

as M is semisimple. Note that $\pi \colon M \to Rx_1$ is an element of S. It follows that

$$\phi(x_1) = \phi(\pi(x_1)) = \pi(\phi(x_1)),$$

therefore $\phi(x_1) \in Rx_1$.

Consider now M^n and $\phi^{(n)} \colon M^n \to M^n$ as the point-wise application of ϕ. Observe that $\phi^{(n)} \in \mathrm{End}_{\mathrm{End}_R(M^n)}(M^n)$. As M^n is a semisimple R-module, we can apply the $n = 1$ case. □

Theorem 2.1.4 (Jacobson)**.** A ring R is primitive if and only if R is a dense ring of linear transformations on a vector space over a division ring.

Proof. Assume that R is a primitive ring and let M be a faithful and simple R-module. By Schur's lemma, $D = \mathrm{End}_R(M)$ is a division ring, therefore, M is a D-vector space. Since M is faithful, we have $R \subseteq \mathrm{End}_D(M)$, therefore R acts as a ring of linear transformations on M. By the density theorem for modules the ring R is dense.

Assume now that R is a dense ring of linear transformations on a vector space V over a division ring D. In particular, V is an R-module. By definition we have $R \subseteq \mathrm{End}_D(V)$, therefore V is a faithful R-module. It is clear that every non-zero element generates V, therefore V is simple. □

[4] $\mathrm{ann}(M) = (0)$.

[5] R acts densely on V.

Corollary 2.1.4.1. Any simple artinian ring R is isomorphic to $M_n(D)$ for a division ring D.

Proof. As R is simple, it is primitive. Let M be a faithful and simple R-module and denote $D = \mathrm{End}_R(M)$. This is of course a division ring by Schur's lemma. By Jacobson's theorem, R is a dense subring of $\mathrm{End}_D(M)$.

Assume that $\dim_D M = \infty$ and let $(v_n)_n$ be an infinite sequence of linearly independent vectors in M. Let

$$I_n = \{r \in R \mid \forall i \leq n \colon rv_i = 0\}$$

be submodules of R. Note that these submodules form a strictly decreasing chain, which is impossible.

As $\dim_D M < \infty$, we know that $R = \mathrm{End}_D(M) \cong M_{\dim_D M}(D)$. □

Theorem 2.1.5 (Structure)**.** Let R be a primitive ring with a faithful simple module M and denote $D = \mathrm{End}_R(M)$. Then

i) $R \cong M_n(D)$ for some $n \in \mathbb{N}$ or

ii) for all $m \in \mathbb{N}$ there exists a subring $R_m \subseteq R$ and an epimorphism $R_m \to M_m(D)$.

Proof. If $\dim_D M < \infty$, we have $R = \mathrm{End}_D(M) = M_n(D)$ for $n = \dim_D M$. Now assume that $\dim_D M = \infty$. For an infinite sequence $(v_n)_n$ of linearly independent vectors in M, form $V_m = \mathrm{Lin}_D \{v_i \mid i \leq m\}$. Now set

$$R_m = \{r \in R \mid r \cdot V_m \subseteq V_m\}.$$

Note that

$$I_m = \{r \in R \mid rV_m = 0\}$$

is an ideal in R_m. By Jacobson's theorem we have $R_m/I_m \cong M_m(D)$. □

Remark 2.1.5.1. In the case of finite-dimensional algebras the notions of primitive and simple coincide.

Remark 2.1.5.2. The free algebra is primitive. Every algebra is the image of some primitive algebra.

2.2 An application of primitive rings

Proposition 2.2.1. A ring R is J-semisimple if and only if it has a faithful semisimple module M.

Proof. Suppose that R has a faithful semisimple module M. Recall that the radical is the set of all elements that act trivially on all simple R-modules. It follows that $\operatorname{rad} R \cdot M = 0$, whence $\operatorname{rad} R = (0)$ as M is faithful.

Suppose now that R is J-semisimple. Let $(M_i)_{i\in I}$ be all non-isomorphic simple R-modules and

$$M = \bigoplus_{i\in I} M_i.$$

Note that

$$\operatorname{ann}(M) = \bigcap_{i\in I} \operatorname{ann}(M_i) = \operatorname{rad}(R) = (0). \qquad \square$$

Corollary 2.2.1.1. Every J-semisimple ring R is a subdirect product of primitive rings.

Proof. The inclusion

$$R \hookrightarrow \textstyle\prod_{i\in I} R \big/ \operatorname{ann} M_i$$

is the desired representation. $\square$

Proposition 2.2.2. Suppose that R is a ring in which $x^3 = x$ holds for all $x \in R$. Then R is commutative.

Proof. Note that if $ab = 0$, we also have $ba = (ba)^3 = 0$. Let $e \in R$ be an idempotent. Note that for all $x \in R$ we have $e(x - ex) = 0$, therefore $xe = exe$. Similarly, we have $(x - xe)e = 0$, therefore $ex = exe$. This implies that $e \in Z(R)$.

Let $x \in R$ and note that $(x^2)^2 = x^2$. Therefore, x^2 is an idempotent and we have $x^2 \in Z(R)$. Also note that for all $c \in R$ such that $c^2 = 2c$ we have $c = 2c^2 \in Z(R)$.

Now let $x \in R$. Note that

$$(x^2 + x)^2 = x^4 + 2x^3 + x^2 = 2(x^2 + x),$$

therefore, we have both $x^2 + x \in Z(R)$ and $x = (x^2 + x) - x^2 \in Z(R)$. $\square$

Theorem 2.2.3 (Jacobson)**.** Suppose that R is a ring such that for all x there exists an $n > 1$ such that $x^n = x$.[6] Then R is commutative.

Theorem 2.2.4 (Jacobson-Herstein)**.** A ring R is commutative if and only if for all $x, y \in R$ there exists an $n > 1$ such that

$$(xy - yx)^n = xy - yx.$$

Proof. Assume that the conclusion holds for division rings.[7]

Suppose that R is primitive. Using the structure theorem, we split two cases:

i) There exists a division ring D and $n \in \mathbb{N}$ such that $R \cong M_n(D)$. Note that this is not possible for $n \geq 2$, as $[E_{1,1}, E_{1,2}] = E_{1,2}$, which is nilpotent. It follows that $R \cong D$.

ii) There exists an epimorphism $R_2 \to M_2(D)$ for a subring $R_2 \subseteq R$. As in case i), this is of course not possible.

In both cases the conclusion holds.

Suppose now that R is J-semisimple. By corollary 2.2.1.1, we can map R into a product of primitive rings R_i. By the previous step, the rings R_i are commutative, but then so is R.

Now let R be an arbitrary ring. Note that $R/\operatorname{rad} R$ is a J-semisimple ring that satisfies the given relation. By the previous step, $R/\operatorname{rad} R$ is commutative.

Fix two elements $a, b \in R$. Note that $d = [a, b] \in \operatorname{rad} R$. As we have $d^n = d$, we can write $d \cdot (1 - d^{n-1}) = 0$, but as $1 - d^{n-1}$ is invertible, it follows that $d = 0$. □

[6] We say that x is *torsion*.

[7] To be proven in the next section.

3 Central simple algebras

"Coming soon, poker, chess, or three in a line."

– prof. dr. Igor Klep

3.1 Cyclic algebras

Proposition 3.1.1. Let k be a field and $\sigma \in \mathrm{Aut}(k)$. Let

$$D = k((x,\sigma)) = \left\{ \sum_{i=m}^{\infty} a_i x^i \;\middle|\; m \in \mathbb{Z} \wedge a_i \in k \right\},$$

with $x \cdot a = \sigma(a)x$ for all $a \in k$, be a division ring. Denote $k_0 = \{a \in k \mid \sigma(a) = a\}$. Then

$$Z(D) = \begin{cases} k_0((x^s)), & \operatorname{ord}\sigma = s, \\ k_0, & \sigma \text{ has infinite order.} \end{cases}$$

Moreover, $\dim_{Z(D)} D < \infty$ is equivalent to σ being of finite order.

Proof. Let

$$f = \sum_{i=m}^{\infty} a_i x^i \in Z(D)$$

with $a_j \neq 0$. Note that, as $af = fa$ for all $a \in k$, we must have $aa_j = \sigma^j(a)a_j$, therefore $\sigma^j(a) = a$ for all $a \in k$. If σ has infinite order, it follows that $f = a_0$. But as $xf = fx$, we get $a_0 \in k_0$ and therefore $Z(D) = k_0$.

Suppose now that $s = \operatorname{ord}\sigma$. With same notation and argument as above, we see that $s \mid j$. As $xf = fx$, we also see that all coefficients of f are elements of k_0. The reverse inclusion follows from a trivial calculation. □

Definition 3.1.2. Let K/F be a cyclic Galois extension with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ and let $s = [K : F]$. Fix a non-zero $a \in F \setminus \{0\}$. The *cyclic algebra* $(K/F, \sigma, a)$ is the vector space

$$D = \bigoplus_{i=0}^{s-1} K x^i$$

with multiplication on defined with $x^s = a$ and $x \cdot b = \sigma(b)x$.

Remark 3.1.2.1. We have $\dim_F (K/F, \sigma, a) = \mathrm{ord}(\sigma)^2$.

Remark 3.1.2.2. We have $(K/F, \sigma, a) \cong K[t,\sigma]\big/(t^s - a)$, where K is the skew polynomial ring.

Theorem 3.1.3. Let $D = (K/F, \sigma, a)$ be a cyclic algebra.

i) The algebra D is a simple F-algebra.

ii) We have $C_D(K) = \{y \in D \mid \forall b \in K : by = yb\} = K$.

iii) The field K is a maximal subfield of D.

iv) We have $Z(D) = F$.

Proof.

i) Let $I \triangleleft D$ be a non-trivial ideal in D and let $z \in I$ be a non-zero element. Let

$$z = \sum_{k=1}^{r} b_{i_k} x^{i_k},$$

where $i_k \leq s-1$ and suppose that r is minimal. Assume that $r > 1$. Note that $\sigma^{i_1} \neq \sigma^{i_r}$, so suppose they differ at $b \in K$. But then the element

$$\sigma^{i_r}(b)z - zb \in I$$

has smaller r, which is a contradiction if $r > 1$. It follows that z is invertible and therefore $I = D$.

ii) Clearly $K \subseteq C_D(K)$. Choose an arbitrary element $d \in C_D(K)$ and write

$$z = \sum_{i=0}^{s-1} b_i x^i.$$

As before, compute both elements bd and db and note that $b_i = 0$ for all $i > 0$.

iii) Suppose that $L \subseteq D$ is a subfield with $K \subseteq L$. But as L is a field, we have $L \subseteq C_D(K)$, therefore $L = K$.

iv) Note that $F \subseteq Z(D)$. Now let $b \in Z(D)$ be an arbitrary element. It follows that $b \in C_D(K) = K$. Computing elements bx and xb, we note that $\sigma(b) = b$. □

Definition 3.1.4. Let K/F be a cyclic Galois extension with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ and let $s = [K : F]$. The *norm* is the map $N_{K/F} : K \to F$ given by

$$N_{K/F}(a) = \prod_{k=0}^{s-1} \sigma^k(a).$$

Theorem 3.1.5. If $a \in N_{K/F}(K)$, then $D = (K/F, \sigma, a) \cong M_s(F)$.

Proof. Let $d \in K$ be an element with $N_{K/F}(d) \cdot a = 1$ and let $y = dx$. A simple calculation shows that $y^s = N_{K/F}(d)x^s = 1$. For all $b \in K$, we also have $yb = \sigma(b)y$. We can therefore write $D \cong (K/F, \sigma, 1)$.

Recall that $(K/F, \sigma, 1) \cong B/(t^s - 1)$, where $B = K[t, \sigma]$. Of course it holds that $(t^s - 1) \subseteq B(t-1)$, which is a maximal submodule in B as $B/B(t-1) \cong K$. It follows that $M = B/B(t-1)$ is a simple module of $B/(t^s - 1) \cong (K/F, \sigma, 1)$. The module structure then yields a homomorphism $(K/F, \sigma, 1) \to \mathrm{End}_F(M) \cong M_s(F)$. Since $(K/F, \sigma, 1)$ is simple, the homomorphism is injective. Furthermore, as both dimensions are equal to s^2, this is an isomorphism. □

Remark 3.1.5.1. The converse is also true. Furthermore, if s is a prime, then the algebra $(K/F, \sigma, a)$ is a division algebra if and only if $a \notin N_{K/F}(K)$.

3.2 Tensor product of algebras

Definition 3.2.1. The *tensor product* of k-algebras R and S is the algebra $R \otimes_k S$ with multiplication

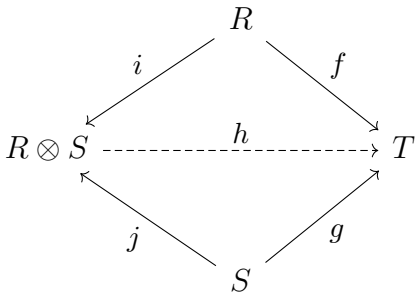
$$(r \otimes s) \cdot (r' \otimes s') = rr' \otimes ss'.$$

Remark 3.2.1.1. If $(e_\alpha)_\alpha$ is a basis for S over k, each $x \in R \otimes S$ has a unique expansion

$$x = \sum_\alpha r_\alpha \otimes e_\alpha.$$

The algebra $R \otimes S$ is a free R-module with basis $(1 \otimes e_\alpha)_\alpha$. In particular, homomorphisms $i\colon r \mapsto r \otimes 1$ and $j\colon s \mapsto 1 \otimes s$ are injective.

Proposition 3.2.2 (Universal property)**.** Given any k-algebras R, S and T and k-algebra homomorphism $f\colon R \to T$ and $g\colon S \to T$ such that $f(R)$ and $g(S)$ commute element-wise and $f|_k = g|_k$. Then there exists a unique k-algebra homomorphism $h\colon R \otimes S \to T$ such that $hi = h$ and $hj = g$.



Proof. Define the map $\varphi\colon R \times S \to T$, given by

$$\varphi(r, s) = f(r) \cdot g(s).$$

This is a k-bilinear map. Indeed,

$$\varphi(r_1 + r_2, s) = f(r_1 + r_2) \cdot g(s) = f(r_1) \cdot g(s) + f(r_2) \cdot g(s) = \varphi(r_1, s) + \varphi(r_2, s)$$

and similarly for $s = s_1 + s_2$, and

$$\varphi(kr, s) = f(kr) \cdot g(s) = kf(r) \cdot g(s) = k \cdot \varphi(r, s) = f(r) \cdot g(ks) = \varphi(r, ks).$$

By the universal property of tensor products of modules, it follows that φ induces a unique homomorphism $h\colon R \otimes S \to T$ of k-modules with $hi = f$ and $hj = g$. Also note that φ is the unique map such that $hi = f$ and $hj = g$ hold. The k-module homomorphism h is therefore unique. It follows that if h is a k-algebra homomorphism, it is unique as well.

It remains to check that h is indeed a k-algebra homomorphism. It is clearly enough to check this on the basis, which we do with a straightforward calculation:

$$\begin{aligned} h((r_1 \otimes s_1) \cdot (r_2 \otimes s_2)) &= h(r_1 r_2 \otimes s_1 s_2) \\ &= \varphi(r_1 r_2, s_1 s_2) \\ &= f(r_1 r_2) \cdot g(s_1 s_2) \\ &= f(r_1) g(s_1) \cdot f(r_2) g(s_2) \\ &= h(r_1 \otimes s_1) \cdot h(r_2 \otimes s_2). \end{aligned}$$

□

3.3 Scalar extensions and semisimplicity

Definition 3.3.1. Let R be a k-algebra and K/k a field extension. Then the algebra $R_K = K \otimes_k R$ is the *extension of scalars*.

Theorem 3.3.2 (Primitive element)**.** If K/k is a finite separable field extension, then $K = k(c)$ for some $c \in K$.

Proof. Algebra 3, theorem 1.1.8. □

Theorem 3.3.3. Let L/k be a finite field extension. Then $L_K = K \otimes_k L$ is semisimple for all K/k if and only if L/k is separable.

Proof. Suppose that L/k is separable. By the primitive element theorem we can write $L = k(\theta)$. Then L has basis $\{\theta^a \mid 0 \leq a < n\}$ and θ has minimal polynomial f of degree n, that is $L = k[t]/(f)$. Note that L_K has the same basis and θ satisfies the same polynomial condition. It follows that $L_K = K[t]/(f)$. Since f is separable, it factors into distinct irreducible polynomials $f_1, \ldots, f_r$. By the Chinese remainder theorem, we have

$$L_K = K[t]/(f) \cong \prod_{j=1}^{r} K[t]/(f_j)\,.$$

It follows that L_K is a product of fields and therefore semisimple.

Now suppose that L/k is not separable. Suppose that $\theta \in L$ is not separable, that is its minimal polynomial f is not separable. Equivalently, f has repeated factors in $K = k(f)$. Then $k(\theta) = K[t]/(f)$ has nilpotent elements. But as $k(\theta) \subseteq L$, it follows that $(a) \triangleleft L_K$ is nil, therefore $\operatorname{rad} L_K \neq (0)$. □

Corollary 3.3.3.1. The tensor product of two field extensions over k is semisimple, provided one of the factors is finite and separable over k.

3.4 Tensor products, simplicity

Definition 3.4.1. Given an algebra S over k, its *center* is the set

$$Z(S) = \{y \in S \mid \forall x \in S \colon xy = yx\}.$$

We call S *central* over k if $k = Z(S)$. We call S *central simple* if S is both simple and central.

Lemma 3.4.2. Let S and R be algebras over k with S being central simple. If $J \triangleleft R \otimes S$ is a non-trivial ideal, then $J \cap R \neq (0)$.

Proof. Let $x \in J$ be a minimal[8] non-zero element. Write

$$x = \sum_{i=1}^{\ell} r_i \otimes s_i.$$

Then both $(r_i)_i$ and $(s_i)_i$ are k-linearly independent. In particular, $s_1 \neq 0$ and thus $(s_1) = S$. We therefore have

$$1 = \sum_{i=1}^{m} x_i s_1 y_i.$$

Let

$$x' = \sum_{j=1}^{m} (1 \otimes x_j) x (1 \otimes y_j) = \sum_{j=1}^{m} \left(\sum_{i=1}^{\ell} r_i \otimes x_j s_i y_j \right) = \sum_{i=1}^{\ell} r_i \otimes \sum_{j=1}^{m} x_j s_i y_j = \sum_{i=1}^{\ell} r_i \otimes s_i'.$$

Note that $s_1' = 1$. Obviously, $x' \in J$. As $(r_i)_i$ are S-linearly independent, we get $x' \neq 0$.

For any $s \in S$ observe the element

$$y = (1 \otimes s)x' - x'(1 \otimes s) = \sum_{i=1}^{\ell} r_i \otimes s s_i' - \sum_{i=1}^{\ell} r_i \otimes s_i' s = \sum_{i=1}^{\ell} r_i \otimes (s s_i' - s_i' s) = \sum_{i=2}^{\ell} r_i \otimes (s s_i' - s_i' s).$$

As $y \in J$, we have $y = 0$ by minimality of x. It follows that $s_i' \in Z(S) = k$ for all i. Now rewrite

$$x' = \sum_{i=1}^{\ell} r_i \otimes s_i' = \left(\sum_{i=1}^{\ell} r_i s_i' \right) \otimes 1 \in R. \qquad \square$$

Theorem 3.4.3. Let S and R be algebras over k with S being central simple.

i) Every two-sided ideal of $R \otimes S$ has the form $I \otimes S$ for some ideal $I \triangleleft R$. In particular, if R is simple, then so is $R \otimes S$.

ii) We have $Z(R \otimes S) = Z(R)$. In particular, if $R = K$ is a field, then $S_K = K \otimes S$ is a central simple algebra over K.

[8] With respect to the length of basis expansions.

Proof.

i) Let $J \triangleleft R \otimes S$ be an ideal and let $I = J \cap R$. Consider the map $\psi\colon R \otimes S \to (R/I) \otimes S$ with $\psi(r \otimes s) = (r + I) \otimes s$. We claim that $\ker \psi = I \otimes S$. Pick a basis $(x_i)_i$ for $I \subseteq R$ and extend it to a basis $(x_i, y_j)_{i,j}$ of R. Then $(y_j + I)_j$ is a basis for R/I. Now note that

$$\sum x_i \oplus a_i + \sum y_j \otimes b_j \in \ker \psi \iff \forall j\colon b_j = 0.$$

By the isomorphism theorem, we have

$$R \otimes S \Big/ I \otimes S \cong R \Big/ I \otimes S.$$

Note that $I \otimes S \subseteq J$. If $I \otimes S \subset J$, the image of the map $\Phi\colon J \to R \otimes S/I \otimes S$ is nonzero. By the above lemma, we have $\mathrm{im}(\Phi) \cap R/I \neq (0)$, which is in contradiction with the choice of I.

ii) Let $x = \sum r_i \otimes s_i \in Z(R \otimes S)$, where r_i are linearly independent. For any $s \in S$, we can write

$$0 = (1 \otimes s)x - x(1 \otimes s) = \sum r_i \otimes (ss_i - s_i s),$$

therefore $s_i \in Z(S) = k$ for all i. It follows that

$$\sum r_i \otimes s_i = \sum r_i s_i \otimes 1 = r \otimes 1.$$

Now, for $y \in R$, we must also have

$$0 = (y \otimes 1)x - x(y \otimes 1) = (yr - ry) \otimes 1,$$

therefore $r \in Z(R)$, as desired. □

Corollary 3.4.3.1. If R and S are central simple algebras, then so is $R \otimes S$.

Remark 3.4.3.2. If $R = R_1 \times R_2$, then $R \otimes S = (R_1 \otimes S) \times (R_2 \otimes S)$.

Proposition 3.4.4. Suppose that S is a simple k-algebra with center C. Then S is a central simple algebra over C and $C \cong \mathrm{End}_{S \otimes S^{\mathsf{op}}}(S)$.

Proof. Note that, for $a \in C \setminus \{0\}$, we have $(a) = S$. It follows that $1 = ab = ba$ for some $b \in S$. In particular, C is a field.

Now let $\Phi\colon C \to \mathrm{End}_{S \otimes S^{\mathsf{op}}}(S)$ be given by $\Phi(c) = (s \mapsto cs)$. First observe that this is in fact a well defined map, as

$$\Phi(c)\,(s_1 \otimes s_2^{\mathsf{op}} \cdot s) = \Phi(c)(s_1 s s_2) = c s_1 s s_2 = s_1 \otimes s_2^{\mathsf{op}} \cdot cs = s_1 \otimes s_2^{\mathsf{op}} \cdot \Phi(c)(s).$$

It is clear that the map is a field homomorphism. Suppose that $\Phi(c) = \Phi(d)$. Then, $\Phi(c)(1) = \Phi(d)(1)$, hence $c = d$ and Φ is injective. Now choose an arbitrary $\varphi \in \mathrm{End}_{S \otimes S^{\mathsf{op}}}(S)$ and set $x = \varphi(1)$. Observe that

$$sx = s \otimes 1^{\mathsf{op}} \cdot x = \varphi\,(s \otimes 1^{\mathsf{op}} \cdot 1) = \varphi(s) = \varphi\,(1 \otimes s^{\mathsf{op}} \cdot 1) = 1 \otimes s^{\mathsf{op}} \cdot x = xs,$$

therefore $x \in C$. It is evident that $\varphi = \Phi(x)$, hence Φ is surjective and therefore an isomorphism. □

Remark 3.4.4.1. We have $R \otimes_k S = (R \otimes_k C) \otimes_C S$.

Definition 3.4.5. Let S be a finite-dimensional semisimple algebra over k. If $C = Z(S)$, then

$$C = \prod_{i=1}^{m} C_i$$

for some fields C_i. The algebra S is *separable* if each C_i/k is separable.

Proposition 3.4.6. If S is separable, then S_K is semisimple for all field extensions K/k.

Theorem 3.4.7. If D is a finite-dimensional division algebra over $k = Z(D)$, then $\dim_k D$ is a perfect square.

Proof. Note that $\dim_k D = \dim_{\overline{k}} D_{\overline{k}}$, where $\overline{k}$ is the algebraic closure of k and $D_{\overline{k}} = \overline{k} \otimes D$. This is a simple artinian algebra, so by Wedderburn's theorem $D_{\overline{k}} \cong M_n(E)$ for some finite-dimensional division algebra E over $\overline{k}$. It follows that $E = \overline{k}$ as it is algebraically closed, therefore $\dim_{\overline{k}} D_{\overline{k}} = n^2$. □

Corollary 3.4.7.1. If A is a finite-dimensional simple algebra over $Z(A)$ then $\dim_{Z(A)} A$ is a perfect square.

Proof. By Wedderburn we have $A \cong M_n(D)$ for some finite-dimensional division algebra D over $Z(A)$. But then

$$[A : Z(A)] = [A : D] \cdot [D : Z(A)] = n^2 \cdot [D : Z(A)],$$

which is a perfect square. □

Proposition 3.4.8. For all finite-dimensional central simple algebra R over k we have $R \otimes R^{\mathsf{op}} \cong M_n(k)$, where $n = \dim_k R$.

Proof. Denote

$$A = \{L_r \in \mathrm{End}_k(R) \mid r \in R\} \quad \text{and} \quad B = \{T_r \in \mathrm{End}_k(R) \mid r \in R\},$$

where $L_r(x) = rx$ and $T_r(x) = xr$. Note that $A \cong R$ and $B \cong R^{\mathsf{op}}$. Elements of A and B obviously commute.

By the universal property there exists a homomorphism $\Omega\colon R \otimes R^{\mathsf{op}} \to \mathrm{End}_k(R)$ given by $\Omega(r \otimes s) = L_r \circ T_s$. As both R and R^{op} are central simple algebras, $R \otimes R^{\mathsf{op}}$ is simple and Ω is injective. Since the dimensions are equal, Ω is an isomorphism. □

3.5 Skolem-Noether theorem

Lemma 3.5.1. Let R be a finite-dimensional simple k-algebra. Suppose M_1 and M_2 are R-modules that are finite-dimensional over k. If $\dim_k M_1 = \dim_k M_2$, then $M_1 \cong M_2$.

Proof. Note that R is simple and artinian. By Wedderburn's theorem there exists a unique simple R-module M, thus $M_j \cong M^{\alpha_j}$. As dimensions are equal, $\alpha_1 = \alpha_2$. □

Theorem 3.5.2 (Skolem-Noether)**.** Let S be a finite-dimensional central simple algebra over k and R be a simple k-algebra. If $f, g\colon R \to S$ are homomorphisms, then there exists an inner automorphism $\alpha\colon S \to S$ such that $\alpha \cdot f = g \cdot \alpha$.

Proof. Note that S is artinian, so by Wederburn's theorem $S \cong \mathrm{End}_D(V)$ for some division algebra D and finite-dimensional vector space V over D.

Homomorphisms f and g induce an R-module structure on V by $r \cdot v = f(r)v$ and $r \cdot g = g(r)v$. These two actions obviously commute with the actions of D. The space V becomes an $R \otimes D$-module in two different ways. Now as $R \otimes D$ is artinian and simple, the two modules are isomorphic by the previous lemma. That is, there exists an abelian group isomorphism $h\colon V \to V$ such that $h(f(r) \cdot v) = g(r) \cdot h(v)$ and $h(dv) = dh(v)$ holds for all $d \in D$, $r \in R$ and $v \in V$. But then $h \in \mathrm{End}_D(V) = S$ and $h \cdot f(r) = g(r) \cdot h$. □

Remark 3.5.2.1. Equivalently, if R_1 and R_2 are simple subalgebras of S, then for all homomorphisms $f\colon R_1 \to R_2$ there exists an inner automorphism $\alpha\colon S \to S$ such that $\alpha|_{R_1} = f$. In particular, every automorphism of S is inner.

Corollary 3.5.2.2. If $\alpha\colon M_n(k) \to M_n(k)$ is an automorphism, then there exists a matrix $P \in \mathrm{GL}_n(k)$ such that $\alpha(x) = P^{-1}xP$ for all $x \in M_n(k)$.

3.6 The (double) centralizer theorem

Definition 3.6.1. Let R be an algebra and $S \subseteq R$. The *centralizer* of S in R is the subalgebra

$$C_R(S) = C(S) = \{r \in R \mid \forall s \in S \colon rs = sr\}.$$

Remark 3.6.1.1. If S is a central simple algebra, then $C(C(S)) = C(k) = S$.

Remark 3.6.1.2. For arbitrary R, we have $R \subseteq C(C(R))$.

Definition 3.6.2. Let S be a finite-dimensional simple algebra. By Wedderburn's theorem, $S \cong M_n(D)$ for a division ring D. We write $S \sim D$ and say that S and D are *equivalent*.

Remark 3.6.2.1. Note that the division ring D is unique.

Theorem 3.6.3 (Centralizer)**.** Let S be a finite-dimensional central simple algebra over k and R be a simple subalgebra of S.

i) The subalgebra $C(R)$ is simple.

ii) If $S \sim D_1$ and $R \otimes D_1^{\mathsf{op}} \sim D_2$, then $C(R) \sim D_2^{\mathsf{op}}$.

iii) We have $[S : k] = [R : k] \cdot [C(R) : k]$.

iv) We have $C(C(R)) = R$.[9]

Proof. Applying Wedderburn's theorem to S, we get $S \cong \mathrm{End}_D(V) \cong M_n(D^{\mathsf{op}})$, where D is a division algebra and V a n-dimensional D-vector space. Note that V is an $R \otimes D$-module and $C(R) = \mathrm{End}_{R\otimes D}(V)$.

i) The algebra $R \otimes D$ is simple, therefore it is isomorphic to $\mathrm{End}_E(W)$ where W is the unique simple $R \otimes D$-module and $E = \mathrm{End}_{R\otimes D}(W)$. By Wedderburn, we have $V \cong W^m$ as an $R \otimes D$-module. Then

$$C(R) = \mathrm{End}_{R\otimes D}(V) \cong \mathrm{End}_{R\otimes D}(W^m) \cong M_n(\mathrm{End}_{R\otimes D}(W)) = M_n(E),$$

which is simple.

ii) We have $S \sim D^{\mathsf{op}} = D_1$ and $R \otimes D_1^{\mathsf{op}} = R \otimes D \sim E^{\mathsf{op}} = D_2$. It follows that $C(R) \sim E = D_2^{\mathsf{op}}$.

iii) We have $C(R) \cong M_m(E)$, therefore $[C(R) : k] = m^2 \cdot [E : k]$. We also have

$$[V : k] = m \cdot [W : k] = m \cdot [W : E] \cdot [E : k],$$

hence

$$[C(R) : k] = m^2 \cdot \frac{[V : k]^2}{m^2 \cdot [W : E]^2 \cdot [E : k]} = \frac{[V : k]^2}{[W : E]^2 \cdot [E : k]}.$$

Note that W is a vector space over D, therefore $W \cong E^d$ and $R \otimes D \cong M_d(E^{\mathsf{op}})$. It follows that

$$[R : k] \cdot [D : k] = [R \otimes D : k] = d^2 \cdot [E : k] = [W : E]^2 \cdot [E : k].$$

[9] Also known as the *double centralizer theorem*.

Returning to the centralizer, we get

$$[C(R):k] = \frac{[V:k]^2}{[W:E]^2 \cdot [E:k]} = \frac{[V:k]^2}{[R:k] \cdot [D:k]} = \frac{[V:D]^2 \cdot [D:k]}{[R:k]} = \frac{[S:k]}{[R:k]}.$$

iv) Note that

$$[R:k] \cdot [C(R):k] = [S:k] = [C(R):k] \cdot [C(C(R)):k]. \qquad \square$$

Corollary 3.6.3.1. If R is a central simple algebra contained in a finite-dimensional central simple algebra S, then $S \cong R \otimes C(R)$.

Proof. Consider the homomorphism $\Psi\colon R \otimes C(R) \to S$ with $\Psi(r \otimes r') = rr'$. Since $R \otimes C(R)$ is simple, Ψ is injective, but given

$$[S:k] = [R:k] \cdot [C(R):k] = [R \otimes C(R):k],$$

we conclude Ψ is an isomorphism. $\square$

Definition 3.6.4. Let D be a division algebra over k. A field $K \supseteq k$ such that $D_K = D \otimes D \cong M_n(K)$ is called a *splitting filed* for D.

A central simple algebra of the form $M_n(k)$ is a *split* central simple algebra. We call n the *degree* of D and the number n^2 the *rank* of D.

Remark 3.6.4.1. The algebraic closure of k is a splitting field for any finite-dimensional division algebra D over k.

Remark 3.6.4.2. If K splits D and K'/K is an extension of K, then K' also splits D, as

$$D_{K'} \cong K' \otimes_K D_K \cong K' \otimes_K M_n(K) \cong M_n(K').$$

Proposition 3.6.5. Let D be a division algebra with center k and $[D:k] = n^2$. If K is a maximal subfield of D, then $[K:k] = n$. Furthermore, any such K is a splitting field for D.

Proof. For $\alpha \in C(K) \setminus K$ the field $K(\alpha)$ is a proper field extension of K. As K is maximal, this is not possible, so we have $C(K) \subseteq K$ and therefore $C(K) = K$. We can then write

$$n^2 = [D:k] = [K:k] \cdot [C(K):k] = [K:k]^2.$$

Note that D is a simple $D \otimes K$-module, therefore

$$\mathrm{End}_{D \otimes K}(D) \cong C_D(K)^{\mathsf{op}} = K^{\mathsf{op}} = K.$$

Since $D \otimes K$ is simple, it is isomorphic to matrices over $\mathrm{End}_{D \otimes K}(D) \cong K$. $\square$

Theorem 3.6.6 (Wedderburn-Koethe)**.** In any finite-dimensional division algebra there is a separable maximal subfield.

3.7 Theorems about division rings

Theorem 3.7.1 (Little Wedderburn)**.** Every finite division ring is a field.

Proof. Let D be a finite division ring and denote $k = Z(D)$. Let K be a maximal subfield of D and assume $K \neq D$. Since $[D : k] = n^2$ for some $n \in \mathbb{N}$, we have $[K : k] = n$ by 3.6.5. If $|k| = q = p^m$, then $|K| = q^n$. Any two subfields of D of order q^n are isomorphic. By the Skolem-Noether theorem, they are conjugate.

Every element of D is contained in a maximal subfield, so we have

$$D = \bigcup_{x \in D^{-1}} xKx^{-1},$$

so

$$D^{-1} = \bigcup_{x \in D^{-1}} xK^{-1}x^{-1}.$$

This is not possible, as a finite group cannot be a union of conjugates of a proper subgroup. □

Theorem 3.7.2 (Frobenius)**.** Let D be a division algebra with $\mathbb{R} \subseteq Z(D)$ and suppose $[D : \mathbb{R}] < \infty$. Then D is either $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

Proof. Without loss of generality assume $[D : \mathbb{R}] > 1$. For any $\alpha \in D \setminus \mathbb{R}$, the field $\mathbb{R}(\alpha)$ is a proper algebraic field extension of $\mathbb{R}$, so $\mathbb{R}(\alpha) = \mathbb{C}$. Fix a copy of $\mathbb{C}$ in D and define

$$D^+ = \{d \in D \mid di = id\} \quad \text{and} \quad D^- = \{d \in D \mid di = -id\}.$$

Clearly, $D^+ \oplus D^- = D$. Note that $\mathbb{C}(d)\big/\mathbb{C}$ is an algebraic field extension for every $d \in D^+$. As $\mathbb{C}$ is algebraically closed, $D^+ = \mathbb{C}$.

If $D^- = (0)$, then $D = D^+ = \mathbb{C}$. Otherwise, take $z \in D^- \setminus \{0\}$ and consider the map $\mu \colon D^- \to D^+$ with $\mu(x) = xz$. This is a well defined injective map. As it is linear over $\mathbb{C}$, we have $\dim_{\mathbb{C}} D^- \leq \dim_{\mathbb{C}} D^+ = 1$ and $D^- \cong \mathbb{C}$.

Observe that z is algebraic over $\mathbb{R}$, hence $z^2 \in \mathbb{R} + \mathbb{R}z$. As $z^2 = \mu(z) \in \mathbb{C}$, it follows that $z^2 \in \mathbb{R}$. Of course $z^2 \neq r^2$, as then $z = \pm r \in \mathbb{R}$. Hence $z^2 = -r^2$ for some $r > 0$. Taking $j = \frac{z}{r}$, we find that $j^2 = i^2 = -1$ and $ij = -ji$. □

3.8 Jacobson-Herstein theorem

Proposition 3.8.1. Let D be a division ring. If $y \in D$ commutes with all commutators, then $y \in Z(D)$.

Proof. Assume that $y \notin Z(D)$. Equivalently, there exists some $x \in D$ such that $[x, y] \neq 0$. Note that $[x, xy] = x \cdot [x, y]$, but as y commutes with both $[x, y]$ and $[x, xy]$, it also commutes with x. □

Corollary 3.8.1.1. If all commutators in a division ring D are central, then D is a field.

Proposition 3.8.2. Let D be a division ring and $K \subseteq D$ a finite subring. Then K is a field.

Proof. For every $a \in K \setminus \{0\}$ consider $L_a \colon K \to K$ with $L_a(x) = ax$. This is an injective map, but as K is finite, it is bijective. It follows that K is a division ring. By the little Wedderburn theorem, K is a field. □

Lemma 3.8.3. If F is a field and $G \leq F^{-1}$ is a finite subgroup, then G is cyclic.

Proof. Note that, as G is a finite abelian group, we have

$$G \cong \bigoplus_{i=1}^{r} \mathbb{Z}_{m_i}.$$

Denote $n = \operatorname{lcm}(m_i)$. As $x^n - 1$ has at most n solutions in F, we have $n \leq |G| \leq n$ and therefore $G \cong \mathbb{Z}_n$. □

Corollary 3.8.3.1. Let D be a division ring with $\operatorname{char} D = p > 0$. Then any finite subgroup $G \leq D^{-1}$ is also cyclic.

Proof. Define

$$K = \left\{ \sum_{i=1}^{r} \alpha_i g_i \;\middle|\; r \in \mathbb{N}_0 \wedge \alpha_i \in \mathbb{F}_p \wedge g_i \in G \right\}.$$

As K is a finite subgroup of D, it is a field. By construction $G \leq K^{-1}$, therefore it is cyclic. □

Lemma 3.8.4. Let D be a division ring with $\operatorname{char} D = p > 0$. Suppose that $a \in D$ is non-central and torsion. Then there exists some $y \in D^{-1}$ such that $yay^{-1} = a^i \neq a$ for some $i \in \mathbb{N}$. Furthermore, we can choose y to be a commutator.

Proof. Let $K = \mathbb{F}_p[a]$. Since a is torsion, K is a finite field, thus $|K| = p^n$, in particular, $a^{p^n} = a$. Now define $\delta_a \colon D \to D$ as $\delta_a(r) = [a, r]$. Since a is non-central, we have $\delta_a \neq 0$, but $\delta_a|_K = 0$. It follows that $\delta_a \in \operatorname{End}_K(D)$.

Denote $\delta_a = L_a - R_a$ where $L_a(x) = ax$ and $R_a(x) = xa$. We again have $L_a, R_a \in \operatorname{End}_K(D)$. Now compute

$$(\delta_a)^{p^n} = (L_a - R_a)^{p^n} = L_a^{p^n} + (-R_a)^{p^n} = L_a^{p^n} - R_a^{p^n} = \delta_a.$$

It follows that

$$0 = \delta_a^{p^n} - \delta_a = \prod_{b \in K} (\delta_a - b) = \prod_{b \in K^{-1}} (\delta_a - b) \cdot \delta_a.$$

Since $\delta_a \neq 0$, there exists a map $\delta_a - b$ that is not injective. Such b is an eigenvalue for δ_a – that is, there exists an element $x \in D^{-1}$ such that $\delta_a(x) = bx$.

We can now write $ax - xa = bx$, which is equivalent to

$$xax^{-1} = b - a \in K \setminus 0.$$

As a and xax^{-1} have the same order in the cyclic group K^{-1}, they generate the same subgroup. In particular, $xax^{-1} = a^i \neq a$ for some $i \in \mathbb{N}$.

Instead of x, we can also use $y = [a, x]$. Indeed,

$$ya = (ax - xa) \cdot a = a^i \cdot ax - a^i \cdot xa = a^i y. \qquad \square$$

Theorem 3.8.5 (Jacobson-Herstein)**.** Let D be a division ring. If for all $a, b \in D$ there exists some $n > 1$ such that $(ab - ba)^n = ab - ba$, then D is a field.

Proof. Suppose that $D \neq Z(D)$. By lemma 3.8.1.1 there exists elements $b_1, b_2 \in D$ such that $a = [b_1, b_2] \notin Z(D)$. For each $c \in Z(D) \setminus \{0\}$, we have

$$ca = [cb_1, b_2].$$

By assumption, there exists some $k \geq 1$ such that $1 = a^k = (ca)^k$, therefore $c^k = 1$ as well. In particular, $\mathrm{char}(D) = p > 0$. By the previous lemma there exists a commutator $y \in D$ such that $yay^{-1} = a^i \neq a$. Now observe the group $\langle a \rangle \cdot \langle y \rangle$. This is again a finite group since y normalizes $\langle a \rangle$. It follows that it is cyclic, thus abelian, but this contradicts $yay^{-1} \neq a$. $\square$

4 Brauer group

"The goal of university bureaucrats is for everyone to have an above-average grade."

– prof. dr. Igor Klep

4.1 Definition

Definition 4.1.1. Let S, T be finite-dimensional central simple algebras over k. We say that S and T are *similar* if any of the following equivalent conditions hold:

i) If $S \cong M_n(D)$ and $T \cong M_m(E)$ for division rings D and E, then $D \cong E$.

ii) There exist numbers $m, n \in \mathbb{N}$ such that $S \otimes_k M_m(k) \cong T \otimes_k M_n(k)$.

iii) There exist numbers $m, n \in \mathbb{N}$ such that $M_m(S) \cong M_n(T)$.

iv) If M and N are the unique S and T-modules respectively, then we have $\mathrm{End}_S(M) \cong \mathrm{End}_T(N)$.

In this case we write $S \sim T$.

Remark 4.1.1.1. The tensor product of central simple algebras is again a central simple algebra. The tensor product of division algebras is not necessarily a division algebra.

Definition 4.1.2. Let k be a field. The *Brauer group* $\mathrm{Br}(k)$ of k is the set of equivalence classes of finite-dimensional central simple algebras over k with respect to the similarity relation. The group operation is induced by the tensor product.

Remark 4.1.2.1. The identity element is $[k]$.

Remark 4.1.2.2. If k is a finite field or algebraically closed, then the Brauer group is trivial.

Remark 4.1.2.3. We have $[M_n(k)] = [k]$.

Remark 4.1.2.4. If A and B are finite-dimensional central simple algebras over k, then $A \cong B$ if and only if $[A] = [B]$ and $\dim A = \dim B$.

Lemma 4.1.3. We have the following:

i) For all k-algebras R, we have $M_n(R) \cong R \otimes_k M_n(k)$.

ii) We have $M_m(k) \otimes M_m(k) \cong M_{mn}(k)$.

Lemma 4.1.4. If $S_1 \sim S_2$ and $T_1 \sim T_2$, then $S_1 \otimes T_1 \sim S_2 \otimes T_2$.

Proof. Set $S_j \cong M_{n_j}(D)$ and $T_j \cong M_{m_j}(E)$. Then

$$\begin{aligned} S_j \otimes T_j &\cong M_{n_j}(D) \otimes M_{m_j}(E) \\ &\cong D \otimes M_{n_j}(k) \otimes M_{m_j}(k) \otimes E \\ &\cong D \otimes E \otimes M_{n_j m_j}(k) \\ &\cong M_{n_j m_j}(D \otimes E). \end{aligned}$$

□

Theorem 4.1.5. The set $\mathrm{Br}(k)$ is an abelian group.

Proof. By the above lemma, the operation is well defined. It is obviously associative, commutative and has unit $[k]$. Note that every element has an inverse, as

$$S \otimes S^{\mathsf{op}} \cong M_n(k) \sim k. \qquad \square$$

4.2 Relative Brauer group

Definition 4.2.1. Let K/k be a field extension and $\Phi\colon \mathrm{Br}(k) \to \mathrm{Br}(K)$ a homomorphism, given by $\Phi([S]) = [K \otimes_k S]$. The *relative Brauer group* is the group

$$\mathrm{Br}\left(K/k\right) = \ker\left(\Phi\right).$$

Remark 4.2.1.1. These are precisely the central division algebras over k that split over K.

Definition 4.2.2. Let S be a simple k-algebra. A *self-centralizing subfield* of S is a field $K \subseteq S$ such that $C(K) = K$.

Remark 4.2.2.1. In division rings, maximal subfields coincide with self-centralizing ones. This is not true in general and in fact fails for some central simple algebras (even when both exist).

Theorem 4.2.3. The following statements are true:

i) Let S be a central simple algebra over k with $\dim_k S = n^2$. Then any self-centralizing subfield K of S is a splitting field for S and $[K : k] = [S : k] = n$.

ii) Given any field extension K/k with $[K : k] = n$, any element of $\mathrm{Br}\left(K/k\right)$ has a unique representative S of degree n^2 that contains K as a self-centralizing subfield.

Proof.

i) Using the centralizer theorem, we find that

$$n^2 = [S : k] = [K : k] \cdot [C(K) : k] = [K : k]^2.$$

It remains to check that K is a splitting field for S. Let $f\colon S \otimes_k K \to \mathrm{End}_K(S) \cong M_n(K)$ be given by $f(s \otimes x) = (s' \mapsto ss'x)$. As S is central simple and K is simple, their tensor product $S \otimes_k K$ is central simple. As f is not constant, it must therefore be injective. But as

$$[S \otimes K : k] = n^3 = [M_n(K) : k],$$

the map f must be an isomorphism.

ii) Let $[D] \in \mathrm{Br}\left(K/k\right)$ for a division algebra D. Equivalently, $K \otimes_k D^{\mathsf{op}} \cong M_m(K)$ for some positive integer m. In particular, $[D^{\mathsf{op}} : k] = m^2$.

Let V be the unique $K \otimes_k D^{\mathsf{op}}$-module. As $K \otimes_k D^{\mathsf{op}} \cong V^m$, we then have

$$[K : k] \cdot [D^{\mathsf{op}} : k] = [K \otimes_k D^{\mathsf{op}} : k] = [V^m : k] = m \cdot [V : k] = m \cdot [V : D^{\mathsf{op}}] \cdot [D^{\mathsf{op}} : k].$$

Observe that K acts on V and that the action commutes with D^{op}. We can therefore embed K into $\mathrm{End}_{D^{\mathsf{op}}}(V) \cong M_{[V:D^{\mathsf{op}}]}(D) = S$. Clearly $[S] = [D]$, and

$$[S : k] = [V : D^{\mathsf{op}}]^2 \cdot [D : k] = [V : D^{\mathsf{op}}]^2 \cdot m^2 = [K : k]^2.$$

By the double centralizer theorem, we find that $[K : k]^2 = [S : k] = [K : k] \cdot [C(K) : k]$. It follows that $[K : k] = [C(K) : k]$, but as $K \subseteq C(K)$, we must have equality. It follows that S is indeed self-centralizing. It is unique by the dimension requirement. □

Remark 4.2.3.1 (Jacobson-Noether theorem)**.** For any division algebra with center k there exists a splitting field $K \subseteq D$ that is separable over k.

Corollary 4.2.3.2. Let D be a finite-dimensional division algebra with center k. Then there exists a finite Galois extension K/k which is a splitting field for D.

Proof. By the Jacobson-Noether theorem there exists a maximal splitting subfield $L \subseteq D$ that is separable over k. Let K be the normal closure of L. Then K/k is a Galois extension and

$$D \otimes_k K \cong (D \otimes_k L) \otimes_L K \cong M_n(L) \otimes_L K \cong M_n(K). \qquad \square$$

Corollary 4.2.3.3. Suppose that D is a central division k-algebra with $[D : k] = n^2$. Then any splitting field K of D satisfies $n \mid [K : k]$.

Proof. Note that $D \otimes_k K \cong M_n(K)$ by comparing dimensions over k. Let V be the unique simple $M_n(K)$-module. In particular, $V \cong K^n$. As V is also a D-vector space, we can write $V \cong D^s$. But then

$$sn^2 = s \cdot [D : k] = [V : k] = n \cdot [K : k]. \qquad \square$$

4.3 Factor sets and crossed product algebras

Definition 4.3.1. Let K/k be a Galois field extension and denote $G = \mathrm{Gal}\,(K/k)$. Let S be a central simple k-algebra with center K. For every $\sigma \in G$ choose an element $x_\sigma \in S^{-1}$ such that $x_\sigma \cdot a \cdot x_\sigma^{-1} = \sigma(a)$ for all $a \in K$. Furthermore, let $a_{\sigma,\tau} = x_\sigma \cdot x_\tau \cdot x_{\sigma\tau}^{-1}$. The set $(a_{\sigma,\tau})_{\sigma,\tau\in G}$ is called the *factor set* of S relative to K.

Remark 4.3.1.1. Such elements x_σ exist by the Skolem-Noether theorem. A simple calculation shows that $a_{\sigma,\tau} \in K$ as $x_\sigma^{-1} \cdot x'_\sigma \in K$.

Definition 4.3.2. A factor set is *normalized* if $x_{\mathrm{id}} = 1$.

Remark 4.3.2.1. If the factor set is normalized, we have $a_{\sigma,\mathrm{id}} = a_{\mathrm{id},\sigma} = 1$.

Remark 4.3.2.2. Suppose that $x'_\sigma = f_\sigma \cdot x_\sigma$ gives a factor set $(b_{\sigma,\tau})_{\sigma,\tau\in G}$. Then

$$b_{\sigma,\tau} f_{\sigma,\tau} x_{\sigma,\tau} = b_{\sigma,\tau} x'_{\sigma,\tau} = x'_\sigma x'_\tau = f_\sigma x_\sigma f_\tau x_\tau = f_\sigma \sigma(f_\tau) x_\sigma x_\tau,$$

therefore

$$b_{\sigma,\tau} = \frac{f_\sigma \sigma(f_\tau)}{f_{\sigma,\tau}} a_{\sigma,\tau}.$$

Proposition 4.3.3. The set $(x_\sigma)_{\sigma\in G}$ is a basis for S over K.

Proof. Observe that $|G| = [K : k] = [S : K]$, therefore we only need to check linear independence. Suppose then that they are linearly dependent and let $J \subset G$ be a maximal set such that $(x_\sigma)_{\sigma\in J}$ is linearly independent.

Let $\sigma \in G \setminus J$ and write

$$x_\sigma = \sum_{\tau\in J} a_\tau x_\tau$$

for $a_\tau \in K$. For any $r \in K$, we find that

$$\sum_{\tau\in J} \sigma(r) a_\tau x_\tau = \sigma(r) x_\sigma = x_\sigma r = \sum_{\tau\in J} a_\tau x_\tau r = \sum_{\tau\in J} a_\tau \tau(r) x_\tau.$$

By linear independence, we must have $\sigma(r)a_\tau = a_\tau\tau(r)$ for all $\tau \in J$. But as at least one of a_τ is non-zero, in which case we have $\sigma(r) = \tau(r)$ and therefore $\sigma = \tau \in J$. □

Corollary 4.3.3.1. As a K-vector space,

$$S = \bigoplus_{\sigma\in G} K x_\sigma$$

with multiplication $x_\sigma \cdot a = \sigma(a) \cdot x_\sigma$ and $x_\sigma \cdot x_\tau = a_{\sigma,\tau} x_{\sigma\tau}$.

Definition 4.3.4. Any set $(a_{\sigma,\tau})_{\sigma,\tau} \subseteq K^{-1}$ that satisfies

$$\rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} = a_{\rho,\sigma} \cdot a_{\rho\sigma,\tau}$$

is called a *factor set* relative to K.

Remark 4.3.4.1. Note that a factor set of S is indeed a factor set by this definition, as

$$\rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} x_{\rho\sigma\tau} = \rho(a_{\sigma,\tau}) x_\rho x_{\sigma\tau} = x_\rho x_\sigma x_\tau = a_{\rho,\sigma} a_{\rho\sigma,\tau} x_{\rho\sigma\tau}.$$

Proposition 4.3.5. Let K/k be a Galois extension with $G = \mathrm{Gal}(K/k)$. Then any factor set relative to K is a factor set of some central simple algebra over K. Furthermore, A contains K as a self-centralizing subfield.

Proof. Let A be the K-vector space with basis $(e_\sigma)_{\sigma\in G}$. We define multiplication on A as

$$\alpha e_\sigma \cdot \beta e_\tau = \alpha\sigma(\beta)a_{\sigma,\tau}e_{\sigma\tau}.$$

Associativity follows from the fact that $(a_{\sigma,\tau})_{\sigma,\tau\in G}$ is a factor set. Note that $a_{\mathrm{id},\mathrm{id}}^{-1}e_{\mathrm{id}}$ is the identity element. Then K is clearly a subfield of A by inclusion $r \mapsto ra_{\mathrm{id},\mathrm{id}}^{-1}e_{\mathrm{id}}$.

Next, we prove that K is self-centralizing. Suppose that

$$x = \sum_{\sigma\in G} a_\sigma e_\sigma \in C(K).$$

Multiplication by $a \in K$ gives us $aa_\sigma = a_\sigma a$ for all σ. If $a_\sigma \neq 0$ for some $\sigma \neq \mathrm{id}$, this gives a clear contradiction as $a = \sigma(a)$ does not hold for all $a \in K$. Hence $x \in K$.

We now check that $Z(A) = K$. Clearly, $Z(A) \subseteq K$. Let $a \cdot e_{\mathrm{id}} \in Z(A)$. In particular, $ae_{\mathrm{id}}e_\sigma = e_\sigma ae_{\mathrm{id}}$, which implies

$$aa_{\mathrm{id},\sigma}e_\sigma = \sigma(a)a_{\sigma,\mathrm{id}}e_\sigma.$$

But as $a_{\mathrm{id},\sigma} = a_{\mathrm{id},\mathrm{id}}$ and $a_{\sigma,\mathrm{id}} = \sigma(a_{\mathrm{id},\mathrm{id}})$ by definition, it follows that

$$a \cdot a_{\mathrm{id},\mathrm{id}} = \sigma(a \cdot a_{\mathrm{id},\mathrm{id}}),$$

hence $aa_{\mathrm{id},\mathrm{id}} \in K^G = k$. But then

$$a \cdot e_{id} = aa_{\mathrm{id},\mathrm{id}} \cdot a_{\mathrm{id},id}^{-1}e_{\mathrm{id}} \in k.$$

Finally, we prove that A is simple. Suppose that $I \triangleleft A$ is a proper ideal. Then the map $K \mapsto A/I$ is injective. Let $\overline{e}_\sigma$ be the image of e_σ in A/I. Then $\overline{e}_\sigma a = a\overline{e}_\sigma$ for all $a \in k$. Similarly as above, we can see that $(\overline{e}_\sigma)_{\sigma\in G}$ are linearly independent, hence $\dim A/I \geq |G| = \dim A$. It follows that $I = (0)$. □

Definition 4.3.6. The above algebra A is called the *crossed product* of K and G relative to the factor set $(a_{\sigma,\tau})_{\sigma,\tau\in G}$. We write $A = (K, G, a)$.

Lemma 4.3.7. For factor sets with $x'_\sigma = f_\sigma \cdot x_\sigma$ with factor sets b and a, the map $(K, G, b) \to (K, G, a)$, given by $x'_\sigma \mapsto f_\sigma x_\sigma$, is a k-algebra isomorphism.

Theorem 4.3.8. Let K/k be a finite Galois extension with $G = \mathrm{Gal}(K/k)$. Then there exists a bijective correspondence between $\mathrm{Br}(K/k)$ and equivalence classes[10] of factor sets.

Proof. Recall that for each $x \in \mathrm{Br}(K/k)$ there exists a unique central simple algebra A such that $[A] = x$. This gives rise to a map $\mathrm{Br}(K/k)$ and factor sets. Conversely, the crossed product algebras give us the reverse map. It is clear that they are inverses. □

[10] Factor sets are equivalent if they satisfy the equation in remark 4.3.2.2.

4.4 Group cohomology and Brauer group

Definition 4.4.1. Let G be a group that acts on an abelian group M. The n-th *cochain group* is the group $C^n(G, M) = \{f \colon G^n \to M\}$ under pointwise addition.

Remark 4.4.1.1. The group G acts on $C^n(G, M)$.

Definition 4.4.2. The n-th *coboundary map* is the homomorphism $\delta_n \colon C^n(G, M) \to C^{n+1}(G, M)$, defined as

$$\delta_n f = g_1 f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n).$$

Proposition 4.4.3. For all $n \in \mathbb{N}_0$ we have $\delta_n \circ \delta_{n+1} = 0$.

Proof. Direct calculation. □

Definition 4.4.4. The sequence $(C^n(G, M), \delta_n)$ forms a *cochain complex*. We define *n-cocylces* as $Z^n = \ker(\delta_n)$ and *n-coboundaries* as $\mathrm{x}B^n = \mathrm{im}(\delta_{n-1})$.

Definition 4.4.5. The *n-th cohomology group* of G with coefficients in M is the group

$$H^n(G, M) = {}^{Z^n}\big/_{B^n}\,.$$

Definition 4.4.6. Let ${}^{K}/_{k}$ be a finite Galois extension, $G = \mathrm{Gal}\,({}^{K}/_{k})$ and $M = K^{-1}$. The *n-th Galois cohomology group* of the extension ${}^{K}/_{k}$ with coefficients in K^{-1} is the group $H^n\,(G, K^{-1})$.

Lemma 4.4.7. Let K be a field and $\sigma_1, \ldots, \sigma_n$ be distinct automorphisms of K. Then $\sigma_1, \ldots, \sigma_n$ are linearly independent.

Proof. Permuting the automorphisms if needed, suppose that

$$\sum_{j=1}^{r} c_j \sigma_j = 0,$$

where $c_j \neq 0$ and r is minimal. Note that $r > 1$, as otherwise we'd have $0 = c_1\sigma_1(1) = c_1$.

There exists some $a \in K$ such that $\sigma_1(a) \neq \sigma_r(a)$. For all $x \in K$ we have

$$0 = \sum_{j=1}^{r} c_j \sigma_j(ax) = \sum_{j=1}^{r} c_j \sigma_j(a)\sigma_j(x).$$

But then

$$\sum_{j=1}^{r-1} \left(c_j \cdot (\sigma_j(a) - \sigma_r(a))\right) \sigma_j(x) = 0,$$

which is a contradiction. □

Theorem 4.4.8 (Hilbert's theorem 90)**.** The first two Galois cohomology groups are $H^0(G, K^{-1}) = k^{-1}$ and $H^1(G, K^{-1}) = 1$, respectively.

Proof. Notice that

$$\ker \delta_0 = \left\{ f \in K^{-1} \;\middle|\; \forall g \in G \colon gf = f \right\} = K^{\mathrm{Gal}(K/k)} \setminus \{0\} = k^{-1},$$

which proves $H^0(G, K^{-1}) = k^{-1}$.

Now let $f \in Z^1$, that is

$$1 = (\delta_1 f)(\sigma, \tau) = \sigma(f(\tau)) \cdot f(\sigma\tau)^{-1} \cdot f(\sigma).$$

Equivalently, we have

$$f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau)).$$

We claim that $f \in B^1$, which is equivalent to $f = \delta_0 g$ for $g \in K^{-1}$, that is

$$f(\tau) = \tau(g) \cdot g^{-1}.$$

Consider

$$\sum_{\tau \in G} f(\tau)\tau.$$

By the above lemma, this linear combination is non-zero. Choose $a \in K^{-1}$ such that

$$b = \sum_{\tau \in G} f(\tau)\tau(a) \neq 0.$$

We now have

$$\sigma(b) = \sum_{\tau \in G} \sigma(f(\tau)) \cdot (\sigma\tau)(a) = f(\sigma)^{-1} \cdot \sum_{\tau \in G} f(\sigma\tau) \cdot (\sigma\tau)(a) = f(\sigma)^{-1} \cdot b.$$

We therefore have

$$f(\sigma) = \frac{b}{\sigma(b)} = \frac{\sigma(b^{-1})}{b^{-1}}.$$

□

Remark 4.4.8.1. Observe that $1 = \delta_2(a)(\rho, \sigma, \tau)$ is equivalent to

$$\rho(a_{\sigma,\tau}) \cdot a_{\rho,\sigma\tau} = a_{\rho,\sigma} \cdot a_{\rho\sigma,\tau}.$$

That is, cocycles of $C^2(G, K^{-1})$ are precisely factor sets relative to K. As $B^2(G, K^{-1})$ consists of elements $\sigma(f_\tau) f_{\sigma,\tau}^{-1} f_\sigma$, the second cohomology group is in bijective correspondence with equivalence classes of factor sets.

Lemma 4.4.9. The map $\Psi \colon H^2(G, K^{-1}) \to \mathrm{Br}\,(K/k)$ with $\Psi(a) = [(K, G, a)]$ is a group isomorphism.

Proof. The map is bijective by the earlier observations. Let $A = [(K, G, a)]$, $B = [(K, G, b)]$ and $C = [(K, G, ab)]$ and define $M = A^{\mathsf{op}} \otimes_K B$ as a K-module. Then M is also a right $A \otimes_k B$-module with the natural multiplication.

We claim that M is a C-module as well. Indeed, let $(u_\sigma)_{\sigma \in G}$, $(v_\sigma)_{\sigma \in G}$ and $(w_\sigma)_{\sigma \in G}$ be basis for A, B and C, and define

$$(x \cdot w_\sigma) \cdot (a \otimes_K b) = x u_\sigma a \otimes_K v_\sigma b.$$

This makes M into a left C-module, as

$$\begin{aligned}(xw_\sigma x' w_\tau) \cdot a \otimes_K b &= x\sigma(x') a_{\sigma,\tau} b_{\sigma,\tau} u_{\sigma\tau} a \otimes_K v_{\sigma\tau} b \\ &= x\sigma(x') a_{\sigma,\tau} u_{\sigma\tau} a \otimes_K b_{\sigma,\tau} v_{\sigma\tau} b \\ &= x\sigma(x') u_\sigma u_\tau a \otimes_K v_\sigma v_\tau b \\ &= x w_\sigma \cdot (x' w_\tau \cdot a \otimes_K b).\end{aligned}$$

It follows that there exists a k-algebra homomorphism $\Phi\colon (A \otimes_k B)^{\mathsf{op}} \to \mathrm{End}_C(M)$, given by $x \mapsto (m \mapsto mx)$. As $A \otimes_k B$ is a central simple algebra, Φ is injective.

Now let $n = |G| = [K : k]$. As $n = [A : K] = [B : K] = [C : K]$, we find that $[M : K] = n^2$. But then $[M : k] = n^2 \cdot [K : k] = n^3 = n \cdot [C : k]$. As C is simple, we get $M \cong C^n$ and therefore

$$\mathrm{End}_C(M) \cong M_n(\mathrm{End}_C(C)) \cong M_n\left(C^{\mathsf{op}}\right) \cong C^{\mathsf{op}} \otimes_k M_n(k).$$

But then $\dim_k \mathrm{End}_C(M) = n^2 \cdot [C : k] = n^4 = \dim_k(A \otimes_k B)$ and Φ is indeed bijective. It follows that $(A \otimes_k B)^{\mathsf{op}} \cong C^{\mathsf{op}} \otimes_k M_n(k)$ and so $A \otimes_k B \sim C$, as required. □

Theorem 4.4.10. If G is a finite group, then $|G| \cdot H^2(G, M) = 0$.

Proof. For $f \in Z^2$, we can express

$$f(g_1, g_2) = g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3).$$

Taking a sum over all $g_3 \in G$, we get

$$|G| \cdot f(g_1, g_2) = g_1 \cdot h(g_2) - h(g_1 g_2) + h(g_1) = \delta_1(h),$$

where

$$h(g) = \sum_{x \in G} f(g, x).$$ □

Remark 4.4.10.1. Similarly, $|G| \cdot H^n(G, M) = 0$.

Corollary 4.4.10.2. For any field k, $\mathrm{Br}(k)$ is a torsion abelian group.

Proof. Recall that $\mathrm{Br}(k)$ is the union of $\mathrm{Br}\left(K/k\right)$ over all Galois extensions K/k. As each such group is torsion, so is $\mathrm{Br}(k)$. □

4.5 Primary decomposition for division algebras

Definition 4.5.1. Let K be a splitting field for a central division algebra D over k, that is $D \otimes_k K \cong M_n(K)$. The *degree* of D is defined as

$$\deg D = n = \sqrt{[D : k]}.$$

Definition 4.5.2. Let A be a central simple algebra over k with $A \cong M_m(D)$ for a division algebra D. The *index* of A is defined as $\operatorname{ind} A = \deg D$. The *exponent* of A is defined as $\exp A = \operatorname{ord}_{\mathrm{Br}(k)}[A]$.

Proposition 4.5.3. For a central simple algebra A over k we have $[A]^{\operatorname{ind} A} = 1$, that is $\exp A \mid \operatorname{ind} A$.

Proof. Write $[A] = [(K, G, a)]$ for some finite Galois extension K/k. As $A \cong M_r(D)$ for some division algebra D, we can write $[D : k] = m^2$ and $\operatorname{ind} A = m$. Furthermore, $[A : k] = n^2$, where $n = mr$. As $[A]^m = [(K, G, a^m)]$, it suffices to show that $a^m \in B^2$.

Let $V = (D^{\mathsf{op}})^r$, which is a left $\mathrm{End}_{D^{\mathsf{op}}}(V)$-module. As $A \cong M_r(D) \cong \mathrm{End}_{D^{\mathsf{op}}}(V)$, it is also an A-module and hence a K-vector space. But then

$$rm^2 = [V : D^{\mathsf{op}}] \cdot [D^{\mathsf{op}} : k] = [V : k] = [V : K] \cdot n = [V : K] \cdot rm,$$

hence $[V : K] = m$.

Fix a basis $\{v_i \mid i \leq m\}$ for V over K. For any $c \in A$, we can write

$$cv_i = \sum_{j=1}^{m} c_{i,j} v_j.$$

This gives us a map $A \to M_m(K)$. Let X_σ be the corresponding matrix for the element x_σ. Then

$$a_{\sigma,\tau} X_{\sigma\tau} v = a_{\sigma,\tau} x_{\sigma\tau} v = x_\sigma (x_\tau v) = x_\sigma X_\tau v = \sigma(X_\tau) X_\sigma v.$$

Hence $a_{\sigma,\tau} X_{\sigma\tau} = \sigma(X_\tau) X_\sigma$. Taking the determinant, we find

$$a_{\sigma,\tau}^m = \frac{\sigma(\det X_\tau) \det X_\sigma}{\det X_{\sigma\tau}},$$

which is of course an element of B^2. □

Proposition 4.5.4. Every prime divisor of $\operatorname{ind} A$ divides $\exp A$.

Proof. Take $[A] = [(K, G, a)] = [M_m(D)] = [D]$ as usual and denote $d = \operatorname{ind} A = \deg D$. Suppose that $p \mid d$. As $|G|^2 = [(K, G, a) : k] = m^2 d^2$, $p \mid |G|$. Let then G_p be the p-Sylow subgroup of G and let $K_p = K^{G_p} \subseteq K$. By the fundamental theorem of Galois theory, $[K : K_p] = p^r$ for some $r \in \mathbb{N}$, and as G_p is a Sylow subgroup, $p \nmid [K_p : k]$. In particular, K_p cannot split A, hence $\exp\left(A_{K_p}\right) \neq 1$.

As $A \otimes_k K = (A \otimes_k K_p) \otimes_{K_p} K$ splits and $[K : K_p] = p^r$, it follows that $\operatorname{ind}\left(A_{K_p}\right) \mid p^r$. But then $\exp\left(A_{K_p}\right) \mid p^r$, hence $p \mid \exp\left(A_{K_p}\right)$. As the scalar extension map $\mathrm{Br}(k) \to \mathrm{Br}(K_p)$, given by $[S] \mapsto [S_{K_p}]$, is a group homomorphism, we get $\exp\left(A_{K_p}\right) \mid \exp A$. □

Proposition 4.5.5. Suppose that D_1 and D_2 are central division algebras with coprime degrees. Then $D_1 \otimes D_2$ is a division algebra.

Proof. We can write $D_1 \otimes D_2 \cong M_m(D)$ for some division algebra D. Write $D_1^{\mathsf{op}} \otimes D_1 \cong M_n(k)$. Then $n = [D_1 : k]$ and

$$M_n(D_2) \cong M_n(k) \otimes D_2 \cong D_1^{\mathsf{op}} \otimes M_m(D) \cong M_m(D_1^{\mathsf{op}} \otimes D) \cong M_m(M_r(D')) \cong M_{mr}(D').$$

By uniqueness of Wedderburn's decomposition, we get $mr = n$ and $D' = D_2$, hence $m \mid n = [D_1 : k]$. Similarly, $m \mid [D_2 : k]$ and so $m = 1$. □

Theorem 4.5.6. Let D be a finite-dimensional central division algebra over k with

$$\deg D = \prod_{i=1}^{r} p_i^{n_i}.$$

Then there exists a unique decomposition

$$D = \bigotimes_{i=1}^{r} D_i,$$

where D_j are central division algebras with $\deg D_j = p_j^{n_j}$.

Proof. It suffices to show that we can write $D = D_1 \otimes D_2$ with $\deg D_j = n_j$ if $n = n_1 n_2$ and $\gcd(n_1, n_2) = 1$. Write $un_1 + vn_2 = 1$ and let D_1 be the unique central division algebra with $[D_1] = [D]^{vn_2}$. Define D_2 similarly. Then $[D_1 \otimes D_2] = [D]$ and $[D_1]^{n_1} = [k]$, hence $\exp D_1 \mid n_1$ and $\exp D_2 \mid n_2$. As $\exp A$ and $\operatorname{ind} A$ have the same prime factors, $(\operatorname{ind} D_1, \operatorname{ind} D_2) = 1$. It follows that $D_1 \otimes D_2$ is in fact a division algebra, therefore $D_1 \otimes D_2 \cong D$. A comparison of dimensions shows that $\deg D_j = n_j$. □

5 Local rings, idempotents and decompositions

"We will finish the drilling by end of August."

– Construction workers

5.1 Local rings

Definition 5.1.1. A ring R is *local* if $R/\operatorname{rad} R$ is a division ring. It is *semilocal* instead if $R/\operatorname{rad} R$ is semisimple.

Theorem 5.1.2. For any ring R, the following statements are equivalent:

i) The ring R has a unique maximal left ideal.

ii) The ring R has a unique maximal right ideal.

iii) The ring R is local.

iv) The set $R \setminus R^{-1}$ is an ideal in R.

v) The set $R \setminus R^{-1}$ is a group under addition.

vi) If for some $a, b \in R$ we have $a + b \in R^{-1}$, then $a \in R^{-1}$ or $b \in R^{-1}$.

Proof. Suppose first that R has a unique maximal left ideal. Then the ring $R/\operatorname{rad} R$ only has the trivial left ideals. In particular, every element $x \in R/\operatorname{rad} R \setminus \{0\}$ has a left inverse y. But then so does y, which means that y has both inverses, hence $xy = yx = 1$. The same argument works for right ideals.

Now suppose that R is a local ring. As there is a bijective correspondence between left (right) ideals in $R/\operatorname{rad} R$ and left (right) ideals in R that contain $\operatorname{rad} R$, it follows that maximal ideals (which by definition contain $\operatorname{rad} R$) must be equal to $\operatorname{rad} R$, therefore both i) and ii) hold.

Continue with the assumption that R is a local ring and recall that x is invertible if and only if $x + \operatorname{rad} R$ is invertible in $R/\operatorname{rad} R$. But that means that $R \setminus R^{-1} = \operatorname{rad} R \triangleleft R$.

The next chain of implications is trivial. We are left to prove that item vi) implies that R is local. Indeed, take $a \in R \setminus \operatorname{rad} R$ and let M be a maximal left ideal of R that does not contain a. By maximality, $M + Ra = R$, hence we can write $m + ba = 1$. By point vi), we find that ba is invertible. Therefore both a and $a + \operatorname{rad} R$ are invertible, and $R/\operatorname{rad} R$ is a division ring. □

Proposition 5.1.3. Let R be a local ring.

i) The ring R has a unique maximal ideal.

ii) The ring R has no non-trivial idempotents.

iii) The ring R is Dedekind-finite.[11]

Proof.

[11] The equation $ab = 1$ implies $ba = 1$.

i) It is clear that $\operatorname{rad} R$ is the unique maximal ideal.

ii) Suppose that $e \in R$ is a non-trivial idempotent. Then $1-e$ is also an idempotent and $e \in R^{-1}$ or $(1-e) \in R^{-1}$. But as $e \cdot (1-e) = 0$, that means that either $e = 0$ or $e = 1$.

iii) Note that, as $(ba)^2 = ba$, we must have $ba = 0$ or $ba = 1$. The first one implies $0 = a \cdot ba = a$, which is impossible. □

Proposition 5.1.4. If each $a \in R \setminus R^{-1}$ is nilpotent, then R is a local ring.

Proof. First note that $Ra \subseteq R \setminus R^{-1}$. Indeed, suppose that $a^k = 0$ where k is minimal. If ba is invertible for some $b \in R$, then $ba \cdot a^{k-1} = 0$, hence $a^{k-1} = 0$, which is a contradiction. But then $Ra \triangleleft R$ is a nil ideal, hence $Ra \subseteq \operatorname{rad} R$. In particular, $a \in \operatorname{rad} R$, which implies that $R \setminus R^{-1} = \operatorname{rad} R$. □

Proposition 5.1.5. Suppose that R is a subring of a division ring D. If for each $d \in D$ we have $d \in R$ or $d^{-1} \in R$,[12] then R is local.

Proof. Suppose that $a + b = x \in R^{-1}$ and set $c = a^{-1}b$. If $c \in R$, then

$$a^{-1} = a^{-1}(a+b)x^{-1} = (1+c)x^{-1} \in R.$$

Otherwise, compute b^{-1} using c^{-1}. □

Definition 5.1.6. Let R be a commutative ring.

i) A set $S \subseteq R$ is *multiplicative* if $1 \in S$ and for all $a, b \in S$ we also have $ab \in S$.

ii) Define an equivalence relation on $R \times S$ by $(a,s) \sim (a',s') \iff \exists u \in S\colon u(as' - a's) = 0$. Denote $\frac{a}{s} = [(a,s)]_\sim$. The set

$$S^{-1}R = \left\{ \frac{a}{s} \;\middle|\; a \in R, s \in S \right\}$$

is the *localization* of R at S.

Remark 5.1.6.1. Note that the localization is again a ring with the usual operations on fractions.

Remark 5.1.6.2. There is a homomorphism $\varphi\colon R \to S^{-1}R$, given by $r \mapsto \frac{r}{1}$. If S has no zero divisors, the homomorphism is injective.

Remark 5.1.6.3. If $0 \in S$, then $S^{-1}R = (0)$. If R is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is the quotient field of R.

Proposition 5.1.7 (Universal property)**.** Suppose that $S \subseteq R$ is multiplicative and that $\psi\colon R \to T$ is a ring homomorphism. If $\psi(s)$ is invertible for all $s \in S$ then there exists a unique homomorphism $\widetilde{\psi}\colon S^{-1}R \to T$ such that $\psi = \widehat{\psi} \circ \varphi$.

Proposition 5.1.8. Let $S \subseteq R$ be a multiplicative subset and $\varphi\colon R \to S^{-1}R$ be given by $\varphi(r) = \frac{r}{1}$. Then there exists a bijective correspondence between prime ideals of $S^{-1}R$ and prime ideals P of R such that $P \cap S = \emptyset$, given by $Q \mapsto \varphi^{-1}(Q)$ and $P \mapsto S^{-1}P$.

[12] The ring R is a *valuation ring* in D.

Corollary 5.1.8.1. Let $P \triangleleft R$ be a prime ideal. Then there exists a bijection between prime ideals of $R_P = (R \setminus P)^{-1}P$ and prime ideals $Q \triangleleft R$ with $Q \subseteq P$. In particular, R_P has a unique maximal ideal.

5.2 Indecomposable modules

Definition 5.2.1. A left R-module M is *indecomposable* if it is not of the form $M = A \oplus B$ for some non-trivial submodules A and B.

Lemma 5.2.2. A module M is indecomposable if and only if $E = \mathrm{End}(M)$ has no non-trivial idempotents.

Proof. If $e \in E$ is a non-trivial idempotent, then we can write $M = eM \oplus (1-e)M$. If M is decomposable, that is $M = A \oplus B$ for non-trivial A and B, then the projections are non-trivial idempotents. □

Definition 5.2.3. A left R-module M is *strongly indecomposable* if $\mathrm{End}(M)$ is a local ring.

Definition 5.2.4. A left R-module M has *finite length* if all of its chains of submodules $(0) = N_0 < N_1 < \cdots < N_s = M$ have bounded length. The largest such length s is called the *length* of M.

Remark 5.2.4.1. If M has finite length, then it is artinian and noetherian. Equivalently, M has a composition series chain $(0) = N_0 < N_1 < \cdots < N_s = M$ where each composition factor $N_i \big/ N_{i-1}$ is simple. These composition factors are unique.

Theorem 5.2.5 (Fitting lemma)**.** Let M be a left R-module with finite length and $f \in \mathrm{End}(M)$. Then for all large enough n we have $M = \ker f^n \oplus \operatorname{im} f^n$.

Proof. Consider the chains

$$M \supseteq \operatorname{im} f \supseteq \operatorname{im} f^2 \supseteq \ldots \quad \text{and} \quad (0) \subseteq \ker f \subseteq \ker f^2 \subseteq \ldots$$

As M is both noetherian and artinian, both chains stabilize at some index r. We now claim that $M = \ker f^r \oplus \operatorname{im} f^r$.

Suppose first that $a \in \ker f^r \cap \operatorname{im} f^r$. Write $a = f^r(b)$ and note that $0 = f^r(a) = f^{2r}(b)$, therefore $b \in \ker f^{2r} = \ker f^r$ and $a = 0$.

Now take $c \in M$ and write $f^r(c) = f^{2r}(d)$. As $c = (c - f^r(d)) + f^r(d) \in \ker f^r + \operatorname{im} f^r$, we must have $M = \ker f^r + \operatorname{im} f^r$. □

Theorem 5.2.6. Suppose that M is an indecomposable left R-module of finite length. Then $E = \mathrm{End}(M)$ is a local ring and $\operatorname{rad} E$ is nil. In particular, M is strongly indecomposable.

Proof. We claim that all endomorphisms $f \in E \setminus E^{-1}$ are nil. Indeed, let $M = \ker f^r \oplus \operatorname{im} f^r$. By indecomposability of M, we must have either $\ker f^r = (0)$ or $\operatorname{im} f^r = (0)$. If $\ker f^r = (0)$, we find that f is bijective, therefore invertible, which is a contradiction. It follows that $f^r = 0$. □

Corollary 5.2.6.1. A right artinian ring is local if and only if it has no non-trivial idempotents.

Proof. It is well known that a $M = R$ as a right R-module has finite length. Hence $E = \mathrm{End}(M) = R$ has no non-trivial idempotents and M is indecomposable. By the previous theorem, M is strongly indecomposable and R is local. □

Proposition 5.2.7. Suppose that a left R-module M is noetherian or artinian. Then it can be written as a finite direct sum of indecomposable submodules.

Proof. Assume the opposite. In particular, we can write it as $M = M_{1,1} \oplus M_{1,2}$ where $M_{1,1}$ cannot be decomposed into a finite direct sum of indecomposable submodules. We can repeat this process on $M_{n,1}$ indefinitely. But then the sums of modules $M_{i,2}$ and the chain of modules $M_{n,1}$ form infinite increasing and decreasing chains respectively, contradicting our assumption. □

Definition 5.2.8. We call such a decomposition a *Krull-Schmidt decomposition*.

Theorem 5.2.9 (Krull-Schmidt)**.** Suppose that M is a left R-module of finite length. If

$$M = \bigoplus_{i=1}^{r} M_r = \bigoplus_{i=1}^{s} N_i$$

for indecomposable submodules M_i and N_i, then $r = s$ and there exists a permutation $\sigma \in S_r$ such that $M_i = N_{\sigma(i)}$ for all i.

Proof. Let $\alpha_i \colon M \to M_i$ and $\beta_i \colon M \to N_i$ be projections. Then

$$\sum_{i=1}^{r} \alpha_i = 1 = \sum_{i=1}^{s} \beta_i.$$

But then

$$\sum_{i=1}^{s} \alpha_1 \beta_i|_{M_1} = \alpha_1|_{M_1} = \mathrm{id}_{M_1}.$$

Since M_1 is indecomposable and of finite length, $\mathrm{End}(M_1)$ is a local ring. Hence we can assume that $\alpha_1\beta_1|_{M_1}$ is invertible. In particular, $\beta_1|_{M_1}$ is injective. The short exact sequence

$$0 \longrightarrow M_1 \xrightarrow{\beta_1} N_1 \longrightarrow N_1/M_1 \longrightarrow 0$$

thus splits, therefore $N_1 = M_1 \oplus N_1/M_1$, which is only possible if $M_1 \cong N_1$.

We now claim that

$$M \cong M_1 \oplus \bigoplus_{i=2}^{s} N_i.$$

Indeed, as $\beta_1|_{M_1}$ is an isomorphism, the sum is direct. It remains to check that N_1 is a subset of the above direct sum. Let $a \in N_1$ and write $a = \beta_1(b)$. Note that

$$a - b \in \ker \beta_1 = \bigoplus_{i=2}^{s} N_i,$$

therefore $a = b + (a - b)$ is the required decomposition.

As we have

$$\bigoplus_{i=2}^{r} M_i = M \big/ M_1 = \bigoplus_{i=2}^{s} N_i,$$

the theorem is proven by induction. □

Remark 5.2.9.1. The theorem does not hold in general. There are counterexamples that are artinian/noetherian.

Proposition 5.2.10. If a ring R has only finitely many maximal left ideals, it is semilocal.

Proof. Without loss of generality let $\operatorname{rad} R = (0)$ and let $M_1, \ldots, M_r$ be all the maximal left ideals. Now consider the R-module map

$$\Phi \colon R \to \bigoplus_{i=1}^{r} R\big/M_i \ ,$$

given by $\Phi_i(x) = x + M_i$. As $\operatorname{rad} R = (0)$, Φ is injective. As all R/M_i are simple by maximality, R is a submodule of a semisimple module and hence itself semisimple. □

Remark 5.2.10.1. If R is commutative, the converse also holds.

5.3 Idempotents

Definition 5.3.1. A ring R is *indecomposable* if it cannot be written as a direct product of non-trivial rings.

Definition 5.3.2. An idempotent $e \in R$ is *central* if $e \in Z(R)$.

Proposition 5.3.3. A ring R is indecomposable if and only if it does not have non-trivial central idempotents.

Proof. If $e \in R$ is a non-trivial central idempotent, then $R = Re \oplus R(1-e)$ is a decomposition, hence R is not indecomposable. If R is decomposable, then projections of 1 are non-trivial idempotents. □

Lemma 5.3.4. Let $e \in R$ be an idempotent and $f = 1 - e$. Then e is central if and only if $eRf = fRe = (0)$.

Proof. Both statements are equivalent to $er = ere = re$. □

Definition 5.3.5 (Pierce decomposition)**.** Let R be a ring and $e \in R$ an idempotent. For $f = 1 - e$, we can write $R = Re \oplus Rf$ as a left R-module, $R = eR \oplus fR$ as a right R-module and

$$R = eRe \oplus eRf \oplus fRe \oplus fRf$$

as an abelian group.

Proposition 5.3.6. Suppose that $e, e' \in R$ are idempotents and let M be a right R-module.

i) There exists an isomorphism of abelian groups $\lambda\colon \operatorname{Hom}(eR, M) \to Me$.

ii) The abelian groups $\operatorname{Hom}(eR, e'R)$ and $e'Re$ are isomorphic.

Proof. The second item clearly follows from the first. Let $\theta\colon eR \to M$ be a homomorphism of right R-modules and set $m = \theta(e)$. Then clearly $me = \theta(e^2) = m$, hence $m \in Me$. We can now define $\lambda(\theta) = \theta(e)$, where $\lambda\colon \operatorname{Hom}(eR, M) \to Me$, as required. Note that θ is uniquely determined by $\theta(e)$, therefore λ is injective. To prove surjectivity, take $m \in Me$ and set $\theta(er) = mr$. It is well defined, as $er = 0$ implies $mr \in Mer = (0)$. □

Corollary 5.3.6.1. For each idempotent $e \in R$ there is a canonical isomorphism of rings $\operatorname{End}(eR) \cong eRe$.

Proof. Applying the above proposition, $\lambda\colon \operatorname{End}(eR) \to Me$ is a group isomorphism. For $\theta, \theta' \in \operatorname{End}(eR)$, we have

$$\lambda(\theta \cdot \theta') = \theta(\theta'(e)) = \theta(m).$$

But as $m \in eR$, we can further simplify the expression as

$$\theta(m) = \theta(em) = \theta(e) \cdot m = \lambda(\theta) \cdot \lambda(\theta'),$$

therefore λ is multiplicative as well. □

Definition 5.3.7. Idempotents $e, f \in R$ are *orthogonal* if $ef = fe = 0$.

Proposition 5.3.8. The following statements are equivalent for a non-zero idempotent $e \in R$:

i) The right R-module eR is indecomposable.

ii) The left R-module Re is indecomposable.

iii) The ring eRe has no non-trivial idempotents.

iv) The idempotent e does not decompose as $e = \alpha + \beta$ for non-zero orthogonal idempotents α and β.

Proof. We clearly only need to prove that the items i), iii) and iv) are equivalent. As eR is indecomposable precisely if $\mathrm{End}(eR) \cong eRe$ has no non-trivial idempotents, i) and iii) are indeed equivalent.

If $\alpha \in eRe$ is a non-trivial idempotent, then so is $\beta = e - \alpha$. Furthermore, they are clearly orthogonal, hence e is decomposable. Finally, if $e = \alpha + \beta$ for orthogonal idempotents α and β, then $e\alpha = \alpha = \alpha e \in eRe$ is a non-trivial idempotent. □

Corollary 5.3.8.1. For any non-zero idempotent $e \in R$ the following statements are equivalent:

i) The right R-module eR is strongly indecomposable.

ii) The left R-module Re is strongly indecomposable.

iii) The ring eRe is local.

Proof. The proof is obvious and need not be mentioned. □

Definition 5.3.9. An idempotent $e \in R$ is *local* if the ring eRe is local.

Theorem 5.3.10. Suppose that $e \in R$ is an idempotent and let $J = \mathrm{rad}(R)$.

i) The radical of eRe can be expressed as $\mathrm{rad}(eRe) = J \cap eRe = eJe$.

ii) For the quotient projection $\bar{}\colon R \to R/J$ we have $eRe/eJe \cong \bar{e}\bar{R}\bar{e}$.

Proof. We will show that $\mathrm{rad}(eRe) \subseteq J \cap eRe \subseteq eJe \subseteq \mathrm{rad}(eRe)$. Suppose first that $r \in \mathrm{rad}(R)$. We will show that $1 - yr$ has a left inverse in R for all $y \in R$. Indeed, we can write $b(e - eyer) = e$ for some $b \in eRe$. But as $b, r \in eRe$, this implies $b(1 - yr) = e$, hence $yrb(1 - yr) = yre = yr$. Adding $1 - yr$ to both sides, we find that $yrb + 1$ is the sought left inverse.

Now let $r \in J \cap eRe$. Then $ere = r$, but as $r \in J$, we find that $r = ere \in eJe$.

Finally, let $r \in eJe$. We will show that $e - yr$ has a left inverse in eRe for all $y \in eRe$. Indeed, as $r \in J$, we can write $x(1 - yr) = 1$ for some $x \in R$. But then

$$e = ex(1 - yr)e = ex(e - yr) = exe(e - yr),$$

therefore exe is the left inverse.

For the second part just apply the isomorphism theorem for $\bar{}\colon eRe \to \bar{e}\bar{R}\bar{e}$. □

Theorem 5.3.11. Let $e \in R$ be an idempotent.

i) If $I \subseteq eRe$ is a left ideal, then $RI \cap eRe = I$. In particular, the map $I \mapsto RI \lhd R$ for $I \lhd eRe$ is injective.

ii) For $I \lhd eRe$, we have $e(RIR)e = I$. In particular, the map $I \mapsto RIR \lhd R$ for $I \lhd eRe$ is injective.

iii) If e satisfies $ReR = R$,[13] then the map in ii) is surjective.

Proof.

i) It is clear that $I \subseteq RI \cap eRe = I_0$. But as $I_0 = eI_0 \subseteq eRI = eReI = I$, we must have $I = I_0$.

ii) We can write $eRIRe = (eRe)I(eRe) = I$.

iii) Let $J \lhd R$ and set $I = eJe \lhd eRe$. Then

$$RIR = ReJeR = Re(RJR)eR = RJR = J. \qquad \square$$

Corollary 5.3.11.1. Let $e \in R$ be a non-zero idempotent. If R is J-semisimple, semisimple, simple, or left/right noetherian/artinian, then so is eRe.

Theorem 5.3.12. Suppose that $I \lhd R$ is nil. If $a \in R$ is such that $\overline{a} = a + {}^{R}/_{I}$ is an idempotent, then there exists some idempotent $e \in R$ such that $\overline{e} = \overline{a}$.

Proof. Set $b = 1 - a$. Then clearly $ab = ba = a - a^2 \in I$. As I is nil, we can find an integer m such that $(ab)^m = 0$. Now write

$$1 = (a+b)^{2m-1} = \underbrace{\sum_{i=0}^{m-1} \binom{2m-1}{i} a^{2m-1-i} b^i}_{e} + \underbrace{\sum_{i=m}^{2m-1} \binom{2m-1}{i} a^{2m-1-i} b^i}_{f}.$$

Then clearly $ef = 0$ and $e = e^2 + ef = e^2$ is an idempotent. As $e \equiv a^{2m} \equiv a \pmod{I}$, we indeed have $\overline{e} = \overline{a}$. $\square$

[13] Such idempotents are called *full*.

5.4 Block decomposition and central idempotents

Definition 5.4.1. An idempotent $c \in R$ is *centrally primitive* if $c \in Z(R)$ and it cannot be written as a sum of two non-zero orthogonal central idempotents.

Proposition 5.4.2. Suppose that $1 \in R$ decomposes as

$$1 = \sum_{i=1}^{r} c_i,$$

where c_i are orthogonal centrally primitive idempotents.

i) Every central idempotent is of the form

$$c = \sum_{i \in I} c_i.$$

ii) The idempotents c_i are the only centrally primitive idempotents.

iii) The decomposition is unique.

Proof. Suppose that $c \in R$ is a central idempotent. As c_i is primitive and cc_i is an idempotent, we must have either $cc_i = 0$ or $cc_i = c_i$. But then

$$c = \sum_{cc_i = c_i} c_i.$$

The second statement is a direct corollary of the first. The uniqueness of the decomposition follows from the fact that

$$0 = \sum_{i \in I} c_i$$

implies that $c_i = c_i^2 = 0$ for all $i \in I$, as c_j are orthogonal. □

Definition 5.4.3. If the above decomposition exists, then

$$R = \prod_{i=1}^{m} c_i R$$

is a *block decomposition*.

Theorem 5.4.4. If R is left noetherian/artinian, then a block decomposition exists.

6 Free algebras and polynomial identities

"Can I talk to my lawyer?"
– prof. dr. Igor Klep

6.1 Basic definitions

Definition 6.1.1. Let $X = \{x_i \mid i \in I\}$ be a non-empty set. A *word* is a finite sequence of elements of X. The set $\langle X \rangle$ of all words, with concatenation, is called the *free monoid* on X.

Definition 6.1.2. Let F be a field and $X \neq \emptyset$. The *free algebra* on X over F is the monoid algebra of $\langle X \rangle$ over F. We denote it by $F\langle X \rangle$.

Theorem 6.1.3 (Universal property)**.** Let A be an F-algebra. All homomorphisms $F\langle X \rangle \to A$ are uniquely determined by the image of X. Conversely, any function $f\colon X \to A$ extends uniquely to a homomorphism $F\langle X \rangle \to A$.

Proof. The proof is obvious and need not be mentioned. □

Definition 6.1.4. A polynomial f is *multilinear* if it is linear in each variable.

Proposition 6.1.5. Let A be an F-algebra and $X \subseteq A$ any generating set. Then A is a quotient of the algebra $F\langle X \rangle$.

Proof. By the universal property, $\iota\colon X \hookrightarrow A$ extends to a homomorphism $g\colon F\langle X \rangle \to A$. It is obviously surjective, therefore $A \cong F\langle X \rangle \big/ \ker g$. □

Definition 6.1.6. Given $S = \{f_j \mid j \in J\} \subseteq F\langle X \rangle$, we denote

$$F\langle x_i, i \in I \mid f_j = 0, j \in J \rangle = F\langle X \rangle \big/ (S).$$

Definition 6.1.7. The *Grassman algebra* is defined as

$$G = F\left\langle x_i, i \in \mathbb{N} \;\middle|\; x_i^2, x_i x_j + x_j x_i \right\rangle.$$

Proposition 6.1.8. The Grassman algebra is spanned by sorted words. Its center is spanned by words of even length.

Proof. It suffices to show that a linear combination of sorted words is non-zero. In fact, it is enough to show that sorted words are non-zero, as we can eliminate words in the combination by multiplying them by a variable that appears only in some of them.

Suppose therefore that $y_1 \cdots y_n \in I$, where $I = \langle y_i^2, y_i y_j + y_i y_j \rangle$. We can therefore write $y_1 \cdots y_n$ as a sum of elements of the form $m y_i^2 m'$ and $q(y_i y_j + y_j y_i) q'$ for monomials m, m', q and q'. But as $y_1 \cdots y_n$ is multilinear, it follows that we can write it as a sum of elements

$$\prod_{i=0}^{k-1} y_{\sigma(i)} \cdot \left(y_{\sigma(k)} y_{\sigma(k+1)} + y_{\sigma(k+1)} y_{\sigma(k)} \right) \cdot \prod_{i=k+2}^{n} y_{\sigma(i)}.$$

In such a representation, the sum of coefficients of monomials corresponding to even permutations is equal to that of monomials which correspond to odd permutations. We reached a contradiction. □

Remark 6.1.8.1. We denote by G_0 the span of words of even length and by G_1 the span of words of odd length. Then $G = G_0 \oplus G_1$.

Definition 6.1.9. A multilinear polynomial $f = f(x_1, \ldots, x_m, y_1, \ldots, y_n) \in F\langle X, Y\rangle$ is *alternating* in $x_1, \ldots, x_m$ if f becomes 0 whenever we replace a variable x_i by x_j for $j > i$.

Proposition 6.1.10. Let A be an F-algebra and assume that $a_1, \ldots, a_m \in A$ are linearly dependent. If $f = f(x_1, \ldots, x_m, y_1, \ldots, y_n)$ is an alternating polynomial, then $f(a_1, \ldots, a_m, b_1, \ldots, b_n) = 0$ for all $b_i \in A$.

Proof. The proof is obvious and need not be mentioned. □

6.2 Polynomial identities

Definition 6.2.1. A polynomial $f \in F\langle X \rangle$ is a *polynomial identity* of an F-algebra A if $f(a_1, \ldots, a_n) = 0$ for all $a_i \in A$. An F-algebra A is a *PI-algebra* if there exists a non-trivial $f \in F\langle x \rangle$ such that A satisfies f.

Remark 6.2.1.1. Every finite-dimensional algebra is a PI-algebra, as it satisfies any alternating polynomial in $\dim A + 1$ variables. In particular, we can take the *standard polynomial*

$$s_n = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(i)}$$

for $n = \dim A + 1$.

Remark 6.2.1.2. Subalgebras and quotients of PI-algebras are again PI-algebras, as they satisfy the same polynomial. Finite products of PI-algebras are also PI-algebras.

Theorem 6.2.2 (Regev)**.** A tensor product of two PI-algebras is again a PI-algebra.

6.3 Linearization

Theorem 6.3.1. If A satisfies a non-zero polynomial identity, then it satisfies a non-zero multilinear identity of equal or lower degree.

Proof. Let f be the polynomial identity for A. Set $d_i = \deg_{x_i} f$ and $d = \max d_i$. Now induct on d.

For $d = 1$, take a monomial $\lambda x_1 \dots x_m$ of minimal degree in f. Then $f(x_1, \dots, x_m, 0, \dots, 0)$ is a multilinear identity for A.

Now suppose that $d > 1$. Without loss of generality let $d_i \leq d_{i+1}$ for all i and let k be the minimal index with $d_k = d$. Now define g as

$$g(x_1, \dots, x_{n+1}) = f(x_1, \dots, x_{n-1}, x_n + x_{n+1}) - f(x_1, \dots, x_n) - f(x_1, \dots, x_{n-1}, x_{n+1}).$$

Note that all monomials in f correspond with distinct monomials in g. In particular, $g \neq 0$. As $\deg_{x_n} g < d$ and $\deg_{x_{n+1}} g < d$, while $\deg_{x_i} g \leq d_i$, we can iterate this process until we decrease the degree of all variables. □

6.4 Cayley-Hamilton theorem

Definition 6.4.1. Let C be a commutative algebra. For $A \in M_n(C)$, define its *characteristic polynomial* as $p_A(t) = \det(A - tI) \in C[t]$.

Theorem 6.4.2 (Cayley-Hamilton)**.** For all $A \in M_n(C)$, we have $p_A(A) = 0$.

Definition 6.4.3. *Elementary symmetric polynomials* are defined as

$$e_k = \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I|=k}} \prod_{i \in I} w_i \in \mathbb{Z}[w_1, \dots, w_n].$$

Definition 6.4.4. *Power sums* are defined as

$$p_j = \sum_{i=1}^{n} w_i^j \in \mathbb{Z}[w_1, \dots, w_n].$$

Theorem 6.4.5 (Newton formulas)**.** For $k \leq 1$, we have

$$ke_k = \sum_{j=1}^{k} (-1)^{j-1} e_{k-j} p_j.$$

Proof. Vieta's formulas give us

$$\sum_{j=0}^{n} (-1)^j e_{n-j} w_i^j = 0,$$

therefore

$$\sum_{j=0}^{n} (-1)^j e_{n-j} p_j = 0.$$

This is in fact the formula for $k = n$. Now set

$$P_n = ke_k - \sum_{j=1}^{k} (-1)^{j-1} e_{k-j}.$$

By the above observation, we have $P_k = 0$. This implies $P_n(w_1, \dots, w_k, 0, \dots, 0) = 0$. This means that P contains no monomials in k variables, but as $\deg P_n \leq k$, this means that $P_n \equiv 0$. □

Remark 6.4.5.1. In characteristic 0, we can write $e_k = q_k(p_1, \dots, p_k)$.

Theorem 6.4.6. If C is a commutative $\mathbb{Q}$-algebra, then all $A \in M_n(C)$ satisfy

$$p_A(t) = \sum_{j=0}^{n} (-1)^j q_{n-j} \left(\operatorname{tr}(A), \operatorname{tr}(A^2), \dots, \operatorname{tr}(A^{n-j}) \right) t^j.$$

Proof. It suffices to prove the theorem for $A = (w_{i,j})_{i,j}$ and $C = \mathbb{Q}[w_{i,j}]$. We can embed C into the algebraic closure of its quotient field. We can hence assume that C is an algebraically closed field of characteristic 0. Then

$$p_A(t) = (-1)^n \prod_{i=1}^{n} (t - \lambda_i),$$

where λ_i are the eigenvalues of A, counted with multiplicities. Using the Jordan canonical form, we find that $\operatorname{tr}(A^i) = p_i(\lambda_1, \ldots, \lambda_n)$. But then, by Vieta,

$$p_A(t) = \sum_{j=0}^{n} (-1)^j e_{n-j}(\lambda_1, \ldots, \lambda_n) t^j = \sum_{j=0}^{n} (-1)^j q_{n-j} \left(\operatorname{tr}(A), \operatorname{tr}(A^2), \ldots, \operatorname{tr}(A^{n-j}) \right) t^j. \quad \square$$

Corollary 6.4.6.1. Let C be a commutative $\mathbb{Q}$-algebra. If a matrix $A \in M_n(C)$ satisfies $\operatorname{tr}(A) = \operatorname{tr}(A^2) = \cdots = \operatorname{tr}(A^n) = 0$, then $A^n = 0$.

Proof. The theorem implies that $p_A(t) = (-1)^n t^n$. Now just apply Cayley-Hamilton. $\square$

6.5 Amitsur-Levitzki theorem

Lemma 6.5.1. A non-zero polynomial f with $\deg f < 2n$ is not a polynomial identity of $M_n(F)$.

Proof. Without loss of generality let f be multilinear of degree $2n-1$. Suppose that the monomial $\lambda x_1 x_2 \dots x_{2n-1}$ appears in f. Plugging the sequence $E_{1,1}, E_{1,2}, E_{2,2}, \dots, E_{n,n}$ into the polynomial, we find that only this monomial evaluates to a non-zero element. It follows that f is not a polynomial identity. □

Theorem 6.5.2 (Amitsur-Levitzki)**.** The standard polynomial s_{2n} is a polynomial identity of $M_n(C)$ for every commutative algebra C.

Proof. Note that it suffices to prove the theorem for $C = F$, where F is a field of characteristic 0. Let $A_i \in M_n(F)$. We will show that $s_{2n}(A_1, \dots, A_{2n}) = 0$. Let $G = G_0 \oplus G_1$ be the Grassman algebra over F with generators $x_1, x_2, \dots$ and set

$$A = \sum_{i=1}^{2n} A_i x_i.$$

As $x_i G x_i = 0$, we find that

$$A^{2n} = \sum_{\sigma \in S_{2n}} \prod_{i=1}^{2n} A_{\sigma(i)} x_{\sigma(i)} = \sum_{\sigma \in S_{2n}} \operatorname{sgn}(\sigma) \prod_{i=1}^{2n} A_{\sigma(i)} \cdot \prod_{i=1}^{n} x_i = s_{2n}(A_1, \dots, A_{2n}) \cdot \prod_{i=1}^{n} x_i.$$

It suffices to show that $A^{2n} = (A^2)^n = 0$. But as $A^2 \in M_n(G_0)$ and G_0 is commutative, it is enough to show that $\operatorname{tr}(A^2) = \operatorname{tr}(A^4) = \dots = \operatorname{tr}(A^{2n})$.

Let

$$A^{2k-1} = \sum_j B_j y_j,$$

where $B_j \in M_n(F)$ and $y_j \in G_1$. Then

$$\sum_{i,j} \operatorname{tr}(A_i B_j) x_i y_j = \operatorname{tr}\left(\sum_{i,j} A_i x_i B_j y_j\right) = \operatorname{tr}(A^{2k}) = \operatorname{tr}\left(\sum_{i,j} B_j y_j A_i x_i\right) = \sum_{i,j} \operatorname{tr}(B_j A_i) y_j x_i.$$

As $x_i y_j = -y_j x_i$ and $\operatorname{tr}(B_j A_i) = \operatorname{tr}(A_i B_j)$, we find that $\operatorname{tr}(A^{2k}) = 0$. □

Index