NONCOMMUTATIVE ALGEBRA - NOTES

Gal Anton Gorše

Examples

Definition 0.1. $(R, +, \cdots)$ is a ring if:
1. $(R, +)$ is an abelian group;
2. $(R, \cdot)$ is a semigroup with unity (a monoid);
3. we have
$$x \cdot (y + z) = xy + xz, \quad (x + y) \cdot z = xz + yz$$
for all $x, y, z \in R$.

Aditionally, R is a commutative ring if $xy = yx$ for all $x, y \in R$.

Definition 0.2. Let R be a ring. Then $(M, +) \in \mathrm{Ab}$ is a left R-module if there exists a map
$$R \times M \to M, \quad (r, m) \mapsto r \cdot m$$
such that
1. $r \cdot (x + y) = rx + ry$;
2. $(r + s) \cdot x = rx + sx$;
3. $(rs) \cdot x = x \cdot (s \cdot x)$;
4. $1 \cdot x = x$.

A right module is defined in an analogous way.

Definition 0.3. If A, R are rings then we say that $(A, +, \cdot)$ is an R-algebra if
1. A is an R-module;
2. $r \cdot (xy) = (rx) \cdot y = x(r \cdot x)$ for every $r \in R$ and $x, y \in A$.

Example 0.4. *$\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[x]$ and $\mathbb{R}[x]$ are all rings. In particular, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.*

Example 0.5. *Let R be a ring and $n \in \mathbb{N}$. Then $M_n(R)$ is a ring. If $n \geq 2$, then $M_n(R)$ is not commutative.*

Example 0.6. *Let $\mathbb{H}$ be a ring of quaternions. We know that $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}_i \oplus \mathbb{R}_j \oplus R_k$ is a $\mathbb{R}$-vector space with the basis $\{1, i, j, k\}$ with identities*
$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k.$$
This is not a commutative ring. It's important to note that every nonzero $\alpha \in \mathbb{H}$ has an inverse $\alpha^{-1} = \frac{1}{\alpha \cdot \overline{\alpha}} \overline{\alpha}$. We say that $\mathbb{H}$ is a division ring or a skew field (and is in fact the smallest possible one over $\mathbb{R}$). Now let $R = \{a + bi + ci + di \mid a, b, c, d \in \mathbb{Z}\}$ be a subring of $\mathbb{H}$. The set of all units

of R is

$$U(R) = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Example 0.7. *We construct free algebras. Let $\mathbb{F}$ be a field and $X = \{x_i \mid i \in I\}$ freely noncommuting variables. We define $\langle X \rangle$ as a free monoid on X or a set of all words in X. Then $\mathbb{F}\langle X \rangle$ is defined as a set of all $\mathbb{F}$-linear combinations of words in X. This is a free $\mathbb{F}$-algebra on X. Suppose we have $|I| = 1$. Then $X = \{x\}$ and $\mathbb{F}\langle x \rangle = F[x]$. If A is an $\mathbb{F}$-algebra then $\forall f : X \to A$ there exists exactly one $\overline{f} : \mathbb{F}\langle X \rangle \to \mathbb{R}$ such that the following diagram commutes:*

$$\begin{array}{ccc} X & \xrightarrow{f} & A \\ \downarrow & \nearrow_{\exists! \overline{f}} & \\ K\langle X \rangle & & \end{array}$$

The free algebra $\mathbb{F}\langle x, y \rangle$ on two generators actually contains the free algebra on countably infinitely many generators. Indeed, we have the following F-algebra monomorphism:

$$\begin{aligned} \Phi : \mathbb{F}\langle y_i \mid i \in \mathbb{N} \rangle &\to \mathbb{F}\langle x, y \rangle \\ y_1 &\to x \\ y_2 &\to xy \\ y_3 &\to xy^2 \\ &\vdots \end{aligned}$$

Example 0.8. *We can now describe algebras with its generators and relations. Let k be a ring and $R = k\langle x_i \mid i \in I \rangle$. Denote $F = \{f_j \mid j \in J\} \subseteq R$. Then $(F) \lhd R$, so $R/(F)$ is a algebra generated by $\overline{x_i} = x_i + (F)$ such that $f_j(\overline{x_i})$ for each $f_j \in F$. For example, take $F = \{x_i x_j - x_j x_i \mid i, j \in I\}$. Then*

$$\overline{R} = R/(F) = k[\overline{x_i} \mid i \in I].$$

In $\overline{R}$, we have $\overline{x_i}\overline{x_j} - \overline{x_j}\overline{x_i} = 0$. Now let $R = k\langle x, y \rangle$ and $F = \{xy - yx - 1\}$. Then

$$\overline{R} = R/(F) =: \mathcal{A}_1(k)$$

is called the first Weyl algebra. Generators $\overline{x}, \overline{y}$ of $\mathcal{A}_1(k)$ satisfy $\overline{xy} - \overline{yx} = 1$. As a set, this algebra is

$$\mathcal{A}_1(k) = \left\{ \sum_j^b a_{ij} \overline{x}^i \overline{y}^j \mid a_j \in k \right\}.$$

The multiplication looks like

$$\overline{xyx} = \overline{x}(\overline{yx}) = \overline{x}(\overline{xy} - 1) = \overline{x}^2\overline{y} - \overline{x}.$$

The algebra $\mathcal{A}_1(k)$ is the algebra of differential operators on $K[y]$. Indeed, define the operators

$$D : k[y] \to k[y], \quad p \mapsto \frac{d}{dy}p$$

and

$$L : k[y] \to k[y], \quad p \mapsto y \cdot p.$$

We then have

$$\begin{aligned} (DL - LD)(p) &= D(Lp) - L(Dp) \\ &= p + y\frac{d}{dy}p - y\frac{d}{dy}p \\ &= (\mathrm{Id})p, \end{aligned}$$

so $DL - LD = 1$. We can now define a monomorphism of k-algebras

$$\begin{aligned}\Phi : \mathcal{A}_1(k) &\to \mathrm{End}_k(k[y]) \\ \overline{x} &\to D \\ \overline{y} &\to L.\end{aligned}$$

Example 0.9. *Let k be a field and G a group. Then we define a group k-algebra kG as a k-vector space with basis G with the multiplication*

$$\left(\sum_{\sigma\in G} a_\sigma \sigma\right) \cdot (\sum_{\tau\in G} b_\tau \tau) = \sum_{\eta\in G} c_\eta \eta,$$

where

$$c_\eta = \sum_{\sigma\tau=\eta} a_\sigma b_\tau.$$

Example 0.10. *Let $X = \{x_i \mid i \in I\}$ be variables. Then we define the power series ring*

$$k\langle\langle x_i \mid i \in I\rangle\rangle = \{f_0 + f_1 + f_2 + \dots \mid f_j \in k\langle x_i \mid i \in I\rangle \text{ homogenous of degree } j\}.$$

The set of units of this ring is

$$U(k\langle\langle X\rangle\rangle) = \{f \in k\langle\langle X\rangle\rangle \mid f_0 \in U(k)\}.$$

Example 0.11. *Let R be a ring and $\sigma \in \mathrm{End}(R)$. Then we define the ring of skew polynomials*

$$R[x;\sigma] = \{\sum_{i=0}^{n} b_i x^i \mid b_i \in R, n \in \mathbb{N}\}$$

with the relation $x \cdot b := \sigma(b) \cdot x$. Thus we have the multiplication rule

$$\left(\sum a_i x^i\right)\left(\sum b_j x^j\right) = \sum a_i \sigma^i(b_j) x^{i+j}.$$

If σ is not set injective, say $\sigma(b) = 0$ for some $0 \neq b \in R$, then $x \cdot b = \sigma(b)x = 0$. In this case, x is a zero divisor. If R is a domain (a ring without zero divisors) and σ is injective, then $R[x,\sigma]$ is also a domain.

Example 0.12. *We define the ring of differential polynomials*

$$R[x;\delta] = \{\sum_{i=0}^{n} b_i x^i \mid b_i \in R, n \in \mathbb{N}\}$$

with multiplication $x \cdot a = a \cdot x + \delta(a)$, where $\delta : R \to R$ is a derivation. This means that δ satisfies

$$\delta(a+b) = \delta(a) + \delta(b), \quad \delta(ab) = a\delta(b) + b\delta(a)$$

for every pair $a, b \in R$. We take a look at two special cases. If there exists $c \in R$ such that $\delta(a) = ca - ac$ for all $a \in R$, we say that δ is an inner derivation. In that case, $R[x;\delta] = R[x-c] \cong R[x]$. Now suppose $R = K[y]$ and δ is a derivative with respect to y. Then $R[x;\delta] = \mathcal{A}_1(K)$.

Example 0.13. *If R is a ring, then $R^{\mathrm{op}} = \{r^{\mathrm{op}} \mid r \in R\}$ is a ring with the operations*

$$r^{\mathrm{op}} + s^{\mathrm{op}} := (r+s)^{\mathrm{op}}, \quad r^{\mathrm{op}} \cdot s^{\mathrm{op}} = (s \cdot r)^{\mathrm{op}}.$$

1 Finite-dimensional algebras and Wedderburn's structure theory

1.1 Chain conditions

Let C be a set and $\{C_i \mid i \in I\}$ a set of some of its subsets. We say that this family satisfies the ascending chain condition (ACC) if there does not exist an infinite strictly increasing chain

$$C_{i_1} \subsetneq C_{i_2} \subsetneq \cdots$$

for $i_j \in I$. Equivalently:

1. If we have a chain
$$C_{i_1} \subseteq C_{i_2} \subseteq \cdots,$$
then there exists a $k \in \mathbb{N}$ such that $C_{i_k} = C_{i_{k+1}} = \cdots$
2. Every subset of $\{C_i \mid i \in I\}$ admits a maximal element w.r.t. inclusion.

Similarly, we define the decreasing chain condition (DCC).

Definition 1.1. Let R be a ring and M a left R-module.
- M is noetherian if the set of all its submodules satisfies ACC.
- M is artinian if the set of all its submodules satisfies DCC.

Proposition 1.2. *1. M is noetherian iff every submodule of M is finitely generated.*

2. Let $N \leq M$. Then M is noetherian iff N and M/N are noetherian.

Remark. The second statement holds true for artinian modules as well.

Proof. 1. Start with the left implication ($\Leftarrow$). Suppose that

$$M_1 \leq M_2 \leq \cdots \leq M.$$

Define $N = \bigcup_{j \in \mathbb{N}} M_j \leq M$. By assumption, N is finitely generated, say by $x_1, \ldots, x_n \in N$. For each $i \in \{1, \ldots, n\}$, there exists a $j_i \in \mathbb{N}$ such that $x_i \in M_{j_i}$. Let $m = \max\{j_1, \ldots, j_n\}$. Then $\forall i \in \{1, \ldots, n\}$ we have $x_i \in M_{j_i} \leq M_m$, which implies $N = M_m$. From there it follows $N = M_m = M_{m+1} = \cdots$ Now for the converse ($\Rightarrow$). Let $N \leq M$ and define $\mathcal{C}$ as a set of all finitely-generated submodules of N. Since M is noetherian, $\mathcal{C}$ has a max element, say $N_0 \in \mathcal{C}$. Then $N_0 \leq N$. If $N_0 \subsetneq N$, then $b \in N \setminus N_0$. But that would imply that $N_0 + Rb \in \mathcal{C}$ and $N_0 \subsetneq N_0 + Rb$, contradicting our assumption of maximality.

2. ($\Rightarrow$) We know that
$$0 \to N \xrightarrow{f} M \xrightarrow{g} M/N \to 0$$
is a short exact sequence. It's obvious that N is noetherian, so we need to prove the same for M/N. Suppose that
$$\widetilde{N_1} \leq \widetilde{N_2} \leq \cdots \leq M/N.$$
Then
$$g^{-1}(\widetilde{N_1}) \leq g^{-1}(\widetilde{N_2}) \leq \cdots \leq M.$$
Since M is noetherian, there exists a $k \in \mathbb{N}$ such that
$$g^{-1}(\widetilde{N_k}) = g^{-1}(\widetilde{N_{k+1}}) = \cdots$$

But since g is onto, we have

$$\widetilde{N_k} = \widetilde{N_{k+1}} = \cdots$$

Now the converse ($\Leftarrow$). Suppose

$$M_1 \leq M_2 \leq \cdots \leq M.$$

Set $\widetilde{M_i} := g(M_i) \leq M/N$ and $N_i := f^{-1}(M_i) \leq N$. We have

$$N_1 \leq N_2 \leq \cdots \leq N$$

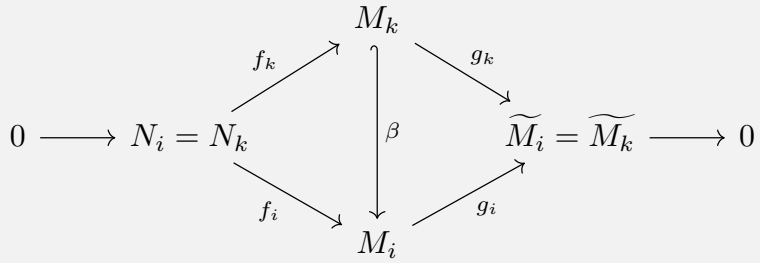
and

$$\widetilde{M_1} \leq \widetilde{M_2} \leq \cdots \leq M/N.$$

Because both of there modules are noetherian, there exists a $k \in \mathbb{N}$ such that $N_k = N_{k+1} = \cdots$ and $\widetilde{M_k} = \widetilde{M_{k+1}} = \cdots$ We now use the notation

$$0 \to N_i \xrightarrow{f_i} M_i \xrightarrow{g_i} \widetilde{M_i} \to 0.$$

Let $i \geq k$.



We just have to prove that β is onto M_i. Let $b \in M_i$ and $g_i(b) = g_k(b')$ for some $b' \in M_k$. Then we have

$$\begin{aligned} g_i(\beta(b') - b) &= (g_i \circ \beta)(b') - g_i(b) \\ &= g_k(b') - g_i(b) \\ &= 0. \end{aligned}$$

Since $\beta(b') - b \in \ker g_i = \operatorname{im} f_i$, we have $\beta(b') - b = f_i(b'')$ for some $b'' \in N_i$. It follows that

$$\begin{aligned} \beta(b' - f_k(b'')) &= \beta(b') - (\beta \circ f_k)(b'') \\ &= \beta(b') - f_i(b'') \\ &= b \end{aligned}$$

and we are finished. □

Definition 1.3. A ring R is left noetherian (artinian) if R is noetherian (artinian) as a left R-module. The definition for right noetherian (artinian) is similar as above.

Remark. Ring R is left noetherian iff each left ideal is finitely generated.

Example 1.4.

- *If F is a field, then any finitely generated F-algebra is left and right noetherian.*
- *The ring of integers $\mathbb{Z}$ is noetherian (because it is a PID), but not artinian:*

$$\mathbb{Z} \supset \mathbb{Z}/2\mathbb{Z} \supset \mathbb{Z}/4\mathbb{Z} \supset \cdots$$

Definition 1.5. A ring R is called noetherian if it is left and right noetherian.

Proposition 1.6. *If R is a noetherian and M is a finitely generated R-module, then M is noetherian.*

Proof. If M is finitely generated. Then there exists a linear map $\phi : R^n \to M$ for some $n \in \mathbb{N}$. By the proof of previous proposition, it suffices to show R^n is noetherian. Observe the next short exact sequence:

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

We use the previous proposition and proceed by induction. □

1.2 Simple modules

Definition 1.7. Non-trivial left R-module M is called simple if it has no proper non-trivial submodules and cyclic (with generator $m \in M$) if $M = R \cdot m = \{r \cdot m \mid r \in R\}$.

Example 1.8. *Over fields F, simple F-modules are one-dimensional vector spaces.*

Proposition 1.9. *For a left R-module M the following statements are equivalent.*

1. *M is simple.*
2. *M is cyclic and every nonzero element is a generator.*
3. *$M \cong R/I$ for a maximal left ideal $I \lhd R$.*

Proof. Begin with (1) $\Rightarrow$ (2). Take any element $m \in M \setminus \{0\}$. Then $Rm \leq M$ is a non-trivial submodule, so we have $Rm = M$. Now the implication (2) $\Rightarrow$ (3). Define a homomorphism of R-modules

$$\Phi : R \to M = Rm, \quad r \mapsto r \cdot m.$$

Then we define $I = \ker \Phi = \operatorname{ann}(m)$. Clearly, I is a R-submodule of R and $Rm = M \cong R/I$. We only have to prove the maximality of I. We have a bijective correspondice between ideal $I \subseteq J \subseteq R$ and submodules of M. Since any element in a proper submodule of M cannot generate M, the only possible J are I, R. We finish off with (3) $\Rightarrow$ (1). If $(0) \subseteq M' \leq M = R/I$, M' corresponds to a left ideal J of of R containing I. Thus $J = R$ or $J = I$, hence $M' = M$ or $M = (0)$. □

Example 1.10.
1. *Simple $\mathbb{Z}$-modules are of the form $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number.*
2. *If F is a field, then simple $F[x]$-modules are of the form $F[x]/(p)$ for some irreducible polynomial $p \in F[x]$.*
3. *Let V be a n-dimensional vector space over F and $R = \operatorname{End}_R(V) \cong M_n(F)$. We already know that V is an R-module, but it is also simple.*

Lemma 1.11 (Schur's lemma)**.** *Let M, N be simple R-modules and $f : M \to N$ a homomorphism. Then f is either an isomorphism or a zero map. In particular, $\operatorname{End}_R(M)$ is a division ring.*

Proof. Since $\ker f \leq M$ and $\operatorname{im} f \leq N$, we have $\ker f \in \{(0), M\}$ and $\operatorname{im} f \in \{(0), N\}$. If $\ker f = (0)$, then $\operatorname{im} f = N$, so f is an isomorphism. But if $\ker f = M$, then f is the zero map. If $f \in \operatorname{End}_R(M) \setminus \{0\}$, then f is an isomorphism, so there exists an inverse. □

Example 1.12. *Suppose R is commutative, $I \lhd R$. Then we have*

$$\mathrm{End}_R(R/I) = \mathrm{End}_{R/I} \cong R/I, \quad f \mapsto f(1).$$

If M is a simple left R-module, then $M \cong R/I$ for some maximal $I \leq R$. Then $\mathrm{End}_R(M) \cong R/I$ is a field.

Example 1.13. *Let D be a division ring, V a D-module and $R = \mathrm{End}_D(V)$. Both D and R act on V and their actions commute:*

$$\varphi(d \cdot v) = d \cdot (\varphi(v)).$$

Because of that, we can define a map

$$\Psi : D \to \mathrm{End}_R(V), \quad d \mapsto (v \mapsto d \cdot v).$$

Such a Ψ is a isomorphism of rings; it is obviously injective, we just need to prove that is is onto. Suppose $T \in \mathrm{End}_R(V)$. Choose $v \in V \setminus \{0\}$. For any $w \in V$ there exists an endomorphism of V sending v to w, so $V = R \cdot v$. Hence every R-endomorphism (such as T) is determined by its image of v. So it suffices to show that $Tv = d \cdot v$ for some $d \in D$. T+here exists a projection $p \in \mathrm{End}_D(V) = R$ onto Dv. Thus

$$Tv = T(pv) = p(Tv) \in Dv.$$

Example 1.14. *Let k be a field, R a k-algebra and $M \in {}_R\mathrm{Mod}$ simple. Additionally, let $\dim_k M < \infty$. By Schur's lemma, $D := \mathrm{End}_R(M)$ is a division ring. Since $D \subseteq \mathrm{End}_k(M)$, it is also a finite-dimensional k-algebra. If k is an algebraically closed field (ACF), then $k \cong \mathrm{End}_R(M)$.*

Lemma 1.15. *A finitely dimensional division algebra D over an ACF is k itself.*

Proof. Take an arbitrary element $\alpha \in D$. Then the span of $\{1, \alpha, \alpha^2, \dots\}$ is finitely-dimensional, so $k(\alpha)/k$ is a finite field extension. Since k is an ACF, it admits no proper finite (even algebraic) extensions, so $k(\alpha) = k$. This gives us $\alpha \in k$. □

1.3 Semisimple modules

Definition 1.16. A module is semisimple if it is direct sum of simple modules.

Example 1.17.
- *Every simple module is semisimple.*
- *Every vector space over a division ring D is semisimple.*
- *A direct sum of semisimple modules is semisimple.*

Proposition 1.18. *If M is a left R-module that is a sum (not necessarily direct) of simple submodules M_i (where $i \in I$), then M_i is a semisimple module. Moreover, there is a subset $I' \leq I$ such that*

$$M = \bigoplus_{j \in I'} M_j.$$

Proof. A family of submodules M_j (where $j \in J$) is called independent if $\sum_{j \in J}^{\text{finite}} m_j = 0$ implies

$m_j = 0, \forall j \in J$. Equivalently, $\sum_{j\in J} M_j = \bigoplus_{j\in J} M_j$. Define

$$\mathcal{S} = \{J \subseteq I \mid (M_j)_{j\in J} \text{ is independent}\}.$$

Since $\mathcal{S} \neq \emptyset$, every chain in $\mathcal{S}$ has an upper bound (in this case, a union). Thus Zorn's lemma applies and there exists a maximal element $I' \in \mathcal{S}$. Set $M' = \sum_{i\in I'} M_i \leq M$. We have to prove that $M' = M$. For each $j \in I$, we have $M' \cap M_j \in \{(0), M_j\}$. If $M' \cap M_j = (0)$, then $I' \cup \{j\}$ is i-independent, contradicting maximality of I'. So $M' \cap M_j = M_j$ for each $j \in I$, hence $M' \supseteq \sum_{j\in I'} M_j$ and we are done. □

Corollary 1.19. *If M is semisimple, then so is every submodule and quotient module 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 let $M' \leq M$. Then M'/M is generated by the images $\overline{M_i}$ of the M_i (under $M \to M/M'$). if $\overline{M_i} \neq (0)$, then $\overline{M_i} \cong M_i$, since M_i is simple. Therefore M/M' is a sum of simple modules, thus semisimple. Moreover, there exists $I'' \subseteq I$ such that

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

Then

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

The module M' is also semisimple, since

$$M/\textstyle\bigoplus_{i\in I''} M_i = \displaystyle\bigoplus_{i\in(I\setminus I'')} M_i = M'.$$ □

Proposition 1.20. *Let M be a module such that every submodule of M is a direct summand. Then M is semisimple.*

Remark. We say that such M has the complement property.

Proof.
1. First we notice that any $N \leq M$ has the complement property.
2. Next, we prove that there exists a simple submodule of M. Let's choose an arbitrary cyclic submodule $(0) \neq M' \leq M$, say $M' = Rm$ for some $m \in M'$. By Zorn's lemma, there exists a maximal proper submodule $M'' \lneq M'$. Then M'/M'' is simple. Because M' has complement property, there exists a submodule $S \leq M' \leq M$ such that $M' = M'' \oplus S$. But then $S = M'/M''$ is a simple submodule of M that we were looking for.
3. We define
$$M_1 = \sum \{\text{simple submodules of } M\} \leq M.$$
There exists a submodule $M_2 \leq M$ such that $M = M_1 \oplus M_2$. If $M_2 \neq (0)$, then the second point shows that M_2 has a simple submodule, say $S_2 \leq M_2$. By construction, $S_2 \subseteq M_1$ and we arrive at a contradiction. Therefore $M_2 = (0)$ and $M = M_1$ is semisimple. □

1.4 Endomorphism ring of a semisimple module

Proposition 1.21. *Let $M \in {}_R\mathrm{Mod}$, $S \in \mathrm{End}_R(M)$ and $p, m, n \in \mathbb{N}$. There is a canonical isomorphism of an abelian group*

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

such that the composition

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

corresponds to matrix multiplication

$$S^{m\times n} \times S^{n\times p} \to S^{m\times p}$$
$$(A, B) \mapsto A \cdot B.$$

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

Proof. Let $f : M^n \to M^m$. We have

$$M \xrightarrow{\iota_j} M^n \xrightarrow{f} M^m \xrightarrow{\pi_i} M, \qquad \alpha_{ij} : M \to M$$

where ι_j is the inclusion into the j-th summand and π_i is the projection onto the i-th summand. Then the isomorphism

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

is given by a map $f \mapsto [\alpha_{ij}] \in S^{m\times n}$. Conversely, given $[\alpha_{ij}]_{i,j}$ define

$$f(x_1, \dots, x_n) = (y_1, \dots, y_m)$$

where $y_i = \sum_{j=1}^n \alpha_{ij} x_j$. □

For an element $r \in R$ define a R-linear map

$$T_r : R \to R, \quad x \mapsto x \cdot r.$$

Notice that we have

$$T_r \circ T_s = T_{sr}.$$

Now define

$$\Phi : R \to \mathrm{End}_R(R), \quad r \mapsto T_r.$$

This map is a bijection. It's clearly injective, since $T_r = T_s$ implies

$$r = T_r(1) = T_s(1) = s.$$

But it is also onto, because for every $f \in \mathrm{End}_R(R)$ we have $f = T_{f(1)}$. If R is commutative, then $\mathrm{End}_R(R) \cong R$. But in general, $\mathrm{End}_R(R) \cong R^{\mathrm{op}}$.

Example 1.22. *Let D be a division ring. Then any D-linear map $D^n \to D^n$ can be represented as a matrix with entries in* $\mathrm{End}_D(D) \cong D^{\mathrm{op}}$*, hence*

$$\mathrm{End}_D(D^n) \cong M_n(\mathrm{End}_D(D)) = M_n(D^{\mathrm{op}}).$$

Definition 1.23. A semisimple module has finite length if it is a finite direct sum of simple modules.

Proposition 1.24. *If $M \in_R$ Mod is semisimple of finite length, then* $\mathrm{End}_R(M)$ *is isomorphic to a finite product of matrix rings over division rings.*

Proof. Let $M \cong \bigoplus_{i=1}^k M_i^{n_i}$, where M_i are simple (we call them isotypical components) and $M_i \ncong M_j$ for $i \neq j$. By Schur's lemma, we have $\mathrm{Hom}_R(M_i, M_j) = (0)$ for $i \neq j$. So every endomorphism

of M must take each isotypical component into itself. Hence

$$\begin{aligned}\mathrm{End}_R(M) &= \mathrm{End}_R\left(\bigoplus_{i=1}^{k} M_i^{n_i}\right)\\ &= \prod_{i=1}^{k} \mathrm{End}_R(M_i^{n_i})\\ &= \prod_{i=1}^{k} M_{n_i}(\mathrm{End}_R(M_i)),\end{aligned}$$

where $\mathrm{End}_R(M_i)$ is a division ring by Schur's lemma. □

1.5 Semisimple rings

Definition 1.25. Ring R is (left) semisimple ring if it is a semisimple left R-module.

Theorem 1.26.

For a ring the following is equivalent.

1. *R is semisimple;*
2. *every R-module is semisimple;*
3. *any short exact sequence of R-modules splits.*

Proof. Start with the statement (1) ⇒ (2). Since $R \in {}_R\mathrm{Mod}$ is semisimple, so for any index set I, $\bigoplus_I R \in {}_R\mathrm{Mod}$ is semisimple. Any $M \in {}_R\mathrm{Mod}$ is a quotient of some free R-module $\bigoplus_I R$ and is therefore semisimple by an earlier proposition. The implication (2) ⇒ (3) follows from the fact that semisimple modules have the complement property. Finally, we need to prove the implication (3) ⇒ (1). Let $I \leq_R R$. Then

$$0 \to I \to R \to R/I \to 0$$

is a short exact sequence. By assumption it splits, so I is a direct summand of R. So R has the complement property, so it is semisimple. □

Corollary 1.27. *Suppose R is semisimple. Then $R \in {}_R\mathrm{Mod}$ has finite length and any simple R-module is isomorphic to a simple component of R. In particular, there are only finitely many nonisomorphic simple R-modules.*

Proof. Let $R \cong \bigoplus_{i\in I} M_i$ as R-module, where M_i are simple. Recall that R is generated by $1 \in R$, so the set I must be finite. Indeed, write $1 = \sum_{i\in I} e_i$, where $e_i \in M_i$ and $e_i \neq 0$ for finitely many indices i. Let M_i be some module such that $e_i = 0$ and $x \in M_i$. Then $x = 1 \cdot x = e_i = 0$ and M_i is a zero module. Therefore R is of finite length. Suppose $M \in {}_R\mathrm{Mod}$ is simple. Then we have the surjective map

$$\bigoplus_{i\in I} M_i \cong R \to M = Rm$$

and thus at least one of the induced maps $M_i \to M$ is nonzero, therefore an isomorphism by Schur. □

Example 1.28. *Any division ring D is semisimple; D is a simple D-module.*

Example 1.29. *If F is a field, then $F[x]$ is not semisimple.*

Example 1.30. *The ring $\mathbb{Z}$ is not semisimple, since the simple $\mathbb{Z}$-modules $\mathbb{Z}/p\mathbb{Z}$ and there's infinitely many of them. Additionally, we know that $\mathbb{Z} \ncong \mathbb{Z}/p\mathbb{Z}$ for every prime p.*

Example 1.31. *Let D be a division ring and V a n-dimensional vector space over D. Let $R = \mathrm{End}_D(V)$. Then R is semisimple. Indeed, let $\{e_1, \dots, e_n\}$ be a basis of V. Define a map*

$$\Omega : R \to V \oplus \cdots \oplus V, \quad f \mapsto (f(e_1), \dots, f(e_n))$$

and it is clear to see that Ω is an isomorphism. Since we know that V is a simple R-module, $R \cong V^n$ is a semisimple R-module, so R is a semisimple ring like we wanted. Notice that R has a unique simple R-module, namely V. In matrix form, we have

$$\mathrm{End}_D(V) = \mathrm{End}_D(D^n) \cong M_n(D^{\mathrm{op}}).$$

The space

$$V_i = \begin{pmatrix} 0 & \cdots & a_{1i} & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & a_{ni} & \cdots & 0 \end{pmatrix}$$

is a simple submodule of $M_n(D^{\mathrm{op}}) \cong \mathrm{End}_D(V) = R$ and $R \cong \bigoplus_{i=1}^r V_i$, where $V_i \cong V$.

Example 1.32. *If R, S are semisimple rings, then $R \times S$ is semisimple.*

Corollary 1.33. *A finite product of matrix rings over division rings is semisimple.*

1.6 Wedderburn structure theorem

Theorem 1.34 (Wedderburn)**.**

Every semisimple ring R is isomorphic to a finite product of matrix rings over division rings. If R is also commutative, then it is a finite direct product of fields.

Proof. We know that $R \in {}_R\mathrm{Mod}$ is semisimple of finite length, so $R^{\mathrm{op}} \cong \mathrm{End}_R(R)$ is isomorphic to a finite product $\prod M_{n_i}(D_i)$. Then we have

$$R \cong (R^{\mathrm{op}})^{\mathrm{op}} \cong \left(\prod M_{n_i}(D_i)\right)^{\mathrm{op}} = \prod M_{n_i}(D_i)^{\mathrm{op}} \cong \prod M_{n_i}(D_i^{\mathrm{op}}). \qquad \square$$

Definition 1.35. A ring is simple if it has no nontrivial proper two-sided ideals.

Remark.
1. This is not the same as R being a simple R-module. For example $M_n(D)$ is a simple ring but is not simple as a module.
2. Simple ring is not necessarily semisimple: an example would be $\mathcal{A}(k)$.

Theorem 1.36.

Let R be semisimple and $S_1, \dots, S_s$ be, up to isomorphism, all the distinct simple left R-modules. Let R_i be the sum of all the minimal left ideals $L \cong S_i$ of R. Then R_i is a two-sided ideal of R, R_i

is a simple left artinian ring and

$$R = R_1 \times \cdots \times R_s.$$

Proof. Pierre Antoine Grillet, proposition IX.3.9. □

Remark. Here, we the product of rings was "internal" (see the above reference).

Proposition 1.37 (Uniqueness of decomposition of semisimple rings)**.** *If* $R = \prod_{i=1}^{n} R_i$ *and* $R = \prod_{j=1}^{m} R'_j$*, where* R_i, R'_j *are simple rings, then* $n = m$ *and each* R_i *equals some* R'_j*.*

Proof. Since $R_i \lhd R$, we have $R_i R = R_i$. From $R = \prod R'_j$ we get $R_i = \prod_j R_i R'_j$. Since $R_i R'_j \lhd R_i$ and R_i is simple, we either have $R_i R'_j = (0)$ or $R_i R'_j = R_i$. There has to exist some j such that $R_i R'_j = R_i$. But since $R_i R'_j \lhd R'_j$ and R'_j is also simple, we have $R_i = R'_j$. We then proceed by induction. □

1.7 Jacobson radical

Definition 1.38. Jacobson radical of a ring R, denoted by $\operatorname{rad} R$, is the intersection of all maximal left ideals of R.

Lemma 1.39. *For* $y \in R$ *the following is equivalent.*

1. $y \in \operatorname{rad} R$*;*
2. $1 - xy$ *is left invertible,* $\forall x \in R$*;*
3. *for every simple* $M \in {}_R\operatorname{Mod}$ *we have* $yM = (0)$*.*

Proof. We start with (1) ⇒ (2). We prove by contraposition: if there exists $x \in R$ such that $1 - xy$ is not left invertible. Then $R(1 - xy) \lhd R$ is a proper left ideal of R, so by Zorn lemma there exists a maximal left ideal m such that $R(1 - xy) \subseteq m \lhd R$. In particular, $1 - xy \in m$. But since m is maximal, y can't be included in it and as a result $y \notin \operatorname{rad} R$. We now prove the second implication (2) ⇒ (3). If (3) fails, then there exists an element $m \in M$ such that $y \cdot m \neq 0$, so by simplicity of R we get $R(ym) = M$. There exists a $x \in R$ such that $xym = m$ or equivalently $(1 - xy)m = 0$, which means $(1 - xy)$ is not left invertible. Lastly, we show that (3) ⇒ (1). Take an arbitrary left maximal ideal $m \lhd R$. Then $R/m \in {}_R\operatorname{Mod}$ is simple, so $y \cdot R/m = (0)$, so $y \in m$. But since m is arbitrary, we have $y \in \operatorname{rad} R$. □

Definition 1.40. Annihilator of $M \in {}_R\operatorname{Mod}$ is

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

We notice that $\operatorname{ann}(M) \lhd R$.

Corollary 1.41. $\operatorname{rad} R = \bigcap\{\operatorname{ann} M \mid M \in {}_R\operatorname{Mod}$ *simple*$\}$

Lemma 1.42. *For* $y \in R$ *the following is equivalent.*

1. $y \in \operatorname{rad} R$*;*
2. $1 - xyz$ *is invertible,* $\forall x, z \in R$*.*

Proof. It's enough to show that (1) ⇒ (2). If $y \in \operatorname{rad} R$, then $yz \in \operatorname{rad} R$ and $1 - xyz$ is left invertible, so there exists $u \in R$ so that $u(1 - xyz) = 1$. Since $xyz \in \operatorname{rad} R$, $1 - u(xyz) = u$ is left

invertible. So u is left and right invertible and we have $(1-xyz)^{-1} = u$. □

Proposition 1.43.
- *Jacobson radical* $\operatorname{rad} R$ *is the largest (left) ideal* J *satisfying* $1 + J \subseteq R^{-1}$.
- *Jacobson radical for left ideals concides with the one for right ideals.*
- *Suppose* $I \lhd R$ *and* $I \subseteq \operatorname{rad} R$. *Then* $\operatorname{rad}(R/I) = \operatorname{rad} R/I$.

Proof. We only prove the third item. The maximal left ideals in R/I correspond to the maximal left ideals in R which contain I, and the rest is routine. □

Definition 1.44. A ring R is J-semisimple if $\operatorname{rad} R = (0)$.

Remark. Note that for each ring R, the ring $R/\operatorname{rad} R$ is J-semisimple.

Proposition 1.45.
- R *and* $R/\operatorname{rad} R$ *have the same simple left modules.*
- *A element* $x \in R$ *if (left) invertible iff* $\overline{x} = x + \operatorname{rad} R$ *is (left) invertible in* $R/\operatorname{rad} R$.

Proof.
- First point follows from (1) ⇒ (3) in the lemma above.
- It's enough to prove (⇐). Suppose $\overline{yx} = 1$ for some $y \in R$. Then $1 - yx \in \operatorname{rad} R$, so $yx \in 1 + \operatorname{rad} R \subseteq R^{-1}$ and yx is invertible, therefore x has a left inverse. □

Definition 1.46. A one-sided or two-sided ideal $I \subseteq R$ is:
- nil if all its elements are nilpotent;
- nilpotent if there exists $n \in \mathbb{N}$ such that $I^n = (0)$.

Example 1.47. *Let* $R = \mathbb{Z}[x_1, x_2, x_3 \dots]/(x_1^2, x_2^3, x_3^4, \dots)$. *Then* $I = (\overline{x_1}, \overline{x_2}, \overline{x_3}, \dots)$ *is nil but not nilpotent.*

Lemma 1.48. *If* $I \leq {}_R R$ *is nil, then* $I \subseteq \operatorname{rad} R$.

Proof. Let $y \in I$. Then $xy \in I$ for all $x \in I$, so xy is nilpotent. Say $(xy)^n = 0$. Then $1 - xy$ is invertible and its inverse is

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

□

Theorem 1.49.

Suppose R *is left artinian. Then* $\operatorname{rad} R$ *is the largest nilpotent left ideal.*

Proof. By lemma, it suffices to show $\operatorname{rad} R$ is nilpotent. Consider a descending chain

$$\operatorname{rad} R \supseteq (\operatorname{rad} R)^2 \supseteq (\operatorname{rad} R)^3 \supseteq \cdots$$

Since R is left artinian, there exists a $k \in \mathbb{N}$ such that

$$(\operatorname{rad} R)^k = (\operatorname{rad} R)^{k+1} = \cdots = I.$$

We now prove that $I = (0)$. Suppose it wasn't. By the artinian property, we have a minimal left ideal I_0 such that $I \cdot I_0 \neq (0)$, hence $\exists a \in I_0$ such that $I \cdot a \neq (0)$. Then

$$I \cdot (Ia) = I^2 a = Ia \neq (0),$$

so $Ia = I_0$. In particular, there exists $y \in I$ such that $ya = a$ or equivalently $(1-y)a = 0$. But since $y \in I \subseteq \operatorname{rad} R$, we have $1 - y \in R^{-1}$. Thus $a = 0$ and we have a contradiction. □

Theorem 1.50.

For a ring R the following is equivalent.

1. *R is semisimple.*
2. *R is J-semisimple and left artinian.*

Corollary 1.51. *Simple left artinian ring is semisimple.*

Proof. We begin with the implication (1) ⇒ (2). If R is semisimple, then it is left artinian (Artin-Wedderburn theory). Since R is semisimple, there exists $I \leq {}_R R$ such that $R = \operatorname{rad} R \oplus I$. If $\operatorname{rad} R \neq (0)$, then $I \subsetneq R$, so there exists a maximal submodule $m \leq {}_R R$ such that $I \subseteq m$. Hence $I \subseteq m$ and $\operatorname{rad} R \subseteq m$ which implies $R = \operatorname{rad} R + I \subseteq m$, a contradiction. Now the converse (2) ⇒ (1). By definition

$$\operatorname{rad} R = \bigcap_{m^{\max} \leq_R R} m$$

and since R is artinian, there exist $m_1, \ldots, m_n^{\max} \leq {}_R R$ such that

$$\operatorname{rad} R = \bigcap_{i=1}^{n} m_i.$$

Consider

$$\varphi : R \to \bigoplus_{i=1}^{r} R/m_i, \quad x \mapsto \oplus(x + m_i).$$

This is obviously a homomorphism of R-modules. We have

$$\ker \varphi = \bigcap_{i=1}^{n} m_i = \operatorname{rad} R = (0),$$

so it is also injective. Since ${}_R R \leq \bigoplus_{i=1}^{n} R/m_i$, ${}_R R$ is also semisimple. □

Example 1.52. *Let k be a field and R a ring of upper-triangular $n \times n$ matrices on k and let J be the set of all matrices in R with the zero diagonal. It's clear to see that $\operatorname{rad} R = J$. Indeed, since $J^n = (0)$, J is nilpotent and therefore included in R. But since*

$$R/J \cong \begin{pmatrix} k & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & k \end{pmatrix} \cong k \times \cdots \times k$$

is semisimple, it is J-semisimple and we can conclude

$$\operatorname{rad} R/J = \operatorname{rad}(R/J) = (0),$$

so $J = \operatorname{rad} R$. We can also point out that R has n simple modules. They are $V_i = {}_R k$ with the

action

$$\begin{pmatrix} a_{11} & * & * \\ & \ddots & * \\ & & a_{nn} \end{pmatrix} \cdot b = a_{ii} b.$$

Lemma 1.53 (Nakayama)**.** *For a left ideal $J \leq {}_R R$ the following is equivalent.*

1. *$J \subseteq \operatorname{rad} R$.*
2. *For every finitely generated $M \in {}_R\operatorname{Mod}$ we have*

$$JM = M \Rightarrow M = (0).$$

3. *For every $N, M \in {}_R\operatorname{Mod}$ such that $N \subseteq M$ and M/N is finitely generated, we have*

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

Proof. First we prove (1) $\Rightarrow$ (2). Suppose $M \neq (0)$ is finitely generated and take a ,minimal set of generators $x_1, \ldots, x_k$. Since $JM = M$, there are $a_1, \ldots, a_k \in J$ such that

$$x_k = a_1 x_1 + a_2 x_2 + \cdots + a_k x_k.$$

Thus $(1 - a_k)x_k = a_1 x_1 + \cdots + a_{k-1} x_{k-1}$. But $1 - a_k \in 1 + J \subseteq 1 + \operatorname{rad} R \subseteq R^{-1}$, so $x_k \in Rx_1 + \cdots + Rx_{k-1}$, which contradicts our assumption of minimality. The implication (2) $\Rightarrow$ (3) is proved by directly applying item (2) to M/N. Lastly, we need to prove (3) $\Rightarrow$ (1). Suppose there exists $y \in J \setminus \operatorname{rad} R$. Then there exists a maximal ideal $m \leq {}_R R$ such that $y \notin m$. Then $m + J = R$, so $m + J \cdot R = R$. Now we apply (3) to get $m = R$, which is a contradiction. □

1.8 Group rings and Maschke's theorem

Recall: given a group G and field k, the group ring kG is a vector space with basis G and multiplication induced by G.

Theorem 1.54 (Maschke**).**

Suppose G is a finite group and $\operatorname{char} k$ is not a divisor of $|G|$. Then kG is semisimple.

Proof. Let $W \leq V$ be kG-modules. In particular, W, V are k-vector spaces. That means there exists a k-linear map $f : V \to W$ such that $f\big|_W = \mathrm{id}$. Define a new map $g : V \to V$ by

$$v \mapsto \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma v).$$

It's obvious that g maps to W. We now prove that $g\big|_W = \mathrm{id}$:

$$\begin{aligned} g(w) &= \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma w) \\ &= \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} \sigma w \\ &= \frac{1}{|G|} \sum_{\sigma \in G} w \\ &= w. \end{aligned}$$

Clearly, g is k-linear since it is a sum of k-linear maps. We just have to prove that g is a kG-module

homomorphism. Let $v \in V$ and $\tau \in G$:

$$\begin{aligned} g(\tau \cdot v) &= \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma\tau v) \\ &= \frac{1}{|G|} \sum_{\sigma\tau \in G} \tau(\sigma\tau)^{-1} f(\sigma\tau v) \\ &= \frac{1}{|G|} \sum_{\sigma' \in G} \tau(\sigma')^{-1} f(\sigma' v) \\ &= \tau \cdot \frac{1}{|G|} \sum_{\sigma' \in G} (\sigma')^{-1} f(\sigma' v) \\ &= \tau \cdot g(v). \end{aligned}$$

Since $V = W \oplus \ker g$ and $\ker g \leq {}_{kG}V$, V has the complement property, hence is semisimple. So kG has to be semisimple. □

Proposition 1.55. *If k is a field and G is an infinite group, then kG is not semisimple.*

Proof. Consider the augmentation map $\varepsilon : kG \to k$, given by $\varepsilon\big|_k = \mathrm{id}$ and $\varepsilon(g) = 1$, $\forall g \in G$. The map ε is not only a homomorphism of modules, but also of rings. Denote $I = \ker \varepsilon \leq kG$. (DOPOLNI) □

Remark. 1. $\mathbb{C}G$ is always J-semisimple.

2. If G is finite and $\operatorname{char} k$ divides $|G|$, then kG is not semisimple.

Example 1.56. *The ring $\mathbb{C}S_3$ is semisimple by Maschke's theorem. By Wedderburn, we have*

$$\mathbb{C}S_3 \cong \prod_{i=1}^{r} M_{n_i}(D_i),$$

where D_i are division rings that include $\mathbb{C}$. Since $\dim_{\mathbb{C}} \mathbb{C}S_3 = |S_3| = 3! = 6$, we have $\dim_{\mathbb{C}} D_i < \infty$ and since $\mathbb{C}$ is an ACF, we have $D_i = \mathbb{C}$, so

$$\mathbb{C}S_3 = \prod_{i=1}^{r} M_{n_i}(\mathbb{C}).$$

Its dimension is $6 = \sum_{i=1}^{r} {n_i}^2$. Since $6 = 1+1+1+1+1+1 = 4+1+1$, we have two options: $CS_3 = \mathbb{C}^6$ or $CS_3 = M_2(\mathbb{C}) \times \mathbb{C} \times \mathbb{C}$. Since CS_3 is not commutative, we get $CS_3 = M_2(\mathbb{C}) \times \mathbb{C} \times \mathbb{C}$.

2 Primitive rings

In commutative rings, we often reduce the general problem to a problem for fields. If we have a commutative ring R, then we can quotient it with its Jacobson radical to get a reduced ring (i. e. a ring with no nilpotents). Then we can quotient it with a prime ideal to get an integral domain (i. e. a ring with no zero divisors). Lastly, we take a quotient ring of our integral domain to reduce a problem to a field.

In noncommutative case, we would like to proceed as follows: from a general ring, we want to obtain a ring without nilpotents, from which we would get domains and lastly division ring. The problem is that in general, there is no way to reduce a problem on domain to a problem on a division ring.

Example 2.1. *Let H be the monoid generated by a, b, c, d, u, v, x, y subject to*

$$ax = by, \quad au = bv, \quad cx = dy.$$

In matrix form, that would be

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & u \\ -y & -v \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix}.$$

The H is a cancellative monoid and there does not exist a group G containing H. If there were, then

$$cu = cxx^{-1}a^{-1}au = dyy^{-1}b^{-1}bv = dv,$$

a contradiction. Furthermore, given a field k the semigroup algebra kH is a domain that does not embed in a division ring.

Example 2.2. *There exist domains that embed into different division rings. Let $k\langle x, y\rangle$ be a free algebra on 2 generators. This free algebra embeds into a division algebra; in fact it embeds into many.*

1. *Let's start with $k[x; \sigma]$ which embeds into a division ring (Ore domains).*
2. *Let R be a ring and $a, b \in R$ two R-independent elements. Define*

$$C := \{x \in R \mid ax = xa,\ bx = xb\}$$

   and the subring of R, generated by C, a, b, is isomorphic to $C\langle u, v\rangle$.
3. *Let C be a field, $k := C(t)$ and $n > 1$. Define $\sigma_n \in \mathrm{End}(k)$ by $\sigma_n\big|_C = \mathrm{id}$ and $\sigma_n(t) = t^n$. By the first item, we can embed R_n into some division ring D_n. Without loss of generality, we can assume that D_n is generated as a division ring by D_n, so we have a ring epimorphism from R_n to D_n. By the second item, the map*

$$u \mapsto x, \quad v \mapsto t \cdot x$$

   is an surjective embedding of $C\langle u, v\rangle$ into R_n. But $n \in \mathbb{N}$ was arbitrary, so we have surjective embeddings of $C\langle u, v\rangle$ into different division rings D_n and D_m for $n \neq m$, which proves our goal.

A second approach for noncommutative rings would be to focus on ideals instead of elements. We would ideally reduce rings to semiprime rings where (0) would be a semiprime ideal (a semiprime ideal $I \lhd R$ is an ideal such that $(a) \cdot (a) \subseteq I$ implies $a \in I$). From there we would proceed to prime rings where (0) is a prime ideal ($I \lhd R$ is prime if $(a)(b) \subseteq I$ implies $a \in I$ or $b \in I$). Lastly, we would reduce our problem from prime to simple rings. This approach is better than the first, but still not feasible. Instead of ideals, let's focus on modules!

Definition 2.3. A ring R is primitive if it is a faithful simple module M (meaning that $\mathrm{ann}_R(M) = (0)$). The module M is faithful iff the map

$$\rho : R \mapsto \mathrm{End}_R(M), \quad r \mapsto (m \mapsto r \cdot m)$$

is injective. If M is also simple, such a ρ is called an irreducible representation.

Example 2.4. *Simple artinian rings (By Wedderburn these are $M_n(D)$) are exactly those artinian rings that have a faithful simple module (namely D^n). Hence simple artinian rings are primitive.*

Example 2.5. *Let R be a simple ring and $I <_R R$ a maximal left ideal. Then $M := R/I \in {}_R\mathrm{Mod}$ is simple. Let $\rho : R \to \mathrm{End}_R(M)$ be a representation. Since $\ker\rho \lhd R$ and R is simple, we get $\ker\rho = (0)$ and M is faithful.*

Example 2.6. *Let D be a division ring and V a D-vector space (can be infinitely-dimensional). It's trivial to check that $R = \mathrm{End}_D(V)$ is faithful, but if $\dim_D V = \infty$, it is not simple.*

2.1 Density theorem

Definition 2.7. Let V be a vector space over a division ring D and let $R \subseteq \mathrm{End}_D(V)$ be a subring. Then R is a dense ring of linear transformations (R acts densely on V) if for every finite set $\{v_1, \dots, v_n\} \subseteq V$ of linearly independent vectors and any $\{w_1, \dots, w_n\} \subseteq V$ there exists $\phi \in R$ such that $\phi(v_i) = w_i$.

Example 2.8. *Let $\dim_D V < \infty$ and R acts densely on V. We can show that $R = \mathrm{End}_D(V)$. Let $\phi \in \mathrm{End}_D(V)$ and pick a basis $\{v_1, \dots, v_n\}$ of V By density, there exists a $\psi \in R$ such that ϕ and ψ agree on a basis $\{v_1, \dots, v_n\}$. But that means that $\phi = \psi \in R$.*

Remark. Endow V with the discrete topology and $\mathrm{End}_D(V)$ with the compact-open topology. The R acts densely on V iff R is dense in $\mathrm{End}_D(V)$ with regards to the compact- open topology.

Theorem 2.9 (Density)**.**

Let $M \in {}_R\mathrm{Mod}$ be semisimple, $S = \mathrm{End}_R(M)$ and $\phi \in \mathrm{End}_S(M)$. Then for any finite set $\{x_1, \dots, x_n\} \subseteq M$ there exists $r \in R$ such that $\phi(x_i) = r \cdot x_i$ for all $i = 1, \dots, n$.

Proof. Start with $n = 1$. The module $Rx_1 \leq M$ is complemented in M: there exists $M' \leq M$ such that $M = Rx_1 \oplus M'$. Define a projection $\pi : M \to Rx_1$. Clearly, $\pi \in S$, so we have

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

and

$$\phi(x_1) \in \{y \in M \mid \pi(y) = y\} = Rx_1.$$

Now onto the general n. Define a map

$$\phi^{(n)} : M^n \to M^n, \quad (y_1, \dots, y_n) \mapsto (\phi(y_1), \dots, \phi(y_n)).$$

By assumption, $\phi^{(n)} \in \mathrm{End}_{\mathrm{End}_R(M^n)}(M^n)$ and $M_n(\mathrm{End}_R(M)) = M_n(S)$. By the case $n = 1$, there exists $r \in R$ such that

$$(rx_1, \dots, rx_n) = \phi^{(n)}(x_1, \dots, x_n) = (\phi x_1, \dots, \phi x_n). \qquad \square$$

Theorem 2.10 (Jacobson density theorem)**.**

A ring R is primitive iff R is a dense ring of linear transformations on a vector space over a division ring.

Proof. Start with the right direction ($\Rightarrow$). Let $M \in {}_R\mathrm{Mod}$ faithful and simple. By Schur's lemma, $D = \mathrm{End}_R(M)$ is a division ring. Clearly, M is a D-vector space. Since M is faithful, we have

$R \subseteq \mathrm{End}_D(M)$, so R acts as a ring of linear transformations on D. Now we just have to prove that it acts densely. Let $\{v_1, \dots, v_n\}$ be D-linearly independent in M and let $\{w_1, \dots, w_n\} \subseteq M$. As before, there exists a linear transformation ϕ such that $\phi(v_i) = w_i$ for all i. Thus $\phi \in \mathrm{End}_D(M)$. Apply the previous density theorem for semisimple modules, so there exists $r \in R$ such that

$$r \cdot v_i = \phi(v_i) = w_i$$

for all i. Hence R acts densely on M. Now the converse direction ($\Leftarrow$). Suppose R acts densely on a vector space V on a division ring D. In particular, V is a R-module. By definition, $R \subseteq \mathrm{End}_D(V)$, so V is a faithful R-module. We now have to prove that it is also simple. Pick a $v \in V \setminus \{0\}$. By density, for any $w \in V$ there exists a $\phi \in R$ such that $\phi(v) = w$, meaning that $Rv = V$. □

This brings us to the statement that we have already seen before. We can prove it again using primitive rings.

Corollary 2.11. *Any simple artinian ring R is isomorphic to $M_n(D)$ for some division ring D.*

Proof. Since R is simple, it is primitive. Let $M \in {}_R\mathrm{Mod}$ be faithful R-module, $D = \mathrm{End}_R(M)$ is a division ring by Schur's lemma. By Jacobson's density theorem, R is a dense subring of $\mathrm{End}_D(M)$, which is $\mathrm{End}_D(M)$ itself. Now assume $\dim_D M = \infty$ and let $v_1, v_2, \dots$ be a set of linearly independent vectors in M. Define

$$I_n = \{r \in R \mid rv_i = 0 \text{ for } 1 \le i \le n\} \le {}_R R.$$

Then $I_1 \supset I_2 \supset I_3 \supset \cdots$ This chain is strictly decreasing. By density, there exists $r \in R$ such that $rv_i = 0$ for $i = 1, \dots, n$ and $rv_{n+1} \neq 0$. This infinitely descending chain of submodules violates the artinian assumption. So $\dim_D V < \infty$, which implies $R = \mathrm{End}_D(M) \cong M_{\dim_D V}(D)$. □

Theorem 2.12 (Structure theorem for primitive rings**).**

Let R be a primitive ring with a faithful simple module M. Let $D = \mathrm{End}_R(M)$. Then at least one of the following is true:

1. *$R \cong M_n(D)$ for some $n \in \mathbb{N}$ or*
2. *for every $n \in \mathbb{N}$ there exists a subring $R_n \subseteq R$ such that there is a surjective homomorphism $R_n \to M_n(D)$.*

Proof. If $\dim_D M < \infty$, then as previously we have $R = \mathrm{End}_D(M) \cong M_n(D)$ for $n = \dim_D M$. Now assume $\dim_D M = \infty$. If $x_1, x_2, \dots$ is an infinite set of linearly independent vectors in M, form a span the first n vectors (call it V_n). This is of course a D-subspace of M. Define

$$R_n := \{r \in R \mid r \cdot V_n \subseteq V_n\}, \quad I_n = \{r \in R \mid rv_i = 0,\ 1 \le i \le n\}.$$

Then $I_n \lhd R_n$ and by Jacobson, $R_n / I_n \cong M_n(D)$. □

Remark.

1. In the case of finite-dimensional algebras, the notions of primitive and simple coincide.
2. The free algebra is primitive (so any algebra is the image of some primitive algebra).

2.2 An application of primitive rings

Example 2.13. *Suppose R is a ring in which $x^2 = x$ for all $x \in R$. Then R is commutative.*

Proof. (DOPOLNI) □

Theorem 2.14 (Jacobson)**.**

Let R be a ring such that for all $x \in R$ there exists $n > 1$ such that $x^n = x$. Then R is commutative.

Theorem 2.15 (Jacobson-Herstein)**.**

A ring R is commutative iff

$$\forall x, y \in R : \ \exists n > 1 : \ (xy - yx)^n = xy - yx. \tag{1}$$

Proposition 2.16. *R is J-semisimple iff there exists a faithful semisimple module M.*

Proof. Start with the left implication ($\Leftarrow$). We know that $\operatorname{rad} R$ kills every simple R-module. Since M is semisimple, we have $\operatorname{rad} R = (0)$. Now the opposite direction ($\Rightarrow$). Let $(M_i)_i$ be all non-isomorphic simple R-modules. Then $M = \bigoplus_i M_i$ is semisimple and $\operatorname{ann}(M) = \bigcap_i \operatorname{ann} M_i = \operatorname{rad} R$. By J-semisimplicity, $\operatorname{ann}(M) = 0$, so M is a faithful R-module. □

Corollary 2.17. *Every J-semisimple R is a subdirect product of primitive rings.*

Proof. We know that $\operatorname{rad} R = \bigcap_i \operatorname{ann}(M_i) = \{0\}$, so $R \hookrightarrow \prod_i R/\operatorname{ann}(M_i)$ is the desired representation. □

This lends us a convienient way of tackling problems on noncommutative rings. We first kill the Jacobson radical of the original ring in order to obtain a J-semisimple (also called semiprimitive) ring. From the previous corollary, we can write any J-semisimple ring as a subdirect product of primitive rings, which we can reduce to division rings (or matrices over those) using density.

Proof of Jacobson-Herstein.

1. For now we assume that the conclusion holds for division rings. This will be proved in the next chapter.
2. Let R be a primitive ring that satisfies (1). By the structure theorem, we either have $R \cong M_n(D)$ for some $n \in \mathbb{N}$ or for every $n \in \mathbb{N}$ there exists a subring $R_n \subseteq R$ such that there is a surjective homomorphism $R_n \to M_n(D)$. If $n \geq 2$ then $M_2(D)$ does not satisfy the Jacobson-Herstein property (take for example $x = E_{11}$ and $y = E_{12}$). So the first statement applies and $R = D$ is a division ring, so we are done.
3. Now suppose R is J-semisimple and satisfies (1). We know that R is a subring of $\prod_i R_i$, where R_i are primitive and satisfy (1), so the're commutative. This implies that $\prod_i R_i$ is commutative and so is R.
4. Let R be an arbitrary ring with the property (1). Then $R/\operatorname{rad} R$ is J-semisimple and also satisfies (1), so it is commutative. Thus $d := [a, b] = ab - ba \in \operatorname{rad} R$ for any $a, b \in R$. Since there exists a $n \in \mathbb{N}$ such that $d^n = d$, we have $d(1 - d^{n-1}) = 0$. But since d^{n-1} is in $\operatorname{rad} R$, it is left-invertible, so $d = 0$. □

3 Central simple algebras

3.1 Cyclic algebras

If D is a division ring with center $Z(D)$, then $Z(D)$ is a field. If $\dim_{Z(D)} D = \infty$, we cannot say much in general. But for the case $\dim_{Z(D)} D < \infty$, the theory is very well developed.

Example 3.1. *Let k be a field and σ a k-automorphism. Then*

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

with the multiplication rule

$$x \cdot a = \sigma(a)x, \quad \forall a \in k$$

is a division ring.

Proposition 3.2. *Let $k_0 = \{a \in k \mid \sigma(a) = a\}$ be the fixed field of σ. Then*

$$Z(D) = \begin{cases} k_0; & \sigma \text{ of order } \infty \\ k_0((x^s)); & \sigma \text{ of order } s \end{cases}.$$

Morover, $\dim_{Z(D)} D < \infty$ iff σ is of finite order.

Proof. Let $f = \sum_{i=m}^{\infty} a_i x^i \in Z(D)$ and $a_j \neq 0$. For all $a \in k$ we have $af = fa$. Notice that

$$af = \sum aa_i x^i, \quad fa = \sum a_i \sigma^i(a) x^i.$$

From there we get $aa_i = a_i\sigma^i(a) = \sigma^i(a)a_i$. If $a_j \neq 0$, we have $\sigma^j(a) = a$ for all $a \in k$.

(a) Firstly, if σ has ∞ order, then $\sigma^j = \mathrm{id}$ implies $j = 0$, so $f = a_0 \in k$. Since $f \in Z(D)$, we have

$$\sigma(a_0)x = xa_0 = xf = fx = a_0 x,$$

so $f = a_0 = \sigma(a_0)$. Hence $Z(D) \subseteq k_0$. The converse inclusion is trivial.

(b) Suppose σ has order s. Then if $\sigma^j = \mathrm{id}$, the integer s divides j. Thus any element $f \in Z(D)$ is of the form $\sum a_i x^{s\cdot i}$. Like in the previous item, we have

$$\sum \sigma(a_i) x^{s\cdot i+1} = \sum x^{s\cdot i+1} a_i = xf = fx = \sum a_i x^{s\cdot i+1},$$

so $a_i = \sigma(a_i)$ for all i and therefore $Z(D) \subseteq k_0((x^s))$. The converse inclusion follows from the observation that if we have $a_0 x^{si} \in k_0((x^s))$, we have

$$(a_0 x^{si})a = a_0 \sigma^{si}(a) x^{si} = a_0 a x^{si} = a(a_0 x^{si})$$

and

$$(a_0 x^{si})x = a_0 x^{si+1} = \sigma(a_0) x^{si+1} = x(a_0 x^{si}).$$

In this case we also obtain the equality $s^2 = \dim_{Z(D)} D < \infty$. □

Example 3.3 (Hilbert)**.** *Let $k = \mathbb{Q}(t)$, σ a k-automorphism that sends $t \mapsto 2t$. Then $D := \mathbb{Q}(t)((x,\sigma))$ is an infinite-dimensional division ring (this was the first ever example).*

There is an alternative view of the case where σ is of finite order. Let $F = k_0((x^s))$ and $K = k((x^s))$. If σ has order s and $C_s = \langle\sigma\rangle$ (a cyclic group of k-automorphisms generated by σ). Then $k_0 = k^{C_s}$,

so k/k_0 is a finite Galois extension[1] and therefore $[k : k_0] = s$. We know that σ extends to an automorphism of K:

$$\sum a_i x^{si} \mapsto \sum \sigma(a_i) x^{si},$$

so $[K : F] = s$, where $F = K^{C_s}$. As a K-vector space

$$D = K \cdot 1 \oplus K \cdot x \oplus \cdots \oplus K \cdot x^{s-1},$$

so $\dim_K D = s$ and $\dim_{Z(G)} D = \dim_K D \cdot \dim_{Z(G)} K = s^2$.

Definition 3.4. Let K/F by a cyclic Galois extension and $s = [K : F]$. Fix $a \in F \setminus \{0\}$ and define the s-dimensional K-vector space

$$D = K1 \oplus Kx \oplus \cdots \oplus Kx^{s-1}.$$

Multiplication in D is determined by $x^s = a$ and $x \cdot b = \sigma(b)x$ for $b \in K$. Then $D = (K/F, \sigma, a)$ is a cyclic algebra. Obviously, $F \subseteq Z(D)$ and $\dim_F D = s^2$.

Example 3.5. *We show that $\mathbb{H}$ is a cyclic algebra. We set $F = \mathbb{R}$, $K = \mathbb{C}$ and σ is a complex conjugation. Now we take $a = -1$, $x = j$ and*

$$D = \mathbb{C} \oplus \mathbb{C}_j = \mathbb{R} \oplus \mathbb{R}_i \oplus \mathbb{R}_j \oplus \mathbb{R}_{ij}.$$

Remark. We have a shortcut to cyclic algebras. If $B := K[t, \sigma]$ is a skew polynomial ring, then

$$(K/F, \sigma, a) = B/(t^s - a).$$

Theorem 3.6.

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

1. *D is a simple F-algebra and $Z(D) = F$.*
2. *$C_D(K) := \{y \in D \mid \forall b \in K : \ by = yb\} = K$.*
3. *K is a maximal subfield of D.*

Proof.

1. Let $(0) \neq I \lhd K$ and pick $0 \neq z \in I$, say
$$z = b_{i_1} x^{i_1} + \cdots + b_{i_r} x^{i_r}, \quad b_j \in K, \quad 0 \leq i_1 < i_2 < \cdots < i_r \leq s - 1.$$
Choose z with the smallest possible number r. We will prove that $r = 1$. If $r > 1$, then $\sigma^{i_1} \neq \sigma^{i_r}$, so there exists a $b \in K$ such that $\sigma^{i_1}(b) \neq \sigma^{i_r}(b)$. Then $\sigma^{i_1}(b)z - zb \in I$ is a nonzero element that has shorter length than r, contradiction. Thus $z = b_{i_1} x^{i_1} \in I$ and since both x^{i_1} and $b_{i_1} \in K \setminus \{0\}$ are invertible, so is z. This means that $I = K$.
2. Clearly, $K \subseteq C_D(K)$. We now need to prove the opposite inclusion. Let $d = \sum_{i=0}^{n-1} b_i x^i \in C_D(K)$, where $b_i \in K$. Then we have
$$\sum b b_i x^i = b \sum b_i x^i = bd = db = \sum \sigma^i(b) b_i x^i.$$
If $b_i \neq 0$, then $\sigma^i(b) = b$, $\forall b$, so $\sigma^i = \mathrm{id}$ and $i = 0$. We have proved that $d = b_0 \in K$.
3. Suppose $L \subseteq D$ is a subfield and $L \supset K$. Then $K \subseteq L \subseteq C_D(K) = K$, so $L = K$. Equipped with all this, we can prove $Z(D) \subseteq F$. If $b \in Z(D)$, then $b \in C_D(K) = K$. From $\sigma(b)x = xb = bx$, we have $\sigma(b) = b$, so $b \in K^{\langle\sigma\rangle} = F$. □

[1] Milne: Fields and Galois theory, theorem 3.10

Example 3.7. *Not every cyclic algebra is a division ring. Say $a = 1$. Then $x^s = 1$, so we can factor*

$$0 = x^s - 1 = (x-1)(1 + x + \cdots + x^{s-1})$$

and both factors are nonzero by construction, so they are zero divisors. Of course, this means that $(K/F, \sigma, 1)$ is not a division ring.

Definition 3.8. Let K/F be a cyclic Galois extension, $s = [K : F]$ and $\langle\sigma\rangle = \mathrm{Aut}(K/F)$. Then we define a norm

$$N_{K/F} : K \to F, \quad a \mapsto a \cdot \sigma(a) \cdot \sigma^2(a) \cdots \sigma^{s-1}(a).$$

Theorem 3.9.

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

Proof. Since $a \in N_{K/F}(K)$, there exists a $d \in K$ such that $N_{K/F}(d) \cdot a = 1$. Set $y := dx$. Then

$$y^s = dx \cdot dx \cdots dx = d\sigma(d)\sigma^2(d) \cdots \sigma^{s-1}(d)x^s = N_{K/F}(d) \cdot a = 1.$$

For all $b \in K$, we have

$$yb = dxb = d\sigma(b)x = \sigma(b)dx = \sigma(b)y.$$

It's enough to prove that $D = (K/F, \sigma, 1) \cong M_s(F)$ since we can take $y = dx$. If $B = K[t, \sigma]$, then

$$D = (K/F, \sigma, 1) \cong B/(t^s - 1).$$

Recall that

$$(t^s - 1) = (1 + t + \cdots + t^{s-1})(t - 1).$$

As a K-module, $B/B(t-1) \cong K$, so it has no K-submodules and therefore also no B-submodules. Therefore, it is a maximal left ideal in B, so we have $(t^s - 1) \subseteq B(t-1) \leq {}_B B$. As a result, $B/(t^s - 1)$ has a simple left module $M = B/B(t-1) \cong K$ (as a left K-module). We know that $\dim_F K = s$, so

$$(K/F, \sigma, 1) \to \mathrm{End}_F(M) = \mathrm{End}_F(F^s) = M_s(F).$$

Since $(K/F, \sigma, 1)$ is simple, the map is injective. But because $\dim_F(K/F, \sigma, 1) = s^2 = \dim_s(F)$, it is also surjective. □

Remark. The converse of this theorem is also true. Furthermore, if s is a prime then $(K/F, \sigma, a)$ is a division ring iff $a \notin N_{K/F}(K)$.

3.2 Tensor products of algebras

All algebras will be over the field k and so is the tensor product. If R, S are k-modules, then so is $R \otimes_k S$. If they are k-algebras, then again $R \otimes_k S$ has a k-algebra structure such that

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

To justify that, notice that $(r, s, r', s') \mapsto rr' \otimes ss'$ is multilinear, so it induces a map $(R \otimes S) \otimes (R \otimes S) \mapsto (R \otimes S)$. Multiplication in $R \otimes S$ is distributive, associative, has a unit element $1 \otimes 1$ and is compatible with a k-module structure. In general, the multiplication in $R \otimes S$ satisfies

$$\left(\sum_i r_i \otimes s_i\right) \cdot \left(\sum_j r'_j \otimes s'_j\right) = \sum_{i,j} r_i r'_j \otimes s_i s'_j.$$

Denote

$$i : R \to R \otimes S, \quad r \mapsto r \otimes 1$$

and

$$j : S \to R \otimes S, \quad s \mapsto 1 \otimes s.$$

If $(e_\alpha)_\alpha$ is a basis for S over k, then every element $x \in R \otimes S$ has a unique expansion

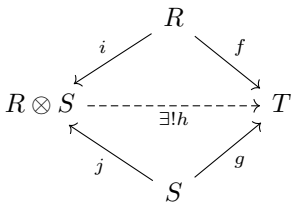
$$x = \sum r_\alpha \otimes e_\alpha = \sum (r_\alpha \otimes 1)(1 \otimes e_\alpha) = \sum i(r_\alpha) j(e_\alpha).$$

Clearly, $R \otimes S$ is an R-module via i. It is free generated with basis $(j(e_\alpha))_\alpha$. In particular, i is injective; in fact, both i and j are injective. Hence we can idenitfy R, S with their images in $R \otimes S$ under i, j. For $r \in R, s \in S$, we have $i(r) \cdot j(s) = j(s) \cdot i(r)$.

Proposition 3.10. *Let k be a field and R, S k-algebras. Then $R \otimes S$ is a k-algebra with the following properties.*

1. *$R \otimes S$ contains R and S as commuting k-subalgebras.*
2. *Any basis $(s_\mu)_\mu$ of S over k is a basis for $R \otimes S$ as a (free) R-module.*
3. *Any basis $(r_\alpha)_\alpha$ of R over k is a basis for $R \otimes S$ as a (free) S-module.*

Proposition 3.11 (Universal property)**.** *Given any k-algebra T and k-algebra homomorphisms $f : R \to T$, $g : S \to T$ such that $f(R)$ and $g(S)$ commute elementwise and $f\big|_k = g\big|_k$, then there exists a unique k-algebra homomorphism $h : R \otimes S \to T$ such that $hi = f$ and $hj = g$.*



Proof. See homeworks. □

3.3 Scalar multiplication and semisimplicity

If R is a k-algebra and K/k is a field extension, then $R_K := K \otimes_k R$ is an extension of scalars. The k-algebra R can be described by giving a basis $(e_i)_i$ over k and prescribing the multiplication of these basis elements:

$$e_i \cdot e_j = \sum_k c_{ijk} e_k,$$

where $c_{ijk} \in k$. Then R_K is the K-algebra with some basis vectors $(e_i)_i$ and their multiplication, given as above (of course, $c_{ijk} \in k \subseteq K$).

Example 3.12 (Complexification)**.** *Given an $\mathbb{R}$-algebra S, we form its complexification $S_\mathbb{C} := \mathbb{C} \otimes_\mathbb{R} S$, where $S_\mathbb{C}$ becomes a $\mathbb{C}$-algebra. If $S = \mathbb{R}$, then $S_\mathbb{C} = \mathbb{C}$. But for $S = \mathbb{H}$, we get a 4-dimensional $\mathbb{C}$-algebra $\mathbb{H} \oplus \mathbb{C}$ which is simple and homeomorphic to $M_2(\mathbb{C})$, as we shall see later.*

Theorem 3.13 (Primitive element**).**

If K/k is a finite separable extension, there exists $c \in K$ such that $K = k(c)$.

Theorem 3.14.

Let L/k be a finite field extension. Then $L_K = K \otimes_k L$ is semisimple for all K/k iff L/k is separable.

Proof. Start with ($\Leftarrow$). By primitive element theorem, there exists $\theta \in L$ such that $L = k(\theta)$. The field L has a k-basis $1, \theta, \cdots, \theta^{n-1}$, where θ satisfies a separable, irreducible polynomial $f \in k[x]$ of degree $n = [L : k]$. That is, $L = k[t]/(f)$. Then L_K has K-basis $1, \theta, \cdots, \theta^{n-1}$ and θ satisfies some polynomial relation $f(\theta) = 0$. So $L_K = K[t]/(f)$. Since f is separable, it factors in K into distinct irreducible polynomials, say $f = f_1 \cdots f_r$ for some $f_i \in F[t]$. By the Chinese remainder theorem:

$$L_K = K[t]/(f) = K[t]/(f_1 \dots f_r) \cong \prod_{j=1}^{r} K[t]/(f_j),$$

so L_K is a direct product of fields and therefore semisimple. Now the converse ($\Rightarrow$). Suppose L is not separable over k. Then there exists $\theta \in L$ that is not separable, meaning its minimal polynomial $f \in k[t]$ is not separable. Hence there exists an extension K/k such that f has repeated factors in K. Then $K[t]/(f) = k(\theta)_K \subseteq L_K$ has nilpotent elements. But that implies that L_K has nilpotent elements, say $a \neq 0$, and is commutative. Since $(0) \neq (a) \lhd L_K$ is nil, $(a) \subseteq \mathrm{rad}(L_K) \neq (0)$, L_K cannot be semisimple. □

Corollary 3.15. *The tensor product of two field extensions over K is semisimple provided one of the two factors is finite and separable over k.*

3.4 Tensor products, (semi)simplicity

Assume that all algebras are over some fixed field k.

Definition 3.16. Given an algebra S, its center is $Z(S) = \{y \in S \mid \forall x \in S : xy = yx\}$. We call S central over k if $k = Z(S)$ and central simple if S is simple and central.

Example 3.17.
1. *The quaternion ring $\mathbb{H}$ is a central simple $\mathbb{R}$-algebra.*
2. *If S is simple, then S is a central simple $Z(S)$-algebra.*
3. *A matrix ring $M_n(k)$ is a central simple algebra over k.*
4. *The complex field $\mathbb{C}$ is a central simple algebra over $\mathbb{C}$, but not over $\mathbb{R}$. No proper field extension K/k is central over k.*

Theorem 3.18.

Let S be a central simple algebra and R any algebra.

1. *Every two-sided ideal of $R \otimes S$ has the form $I \otimes S$ for some $I \lhd R$. In particular, if R is simple, then so is $R \otimes S$.*
2. *We have equality $Z(R \otimes S) = Z(R)$. In particular, taking $R = K$ a field, $S_K = K \otimes S$ is a central simple algebra over K.*

Corollary 3.19. *If R, S are central simple algebra, then $R \otimes S$ is central simple algebra.*

Lemma 3.20. *Let S, R be as in the theorem. If $(0) \neq J \lhd R \otimes S$, then $J \cap R \neq (0)$.*

Proof. Choose $(0) \neq x \in J$ so that $x = \sum_{j=1}^{l} r_i \otimes s_i$ with $r_i \in R$ and $s_i \in S$ has minimal l. Then $(r_i)_i$ are k-linearly independent and the same for $(s_i)_i$. In particular, $s_1 \neq 0$. Thus $\langle s_1 \rangle = S$. Since $1 \in (s_1)$, we have $1 = \sum_{j=1}^{m} x_j s_1 y_j$ for some $x_j, y_j \in S$. Set

$$\begin{aligned} x' &= \sum_{j=1}^{m} (1 \otimes x_j) x (1 \otimes y_j) \\ &= \sum_{j=1}^{m} \sum_{i=1}^{l} (1 \otimes x_j)(r_i \otimes s_i)(1 \otimes y_j) \\ &= \sum_{j=1}^{m} \sum_{i=1}^{l} r_i \otimes x_j s_i y_j \\ &= \sum_{i=1}^{l} r_i \otimes \sum_{j=1}^{m} x_j s_i y_j \\ &= \sum_{i=1}^{l} r_i \otimes s_i'. \end{aligned}$$

Obviously, $x' \in J$. Since r_i are linearly independent and $s_1' = 1$, $x' \neq 0$. For any $s \in S$, we have

$$\begin{aligned} J \ni (1 \otimes s)x' - x'(1 \otimes s) &= \sum_{r=1}^{l} r_i \otimes s s_i' - \sum_{r=1}^{l} r_i \otimes s_i' s \\ &= \sum_{r=1}^{l} r_i \otimes (s s_i' - s_i' s) \\ &= \sum_{r=2}^{l} r_i \otimes (s s_i' - s_i' s). \end{aligned}$$

By minimality of l, this element is 0, so $s s_i' = s_i' s$ for each index $2 \leq i \leq l$. Since this holds for all $s \in S$, we get $s_i' \in Z(S) = k$. Finally, we can rewrite

$$x' = \sum_{i=1}^{l} r_i \otimes s_i' = \left(\sum_{i=1}^{l} r_i s_i' \right) \otimes 1 \in R,$$

so $0 \neq x' \in J \cap R$. □

Proof of theorem. 1. Let $J \lhd R \otimes S$, $I = J \cap R$. Consider the map

$$\varphi : R \otimes S \to (R/I) \otimes S, \quad r \otimes s \mapsto (r + I) \otimes s.$$

First we prove that $\ker \varphi = I \otimes S$. We know that k-linearly independent elements of R stay S-linearly independent in $R \otimes S$. Pick a basis $(x_i)_i$ for $I \subseteq R$, extend to a basis $(x_i, y_j)_{i,j}$ for R. Then $(y_j + I)_j$ is a basis for R/I and

$$\sum x_i \otimes a_i + \sum y_j \otimes b_j \in \ker \varphi \Leftrightarrow b_j = 0, \quad \forall j.$$

We use this fact in the following way:

$$R \otimes S \xrightarrow{\pi} (R \otimes S)/(I \otimes S) \underset{\cong}{\xrightarrow{\overline{\varphi}}} (R/I) \otimes S.$$

Clearly, $I \otimes S \subseteq J$. If $I \otimes S \subsetneq J$, then the image of the above map is nonzero, so $(\overline{\varphi}\pi)(J) \cap (R/I \otimes S) \neq (0)$. By previous lemma, $(\overline{\varphi}\pi)(J) \cap (R/I) \neq (0)$. Pulling back (since $\overline{\varphi}$ is an

isomorphism), this tells us that

$$J/(I \otimes S) \cap (R \otimes 1)/(I \otimes S) \neq (0).$$

This is a contradiction by definition of I.

2. Let $x = \sum r_i \otimes s_i \in Z(R \otimes S)$. Without loss of generality, $(r_i)_i$ are k-linearly independent. For $s \in S$, we have
$$0 = (1 \otimes s)x - x(1 \otimes s) = \sum r_i \otimes (ss_i - s_i s),$$
so by independence of r_i we can conclude $ss_i - s_i s = 0$ for all indexes i. This implies that $s_i \in Z(S) = k$, hence
$$x = \sum r_i \otimes s_i = \underbrace{\sum r_i s_i}_{r} \otimes 1 =: r \otimes 1.$$
For any $y \in R$, we have
$$0 = (y \otimes 1)x - x(y \otimes 1) = (yr - ry) \otimes 1,$$
so $r \in Z(R)$. □

Suppose S is a simple k-algebra with center C. Then C is a field, so S is a central simple algebra over C. We prove that
$$C \cong \mathrm{End}_{S \otimes S^{\mathrm{op}}}(S),$$
where $S \otimes S^{\mathrm{op}}$ acts on S by
$$(s_1 \otimes s_2^{\mathrm{op}}) \cdot s = s_1 s s_2.$$
Define a map
$$\Phi : C \to \mathrm{End}_{S \otimes S^{\mathrm{op}}}(S), \quad c \mapsto (s \mapsto c \cdot s).$$
Firstly, we need to check whether this is well defined. This is fairly simple:
$$\begin{aligned} \Phi(c)((s_1 \otimes s_2^{\mathrm{op}}) \cdot s) &= \Phi(c)(s_1 s s_2) = c \cdot s_1 s s_2 \\ &= s_1 c s s_2 = (s_1 \otimes s_2^{\mathrm{op}}) \cdot (cs) \\ &= (s_1 \otimes s_2^{\mathrm{op}}) \cdot (\Phi(c)(s)). \end{aligned}$$
It is easy to verify Φ is a homomorphism. We prove that it is an isomorphism. Clearly, it is injective: $\Phi(c) = \Phi(d)$ implies
$$c = \Phi(c)(1) = \Phi(d)(1) = d.$$
Every $\varphi \in \mathrm{End}_{S \otimes S^{\mathrm{op}}}$ is determined by $\varphi(1) = x$: we have to prove that $x \in C$. This follows easily:
$$\begin{aligned} sx &= (s \otimes 1) \cdot x = (s \otimes 1)\varphi(1) \\ &= \varphi((s \otimes 1) \cdot 1) = \varphi(s) \\ &= \varphi((1 \otimes s^{\mathrm{op}}) \cdot 1) = (1 \otimes s^{\mathrm{op}}) \cdot \varphi(1) \\ &= (1 \otimes s^{\mathrm{op}}) \cdot x = xs, \end{aligned}$$
thus proving our assertion.

Remark. In general, suppose $A \supseteq B$ are algebras and $C_A(B) := \{a \in A |\ \forall b \in B :\ ab = ba\}$. Then $A \otimes B^{\mathrm{op}}$ acts on A and $C_A(B)^{\mathrm{op}} \cong \mathrm{End}_{A \otimes B^{\mathrm{op}}}(A)$.

Let R, S be rings. If $R \times S$ is a K-algebra, so are R and S. Also, if $M_n(R)$ is a K-algebra, so is R. This allows us to generalize Wedderburn theory to algebras.

Proposition 3.21 (Wedderburn for K-algebras)**.** *Let A be a semi-simple k-algebra. There are division algebras $D_1, \ldots, D_n$ and $m_1, \ldots, m_n \in \mathbb{N}$ such that*
$$A \cong M_{m_1}(D_1) \times \cdots \times M_{m_n}(D_n).$$

The following lemma, repurposed for k-algebras, will be particularly useful.

Lemma 3.22 (Wedderburn)**.** *A k-algebra A is simple left artinian iff it is isomorphic to $M_n(D)$ for some $n > 0$ and a division k-algebra $D \cong \mathrm{End}_A^{\mathrm{op}}(S)$, where S is a simple left A-module.*

Remark. This S is unique up to isomorphism (see Pierre Antoine Grillet, proposition IX.1.8).

We will often use this lemma in conjunction with the fact that a finite dimensional k-algebra is artinian. Also, note that $A \cong M_n(D) \cong \mathrm{End}_{D^{\mathrm{op}}}(S)$.

Remark. The center of $M_n(D)$ is isomorphic to the center of the division ring D.

Definition 3.23. Let S be a finite-dimensional semisimple algebra over k. If $C = Z(S)$, then $C = C_1 \times \cdots \times C_m$ for some fields C_j. S is called separable if each $C_j\,/k$ is separable.

Remark. If $R = R_1 \times R_2$, then $R \otimes S = (R_1 \otimes S) \times (R_2 \otimes S)$. Similarly, if $R = \prod_{i=1}^n R_i$, then $R \otimes S = \prod_{i=1}^n R_i \otimes S$.

Remark. For a simple k-algebra S with center K and a k-algebra R, we have

$$R \otimes_k S = \underbrace{(R \otimes_k C)}_{R_C} \otimes_C S.$$

Indeed, $C \otimes_C S$ is isomorphic to S as a C-algebra, so it is isomorphic as a k-algebra.

Proposition 3.24. *If S is separable, then S_K is semisimple for all field extensions $K\,/k$.*

Proof. By one of the above remarks, we can assume WLOG that S is simple with separable center C. Then

$$K \otimes_k S = (K \otimes_k C) \otimes_C S \cong (\prod_i R_i) \otimes_C S = \prod_i (R_i \otimes_C S),$$

where R_i's are fields from the proof of theorem 3.14. □

Proposition 3.25. *If R, S are finite-dimensional semisimple algebras and at least one of them is separable, then $R \otimes S$ is semisimple.*

Proof. WLOG R is separable and R, S simple. Let $C := Z(S)$. Then

$$R \otimes_k S = (R \otimes_k C) \otimes_C S = (\prod R_i) \otimes_C S = \prod R_i \otimes_C S$$

is a direct product of semisimple algebras, so it is semisimple. □

3.5 Applications of tensor products

Theorem 3.26.

If D is a finite-dimensional division algebra over its center k, then $[D : k]$ must be a square.

Proof. By assumption, $[D : k] = [D_{\overline{k}} : \overline{k}] < \infty$. Then $D_{\overline{k}} = \overline{k} \otimes D$ is simple and artinian (as a finite-dimensional $\overline{k}$-algebra), so it is semisimple. By Wedderburn, $D_{\overline{k}} \cong M_n(E)$ for some finite-dimensional division algebra E over $\overline{k}$. But since $\overline{k}$ is algebraic closure, $E = \overline{k}$ and $D_{\overline{k}} \cong M_n(\overline{k})$, so $[D_{\overline{k}} : \overline{k}] = n^2$. □

Corollary 3.27. *If A is a simple algebra and $[A : Z(A)] < \infty$, then $[A : Z(A)]$ is a square.*

Proof. By Wedderburn, $A \cong M_n(D)$ for some division algebra D over $Z(A)$, where $[D : Z(A)] < \infty$. Then

$$[A : Z(A)] = [A : D][D : Z(A)] = n^2[D : Z(D)] = n^2m^2$$

by the previous theorem. □

Definition 3.28. The degree of a finite-dimensional central simple algebra S over k is $\deg S = \sqrt{[S : k]}$.

Proposition 3.29. *Let R be a finite-dimensional central simple algebra. Then $R \otimes R^{\mathrm{op}} \cong M_n(k)$, where $n = [R : k]$.*

Proof. Let

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

Then $A \cong R$ and $B \cong R^{\mathrm{op}}$. Elements od A and B commute because multiplication in R is associative. By universal property of tensor products,

$$\Omega : R \otimes R^{\mathrm{op}} \to \mathrm{End}_k(R), \quad r \otimes s \mapsto L_r \circ T_s$$

is a homomorphism. Since R, R^{op} are csa's over k, $R \otimes R^{\mathrm{op}}$ is simple and therefore Ω is injective. Furthermore,

$$\dim_k(R \otimes R^{\mathrm{op}}) = \dim_k(R)^2 = \dim_k(\mathrm{End}_k(R)),$$

so Ω has to be surjective and Ω is an isomorphism. □

Example 3.30. *We have $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{\mathrm{op}} \cong M_4(\mathbb{R})$ and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{H}_{\mathbb{C}} \cong M_2(\mathbb{C})$. We can show that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$. We notice that we have an involution*

$$\sigma : \mathbb{H} \to \mathbb{H}, \quad \sigma(a + bi + cj + dk) = a - bi - cj - dk$$

which is also $\mathbb{R}$-linear. Clearly, $\sigma^2 = \mathrm{id}$ and $\sigma(xy) = \sigma(x)\sigma(y)$. But any ring with R with involution is isomorphic to R^{op}, so

$$\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{\mathrm{op}} \cong M_4(\mathbb{R}).$$

3.6 Skolem-Noether theorem

Lemma 3.31. *Let R be a finitely dimensional simple k-algebra. If M_1, M_2 are R-modules that are finitely-dimensional over k with $\dim_k M_1 = \dim_k M_2$, then $M_1 \cong M_2$.*

Proof. We know that R is simple and artinian. By Wedderburn, there exists a unique simple R-module M. Thus $M_j \cong M^{\alpha_j} \in \mathbb{N}$. Hence $\dim M_j = \alpha_j \dim M$, so from $\dim M_1 = \dim M_2$ we deduce $\alpha_1 = \alpha_2$. So $M_1 \cong M^{\alpha_1} = M^{\alpha_2} \cong M_2$. □

Theorem 3.32 (Noether-Skolem)**.**

Let S be a finitely-dimensional central simple algebra over k and let R be a simple k-algebra. If $f, g : R \to S$ are homomorphisms, then there exist an inner automorphism $\alpha : S \to S$, $\alpha(x) = z^{-1}xz$ such that $\alpha f = g$. Equivalently, if R_1, R_2 are simple subalgebras of S, then for every homomorphism

$f : R_1 \to R_2$ there exists an inner automorphism $\alpha : S \to S$ such that $\alpha\big|_{R_1} = f$. In particular, every automorphism of S is inner.

Remark. It is key that S is a central simple algebra.

- If S is a proper field extension of k, then S will typically have many automorphisms, but none of them would be inner (S is commutative).
- Complex conjugation on $\mathbb{C}$ is a non-inner $\mathbb{R}$-algebra automorphism of $\mathbb{C}$.

Proof. Since S is artinian and simple, Wedderburn tells us that $S \cong \mathrm{End}_D(V) = M_n(D^{\mathrm{op}})$, where D is a division algebra over k and V is a finitely-dimensional D-vector space. The maps f, g induce R-module structures in V by multiplication

$$r \cdot v = f(r) \cdot v, \quad r \cdot v = g(r) \cdot v.$$

Since S is a D-linear map on V, those two actions commute with actions of D, so V becomes a $\mathbb{R} \otimes D$-module in two different ways. We know that $R \otimes D$ is artinian and and simple, so by the previous lemma those two module structures on V are isomorphic. There exists an abelian group isomorphism $h : V \to V$ such that

$$h(f(r)v) = g(r)h(v), \quad h(dv) = dh(v).$$

This implies that $h \in \mathrm{End}_D(V) = S$ and $h \cdot f(r) = g(r)h$, which is exactly what we wanted. □

Corollary 3.33. *If $\alpha : M_n(k) \to M_n(k)$ is an automorphism, then there exists $P \in GL_n(k)$ such that $\alpha(x) = P^{-1}xP$ for some $x \in M_n(k)$.*

3.7 The (double) centralizer theorem

Definition 3.34. If R is an algebra and $S \subseteq R$, the centralizer of S in R is

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

This is a subalgebra of R.

Remark.
1. If S is a central simple algebra, then $C_S(C_S(S)) = C_S(k) = S$, then S is its own double centralizer.
2. It's obvious that for a general algebra $R \subseteq C_R(C_R(R))$.

If S is a finite-dimensional simple algebra, then by Wedderburn $S \cong M_n(D)$ for some $n \in \mathbb{N}$ and some division ring D. We use the notation $S \sim D$. Observe that D is unique up to isomorphism: S has a unique (up to isomorphism) simple module, say V and $D^{\mathrm{op}} = \mathrm{End}_S(V)$.

Theorem 3.35 (Centralizer theorem)**.**

Let S be a finitely-dimensional central simple algebra over k and R a simple subalgebra of S. Then:

1. *$C_S(R)$ is simple;*
2. *if $S \sim D_1$ and $R \otimes D_1^{\mathrm{op}} \sim D_2$, then $C(R) \sim D_2^{\mathrm{op}}$;*
3. *$[S : k] = [R : k][C_S(R) : k]$;*

4. $C_S(C_S(R)) = R$.

Proof. Apply Wedderburn to S; then we have

$$S \overset{\theta}{\cong} \mathrm{End}_D(V) \cong M_n(D^{\mathrm{op}})$$

where D is a division algebra and V is a n-dimensional vector space. Then V is a $(R \otimes D)$-module. Since θ is an isomorphism, we see that $a \in C_S(R)$ iff $ab = ba$ for all $b \in B$ iff $\theta(a)\theta(b) = \theta(b)\theta(a)$ for all $b \in B$ iff θ is a $R \otimes D$-module endomorphism of V. This bijection induces the isomorphism $C_S(R) = \mathrm{End}_{R\otimes D}(V)$.

1. Since $R \otimes D$ is simple, we get $R \otimes D \cong \mathrm{End}_E(W) = M_d(E^{\mathrm{op}})$, where W is the unique simple $(R\otimes D)$-module and $E = \mathrm{End}_{R\otimes D}(W)$. Since $R\otimes D$ is semisimple and V is a $(R\otimes D)$-module, it is semisimple, so ${}_{R\otimes D}V = W^m$ for some $m \in \mathbb{N}$. Then

$$\begin{aligned} C_S(R) &= \mathrm{End}_{R\otimes D}(V) \\ &\cong \mathrm{End}_{R\otimes D}(W^m) \\ &\cong M_m(\mathrm{End}_{R\otimes D}(W)) = M_m(E) \end{aligned}$$

   is simple.
2. Since $S \sim D^{\mathrm{op}} = D_1$, $R \otimes D_1^{\mathrm{op}} = R \otimes D \sim E^{\mathrm{op}} = D_2$. From there we get $C_S(R) \sim E = D_2^{\mathrm{op}}$.
3. From $C(R) \cong M_m(E)$ it follows that $[C(R) : k] = m^2[E : K]$. But $V \cong W^m$, so $[V : k] = m[W : k] = m[W : E][E : k]$. So

$$\begin{aligned} [C_S(R) : k] &= m^2 \frac{[E : k]^2}{[E : k]} \\ &= \frac{[V : k]^2}{[W : E]^2[E : k]}. \end{aligned}$$

   Now the following calculation:

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

   so

$$[C_S(R) : k] = \frac{[V : k]^2}{[R : k][D : k]}$$

   and

$$[R : k][C_S(R) : k] = \frac{[V : k]^2}{[D : k]} = \frac{[V : D]^2[D : k]^2}{[D : k]} = [V : D]^2[D : k] = [S : k],$$

   concluding our proof.
4. We have

$$[R : k][C_S(R) : k] = [S : k] = [C_S(R) : k][C_S(C_S(R)) : k],$$

   so $[R : k] = [C_S(C_S(R)) : k]$ and $R = C_S(C_S(R))$. □

Corollary 3.36. *If R is a central simple algebra contained in a finite dimensional central simple algebra S, then $S \cong R \otimes C_S(R)$.*

Proof. Consider the algebra homomorphism

$$\Psi : R \otimes C_S(R) \to S, \quad r \otimes r' \mapsto rr'.$$

Since $R \otimes C_S(R)$ is simple, Ψ is injective. By the centralizer theorem,

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

so Ψ is also surjective. □

Definition 3.37. Let D be a division algebra over k. A field $K \supseteq k$ such that

$$D_K = K \otimes D \cong M_n(K)$$

(as K-algebras) is called a splitting field for D.

Remark.
1. Let $\overline{k}$ be the algebraic closure of k. Then $\overline{k}$ is a splitting field of any finitely dimensional algebra D over k.
2. If K splits D and K'/K, then K' also splits D:

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

Proposition 3.38. *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, K is a splitting field for D.*

Proof. For $\alpha \in C_D(K) \setminus K$, $K(\alpha)$ would be a proper extension of K. This means that $C_D(K) \subseteq K$, therefore $C(K) = K$. By the third item in the double centralizer theorem,

$$n^2 = [D : k] = [K : k][C_D(K) : k] = [K : k]^2.$$

Now onto the second statement. We know that D is a simple $D \otimes K$-module. So

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

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

3.8 Theorems for division rings

Theorem 3.39 (Little Wedderburn)**.**

Every finite division ring is a field.

Proof. Let D be a finite division ring and $k = Z(D)$ a field. Let K be a maximal subfield of D, so $k \subseteq K \subseteq D$. if $K = D$, we are done. Assume $K \subsetneq D$. Since $[D : k] = n^2$ for some $n \in \mathbb{N}$, we have $[K : k] = n$ for some $n \in \mathbb{N}$ by the above proposition. If $|k| = q = p^m$, then $|K| = q^n$. We already know that any two subfields of D of q^n are isomorphic, hence they are conjugates by Skolem-Noether. Every element of D is contained in a maximal subfield, so $D = \bigcup_{x\in D^{-1}} xKx^{-1}$ and $D^{-1} = \bigcup_{x\in D^{-1}} xK^{-1}x^{-1}$. Now we claim that if $H \lneqq G$ are finite groups, then $\bigcup_{g\in G} gHg^{-1} \subsetneq G$. Indeed, if $|H| = k$ and $[G : H] = n$, then $|G| = nk$ and there are at most n conjugates of H in G. But each of these contains the unit element, so

$$|\bigcup_{g\in G} gHg^{-1}| \leq n(k-1) + 1 < nk = |G|.$$

This concludes our proof. □

Theorem 3.40 (Frobenius)**.**

If D is a division algebra with $\mathbb{R} \subseteq Z(D)$ and $[D : \mathbb{R}] < \infty$, then $D \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$.

Proof. Without loss of generality, assume $[D:\mathbb{R}] \geq 2$. For any $\alpha \in D \setminus \mathbb{R}$, $\mathbb{R}(\alpha)$ is a proper algebraic field extension of $\mathbb{R}$, so $\mathbb{R}(\alpha) \cong \mathbb{C}$ (since $\mathbb{C}$ is algebraically closed). Fix a copy of $\mathbb{C}$ in D. Then

$$D^+ = \{d \in D \mid di = id\} \leq_{\mathbb{R}} D, \quad D^- = \{d \in D \mid di = -id\} \leq_{\mathbb{R}} D.$$

Clearly, $D^+ \cap D^- = \{0\}$. We prove that $D = D^+ \oplus D^-$. Now for any $a \in D$, we define

$$a^+ = ai + ia \in D^+, \quad a^- = ia - ai \in D^-$$

and

$$a = (2i)^{-1}(a^+ + a^-) \in D^+ + D^-.$$

For all $d^+ \in D^+$, $\mathbb{C}(d^+)$ is an algebraic extension of $\mathbb{C}$, so $\mathbb{C}(d^+) = \mathbb{C}$ and $D^+ = \mathbb{C}$. If $D^- = (0)$, then $D = D^+ = \mathbb{C}$. Take $z \in D^- \setminus \{0\}$ and consider a map

$$\mu : D^- \to D^+, \quad x \mapsto xz.$$

This map is injective and $\mathbb{C}$-linear, which implies that

$$0 \neq \dim_{\mathbb{C}} D^- \leq \dim_{\mathbb{C}} D^+ = 1,$$

so we have $\dim_{\mathbb{R}} D^- = 2 \dim_{\mathbb{C}} D^- = 2$. Finally, we have $\dim_{\mathbb{R}} D = 4$. Since z is algebraic over $\mathbb{R}$ and $\dim_{\mathbb{R}} D^- = 2$, we have $z^2 \in \mathbb{R} + \mathbb{R}z$, but also $z^2 \in D^+ = \mathbb{C}$. This means that $z^2 \in (\mathbb{R} + \mathbb{R}z) \cap \mathbb{C} = \mathbb{R}$. If $z^2 = r^2 \in \mathbb{R}_{\geq 0}$, then $(z-r)(z+r) = 0$ and $z = \pm r \in \mathbb{R}$, which implies $z = r = 0$ since $\mathbb{R} \cap D^- = (0)$, which is a contradiction. So $z^2 = -r^2$ for some $r \in \mathbb{R}$. Define $j := \frac{z}{r}$. Then $i^2 = j^2 = -1$ and $ij = -ji$ and therefore

$$D = \mathbb{C} \oplus \mathbb{C}j = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R} \underbrace{ij}_{k}.$$

□

3.9 Application of primitive rings to Jacobson-Herstein theorem

Theorem 3.41 (Jacobson-Herstein for division rings)**.**

Suppose D is a division ring. If $\forall a, b \in D$ there exists a $n > 1$ such that

$$(ab - ba)^n = ab - ba,$$

then D is a field.

Proposition 3.42. *Let D be a division ring. If $y \in D$ commutes with all commutators, then $y \in Z(D)$.*

Proof. Assume $y \notin Z(D)$. We have the $x \in D$ such that $[x, y] \neq 0$. Notice that we have

$$[x, xy] = x^2y - xyx = x(xy - yx) = x[x, y].$$

By assumption, y commutes with $[x, y]$ and $[x, xy]$, so it commutes with $[x, xy]^{-1}[x, y]^{-1} = x$. □

Corollary 3.43. *If all commutators in a division ring D are central, then D is a field.*

Proposition 3.44. *Let D be a division ring and $K \subseteq D$ a finite subring. Then K is a field.*

Proof. Pick $0 \neq a \in K$ and consider

$$L_a : K \to K, \quad x \mapsto ax.$$

Then L_a is injective, since $ax = ay$ implies $x = y$. Since K is finite, L_a is also bijective and K is a division ring. By little Wedderburn, it is also a field. □

Lemma 3.45. *If F is a field and $G \leq F^{-1}$ is a finite subgroup, then G is cyclic.*

Proof. Let $G = \bigoplus_i \mathbb{Z}/n_i\mathbb{Z}$ and $n = \operatorname{lcm}(n_i) \leq \prod n_i$. Then $x^n = 1$ for all $x \in G$. The equation $x^n - 1 = 0$ has at most n solutions in F, so

$$n \leq \prod n_i = |G| \leq n$$

and therefore $n = \operatorname{lcm}(n_i) = \prod n_i$, so $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Example 3.46. *The quaternion field includes the quaternion group:*

$$\mathbb{H} \geq \{\pm 1, \pm i, \pm j, \pm k\},$$

which is finite but not cyclic.

Corollary 3.47. *Let D be a division ring with $\operatorname{char} D = p > 0$. Then any finite subgroup $G \leq D^{-1}$ is cyclic.*

Proof. Let $F := \mathbb{F}_p \subseteq D$ be the prime subfield. Form a finite subring

$$K := \{\sum_i \alpha_i g_i \mid \alpha_i \in F,\ g_i \in G\} \subseteq D.$$

By the previous proposition, K is a field, and by the previous lemma $G \leq K^{-1}$ is cyclic. □

Lemma 3.48. *Let D be a division ring with $\operatorname{char} D = p > 0$. Suppose $a \in D$ is non-central and torsion. Then $\exists y \in D^{-1}$ such that $yay^{-1} = a^i \neq a$ for some $i \in \mathbb{N}$. Then y can be chosen to be a commutator.*

Proof. Let $\mathbb{F}_p \subseteq D$ be a prime subfield, $K = \mathbb{F}_p[x]$. Since a is torsion, K is a finite field. Then $|K| = p^n$ and in particular $a^{p^n} = a$. Now we define (this is called an inner derivation) a map

$$\delta_a : D \to D, \quad r \mapsto [a, r] = ar - ra.$$

Since $a \notin Z(D)$, this is not a zero map, however $\delta_a\big|_K = 0$ since K is a field. This implies that $\delta_a : D \to D$ is K-linear, so $\delta_a \in \operatorname{End}_K(D)$. Now we prove that δ_a has an eigenvector $\delta_a = L_a - R_a$, where $L_a : D \to D$ and $R_a : D \to D$ are left and right multiplication maps. Since these two maps commute, we have

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

But since $a^{p^n} = a$, we get $\delta_a^{p^n} = \delta_a$. Now a polynomial $t^{p^n} - t \in K[t]$ can be split into

$$t^{p^n} - t = \prod_{b \in K^{-1}} (t - b)t,$$

so

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

Since $\delta_a \neq 0$ and monomorphisms are left-cancellative, there exists a $b \in K^{-1}$ such that $\delta_a - b$ is not injective. There $\exists x \in D^{-1}$ such that $(\delta_a - b)(x) = 0$. So

$$\delta_a(x) = [a, x] = ax - xa = ba$$

and $xax^{-1} = a - b \in K \setminus \{a\}$. In the cyclic group K^{-1}, a and xax^{-1} have the same order, so they generate the same subgroup. In particular, there exists an $i \in \mathbb{N}$ such that $xax^{-1} = a^i \neq a$. Instead of x, let's use $y = \delta_a(x) = [a, x] \neq 0$. then

$$\begin{aligned} y \cdot a &= axa - xaa \\ &= aa^i x - a^i xa \\ &= a^i(ax - xa) = a^i y. \end{aligned}$$

□

Proof of Jacobson-Herstein for division rings. Suppose $D \neq Z(D)$. Then there exist $b_1, b_2 \in D$ such that

$$a = [b_1, b_2] \notin Z(D).$$

For each $c \in Z(D)$, we have

$$ca = c(b_2b_1 - b_2b_1) = cb_1b_2 - b_2cb_1 = [cb_1, b_2].$$

By assumption, there exists a $k \geq 1$ such that

$$1 = a^k = (ca)^k = c^k a^k = c^k,$$

which implies $\operatorname{char} D = p > 0$ (since every element of a field $Z(D)$ is a root of unity). By previous lemma, there exists a commutator $y \in D^{-1}$ such that $yay^{-1} = a^i \neq a$ for some $i \in \mathbb{N}$. Then again by assumption, y is torsion. The product of the groups $\langle a \rangle \langle y \rangle$ is finite since $\langle a \rangle$, $\langle y \rangle$ are finite and y normalizes $\langle a \rangle$. By an earlier corollary this group must be cyclic, thus abelian, which contradicts $yay^{-1} = a^i$. □

4 Brauer group

Our goal is to classify all finite dimensional central simple algebras over a given field k. Equivalently (by Wedderburn), all finite dimensional division algebras over k. We have already done this for:

- finite fields k: $M_n(k)$ for $n \in \mathbb{N}$.
- algebraically closed fields k: again $M_n(k)$ for $n \in \mathbb{N}$.
- $k = \mathbb{R}$: by Frobenius, $M_n(\mathbb{R})$ and $M_n(\mathbb{H})$ for $n \in \mathbb{N}$.

4.1 An equivalence relation on central simple algebras

Definition 4.1. Let S, T be finite-dimensional csa over k. We say that S and T are similar, $S \sim T$, if any one of the following equivalent conditions hold.

1. If $S \cong M_n(D)$ and $T \cong M_m(E)$ for division rings D, E, then $D \cong E$.
2. There exist $m, n \in \mathbb{N}$ such that $S \otimes_k M_m(k) \cong T \otimes M_n(k)$.
3. There exist $m, n \in \mathbb{N}$ such that $M_m(S) \cong M_n(T)$.
4. If M is the unique simple S-module and N is the unique simple T-module, then $\operatorname{End}_S(M) \cong \operatorname{End}_T(N)$.

Remark. Tension product of csa's is a csa. However, a tensor product of central division algebras is not

necessarily a division algebra:

$$\mathbb{H} \otimes \mathbb{H} \cong M_4(\mathbb{R}).$$

4.2 Definition of Brauer groups

Definition 4.2. Let k be a field. The Brauer group of k $\mathrm{Br}(k)$ is the set of equivalence classes of finite-dimensional csa over k with regards to similarity defined before. The group operation is induced by $\otimes$, the equivalence class of k is the identity element:

$$[S] \cdot [T] = [S \otimes T], \quad [k] = 1 \in \mathrm{Br}(k).$$

So far, we have not shown that $\mathrm{Br}(k)$ is a group. In fact, we need to check whether the multiplication is even well-defined.

Remark.

1. The brauer group is trivial iff k is the only central division algebra over k (for example if k is a finite field).
2. $[M_n(k)] = [k] = 1 \in \mathrm{Br}(k)$.
3. If A, B are csa over k of finite dimension, then

$$A \cong B \Leftrightarrow [A] = [B] \in \mathrm{Br}(k),\ [A : k] = [B : k].$$

Lemma 4.3. *1. $M_n(R) \cong R \otimes_k M_n(k)$ for every k-algebra R.*
2. $M_m(k) \otimes M_n(k) \cong M_{mn}(k)$.
3. $(R \otimes_k S) \otimes_k K \cong (R \otimes_k K) \otimes_K (S \otimes_k K)$ for k-algebras R, S and a field extension K.

Proof.

1. We have natural inclusions (k-algebra homomorphisms) $R \hookrightarrow M_n(R)$ and $M_n(k) \hookrightarrow M_n(R)$ whose images commute in $M_n(R)$, so there exists a ring homomorphism $R \otimes_k M_n(k) \to M_n(R)$. This map sends an element of R-basis $1 \otimes E_{ij}$ to an element of R-basis E_{ij}, so it is an isomorphism of R-algebras.
2. This item is a direct corollary of the previous one:

$$M_m(k) \otimes M_n(k) \cong M_n(M_m(k)) \cong M_{mn}(k).$$

3. See homeworks. □

Lemma 4.4. *If $S_1 \sim S_2$ and $T_1 \sim T_2$, the $S_1 \otimes T_1 \sim S_2 \otimes T_2$.*

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

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

□

Theorem 4.5.

Brauer group is an abelian group.

Proof. If S, T are central simple algebras over k, then $S \otimes T$ is a central simple algebra over k, so by previous lemma the operation $[S] \cdot [T] = [S \cdot T]$ is well-defined. This multiplication is associative because $\otimes$ is associative. Also, $[k] = [M_n(k)] = 1 \in \mathrm{Br}(k)$, since $S \otimes_k k \cong S$. We have proved before that $S \otimes S^{\mathrm{op}} = M_n(k)$, so

$$[S][S^{\mathrm{op}}] = [S \otimes T] = [k] = 1 \in \mathrm{Br}(k)$$

and we get $[S]^{-1} = [S^{\mathrm{op}}]$. Finally, $\mathrm{Br}(k)$ is abelian since $\otimes$ is abelian. □

Example 4.6.
- *By little Wedderburn,* $\mathrm{Br}(\mathbb{F}_q) = 1$ *for any* $q = p^n$*. Furthermore,* $\mathrm{Br}(k) = 1$ *even for every algebraic extension* k *of a finite field (stated without proof).*
- $\mathrm{Br}(k) = 1$ *for algebraically closed* k*.*
- $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}_2$*, generated by* $[\mathbb{H}]$*.*

Remark. A field K is C_1 if every homogenous polynomial $f \in K[x_1, \ldots, x_n]$ of degree $\leq n$ has a nontrivial zero in K. Examples of C_1 fields are finite fields, ACF's and $\mathbb{C}(t)$ (Tsen's theorem). Brauer group of any C_1 field is trivial.

Let's sketch the proof of the Brauer group of $\mathbb{Q}$. An absolute value of the field K is a map $|\cdot| : K \to \mathbb{R}$ that satisfies:

1. $|x| \geq 0, \forall x \in K$;
2. $|x| = 0 \Leftrightarrow x = 0$;
3. $|xy| = |x||y|$;
4. $|x + y| \leq |x| + |y|$.

By Ostrowski's theorem, the only absolute values on $\mathbb{Q}$ are the regular absolute value and the p-adic absolute values. The completion of $\mathbb{Q}$ for a regular absolute value is $\mathbb{R}$, however the completion of $\mathbb{Q}$ for a p-adic absolute value is the set of elements of the form

$$\sum_{i=k}^{\infty} a_i p^i, \quad k \in \mathbb{Z}, \quad a_i \in \{0, 1, \ldots, p-1\}.$$

(DOPOLNI)

We now turn our attention to local-global principles.

(DOPOLNI)

Theorem 4.7 (Albert-Brauer-Hasse-Noether**).**

If A *is a central simple algebra over* $\mathbb{Q}$ *and* A *splits over the completion of* $\mathbb{Q}$*, then* A *splits. That is if* $A \otimes \mathbb{Q}_p \cong M_k(\mathbb{Q}_p)$ *for all* p *and* $A \otimes \mathbb{R} \cong M_n(\mathbb{R})$*, then* $A \cong$ *(DOPOLNI)*

(DOPOLNI)

4.3 Relative Brauer group

Given a field extension K/k, there is a homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(K), \quad [S] \mapsto [S_K].$$

This map is well defined:

$$\begin{aligned} S \sim T &\Rightarrow S \otimes_k M_m(k) \cong T \otimes_k M_n(k) \\ &\Rightarrow (S \otimes_k M_m(k)) \otimes_k K \cong (T \otimes_k M_n(k)) \otimes_k K \\ &\Rightarrow (S \otimes_k K) \otimes_K (M_m(k) \otimes_k K) \cong (T \otimes_k K) \otimes_K (M_n(k) \otimes_k K) \\ &\Rightarrow S_K \otimes_K M_m(K) \cong T_K \otimes_K M_n(K) \\ &\Rightarrow S_K \sim T_K. \end{aligned}$$

Definition 4.8. The relative Brauer group $\mathrm{Br}(K/k) = \ker(\mathrm{Br}(k) \to \mathrm{Br}(K))$.

These are central simple algebras over k that we split by K.

Definition 4.9. Let S be a simple k-algebra. A self-centralizing subfield of S is a field $K \subseteq S$ containing k such that $C_S(K) = K$.

Remark.

1. In division rings, maximal subfields coincide with self-centralizing subfields.
2. For $n > 1$, $M_n(\mathbb{H})$ has no self-centralizing subfields. By the centralizer theorem, each such subfield has dimension $2n$. But the only field extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$, which have the dimension $\leq 2 < 2n$.
3. There exists a csa where both a maximal and self-centralizing subfield exist, but are not the same.

Theorem 4.10.

1. *Let S be a csa over k of dimension n^2. Then any self-centralizing subfield K of S is a splitting field for S and $[K : k] = [S : K] = n$.*
2. *Given any field extension $K \supseteq k$ of degree n, any element of $\mathrm{Br}(K/k)$ has a unique representative S of degree n that contains K as a self-centralizing subfield.*

Proof.

1. We know that

$$\begin{aligned} n^2 &= [S : k] \\ &= [K : k][C_S(K) : k] \\ &= [K : k]^2, \end{aligned}$$

so $n = [K : k]$. Now we prove splitting: S acts on S from the left and K acts on S from the right. These two actions commute, which means there exists

$$f : S \otimes_k K \to \mathrm{End}_K(S) \cong M_n(K), \quad s \otimes x \mapsto (s' \mapsto ss'x).$$

Since S is csa and K is simple, $S \otimes K$ is simple and f injective. Now since

$$\begin{aligned} [S \otimes K : k] &= [S : k][K : k] \\ &= n^3 \\ &= n^2[K : k] \\ &= [M_n(K) : k], \end{aligned}$$

f is an isomorphism.

2. Any element in $\mathrm{Br}(K/k)$ is represented by a central division algebra, say D. Then $K \otimes_k D^{\mathrm{op}} \cong M_m(K)$ for some $m \in \mathbb{N}$. In particular, $[D^{\mathrm{op}} : k] = m^2$. Let V be the unique simple $K \otimes_k D^{\mathrm{op}}$

module, so that $K \otimes_k D^{\mathrm{op}} \cong V^m$. then

$$\begin{aligned} m[V : D^{\mathrm{op}}][D^{\mathrm{op}} : k] &= m[V : k] \\ &= [V^m : k] \\ &= [K \otimes D^{\mathrm{op}} : k] \\ &= [K : k][D^{\mathrm{op}} : k], \end{aligned}$$

so

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

Since K acts on V from the left, this action commutes with the action of D^{op}, so there exists

$$K \hookrightarrow \mathrm{End}_{D^{\mathrm{op}}}(V) \cong M_{[V:D^{\mathrm{op}}]}(D) =: S$$

as a K-algebra isomorphism. Hence $[S] = [D] \in \mathrm{Br}(K/k)$ and

$$\begin{aligned} [S : k] &= [V : D^{\mathrm{op}}]^2 [D : k] \\ &= [V : D^{\mathrm{op}}]^2 m^2 \\ &= (m[V : D^{\mathrm{op}}])^2 \\ &= [K : k]^2 \end{aligned}$$

But since

$$[K : k]^2 = [S : k] = [K : k][C(K) : k],$$

we have $[K : k] = [C(K) : k]$. Since $K \subseteq C(K)$, $K = C(K)$. Also, S is unique because of the dimension assumption. □

Remark. For any division algebra with center k, there exists a splitting field K, which is separable over k. This is obvious if $\mathrm{char}\, k = 0$ and is the Jacobson-Noether theorem for general k.

Theorem 4.11 (Jacobson-Noether**).**

If D is noncommutative division ring which is algebra over its center k, then there is an element in $D \setminus k$ which is separable over k.

Proof. Exercises (DOPOLNI). □

Corollary 4.12 (Koethe)**.** *If D is a finite-dimensional division algebra with center k and $K \subseteq D$ is a separable extension of k, then D has a maximal subfield containing K which is separable over k.*

Proof. Let $D_0 = C_D(K)$. By the double centralizer theorem, $C_D(D_0) = K$, so $Z(D_0) = K$ and D_0 is a division algebra over center K. Now we simply use the Jacobson-Noether. □

Corollary 4.13. *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 Jacobson-Noether, there exists a maximal subfield $L \leq D$ that is separable over k. Let $k \subseteq L \subseteq K$ be the normal closure of L. Then K/k is (finite) Galois and since L splits D, so does K. □

Corollary 4.14.

$$\mathrm{Br}(k) = \bigcup \{\mathrm{Br}(K/k) \mid K/k \text{ finite Galois extension}\}.$$

Proof. Let $[A] = [D]$, where D is a central division algebra over k. Since the map

$$\mathrm{Br}(k) \to \mathrm{Br}(K), \quad [A] \mapsto [A_K]$$

is well defined, any extension K/k which splits D also splits A. Hence in order to split A it suffices to split the division ring D. The rest follows from the previous corollary. □

Corollary 4.15. *Suppose D is a central division k-algebra such that $[D:k] = n^2$. Then any splitting field K of D satisfies $n \mid [K:k]$.*

Proof. Let K be the splitting field for D. Then by the previous theorem, $[D] \in \mathrm{Br}(K/k)$ has a unique representative S such that $[S:k] = [K:k]^2$. This implies that

$$n^2 = [D:k] \mid [S:k] \mid [K:k]^2,$$

which gives us $n \mid [K:k]$. □

4.4 Factor sets and crossed product algebras

Let K/k be a Galois field extension, $G = \mathrm{Gal}(K/k)$. Let S be a csa with K as a self-centralizing subfield. Let $\sigma \in G$ be a k-automorphism of K. By the Skolem-Noether theorem, σ extends to an inner isomorphism of S, so there exists a $x_\sigma \in S^{-1}$ such that

$$x_\sigma a x_\sigma^{-1} = \sigma(a), \quad \forall a \in K.$$

How unique is this x_σ? Suppose x'_σ also satisfies this relation. Then

$$x_\sigma a x_\sigma^{-1} = x'_\sigma a (x'_\sigma)^{-1}, \quad \forall a \in K.$$

This is equivalent to $(x'_\sigma)^{-1} x_\sigma \in C(K) = K$. By the control of the non-uniqueness of x_σ's, there exists $a_{\sigma,\tau} \in K^{-1}$ such that

$$a_{\sigma,\tau} x_{\sigma\cdot\tau} = x_\sigma x_\tau.$$

Then $(a_{\sigma,\tau})_{\sigma,\tau\in G}$ is a factor set of S relative to K and we have

$$a : G \times G \to K^{-1}, \quad (\sigma,\tau) \mapsto a_{\sigma,\tau}.$$

How are factor sets associated to different choices of x_σ related? There exists a $f_\sigma \in K^{-1}$ such that $x'_\sigma = f_\sigma x_\sigma$. Assume that $(b_{\sigma,\tau})$ is the factor set associated to x'_σ:

$$b_{\sigma,\tau} x'_{\sigma\cdot\tau} = x'_\sigma x'_\tau.$$

We now have

$$\begin{aligned} f_\sigma \sigma(f_\tau) a_{\sigma,\tau} x_{\sigma\cdot\tau} &= f_\sigma \sigma(f_\tau) x_\sigma x_\tau = f_\sigma x_\sigma f_\tau x_\tau \\ &= x'_\sigma x'_\tau = b_{\sigma,\tau} x'_{\sigma\tau} \\ &= b_{\sigma,\tau} f_{\sigma,\tau} x_{\sigma\tau}, \end{aligned}$$

so

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

If we choose $x'_1 = 1$, then $a_{\sigma,1} = a_{1,\sigma} = 1$ for all $\sigma \in G$. Such a factor set is normalized.

Proposition 4.16. *The set $(x_\sigma)_{\sigma\in G}$ is a basis for S over K.*

Proof. Firstly,

$$|G| = [K:k] = [S:K],$$

so it suffices to check that $(x_\sigma)_\sigma$ are linearly independent. Assume the contrary and choose $J \subsetneq G$ which is maximal such that $(x_\tau)_{\tau\in J}$ is linearly independent. Let $\sigma \in G \setminus J$. Then there exists $a_\tau \in K$ such that

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

If we multiply this equation on the right with $r \in K$, we get

$$x_\sigma r = \sum_J a_\tau x_\tau r,$$

which implies

$$\sigma(r)x_\sigma = \sum_J a_\tau \tau(r) x_\tau.$$

Now if we multiply the same equation from the left with $\sigma(r)$, we get

$$\sigma(r)x_\sigma = \sum \sigma(r)a_\tau x_\tau,$$

which together with the previous line implies

$$a_\tau\tau(r) = \sigma(r)a_\tau, \quad \forall\tau \in J, \quad \forall r \in K.$$

Since $x_\sigma \neq 0$, at least $a_\tau \neq 0$ (for $\tau \in J$). We thus deduce that $\tau(r) = \sigma(r)$ for all $r \in K$, so $\sigma = \tau \in J$, which is a contradiction. □

As a K-vector space, $S = \bigoplus_{\sigma\in G} Kx_\sigma$ and the multiplication in S is given by

$$x_\sigma a = \sigma(a)x_\sigma, \quad \forall a \in K$$

and

$$x_\sigma x_\tau = a_{\sigma,\tau}x_{\sigma\tau}, \quad \forall\sigma,\tau \in G.$$

Which $a : G \times G \to K$ are factor sets? Not every such function works. If we check associativity, we get

$$\rho(a_{\sigma,\tau})a_{\rho,\sigma\tau} = a_{\rho,\sigma}a_{\rho\sigma,\tau}, \quad \forall\rho,\sigma,\tau \in G. \tag{2}$$

Proposition 4.17. *Given a Galois extension K/k with $G = \mathrm{Gal}(K/k)$, any set of elements $(a_{\sigma,\tau})_{\sigma,\tau\in G} \subseteq K^{-1}$ satisfying the above property is the factor set relative to K of a csa A over k. Furthermore, A contains K as a self-centralizing subfield.*

Definition 4.18. Any set $(a_{\sigma,\tau})_{\sigma,\tau\in G}$ in K^{-1} satisfying the (2) is called a factor set relative to K (regardless or not if the algebra of which they are a factor set is given).

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

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

First, we will show that A is an associative algebra with identity. Multiplication is associative by the above property. The identity element is $a_{1,1}^{-1}e_1$, since

$$1(a_{1,\tau}a_{1,\tau}) = a_{1,1}a_{1,\tau}$$

by property (2), which implies $a_{1,\tau=a_{1,1}}$ for all $\tau \in G$. Similarly, we have

$$\sigma(a_{1,1})a_{\sigma,1} = a_{\sigma,1}a_{\sigma,1},$$

which implies $a_{\sigma,1} = \sigma(a_{1,1})$ for all $\sigma \in G$. Together, this implies

$$(a_{1,1}^{-1}e_1)e_\sigma = a_{1,1}^{-1}a_{1,\sigma}e_\sigma = e_\sigma$$

and

$$e_\sigma(a_{1,1}^{-1}e_1) = \sigma(a_{1,1})^{-1}a_{\sigma,1}e_\sigma = e_\sigma.$$

Next, K is a subfield of A via

$$K \to A, \quad r \mapsto r \cdot 1 = r \cdot a_{1,1}^{-1}e_r.$$

Now we prove that $K = C(K)$. Suppose $\sum_{\sigma\in G} a_\sigma e_\sigma \in C(K)$ for some $a_\sigma \in K$. then

$$a\left(\sum_G a_\sigma e_\sigma\right) = \left(\sum_G a_\sigma e_\sigma\right) a.$$

From there, we get

$$a \cdot a_\sigma = a_\sigma\sigma(a), \quad \forall a \in K, \quad \forall\sigma \in G.$$

If some $a_\sigma \neq 0$, then $a = \sigma(a)$ for all $a \in K$ and $\sigma = \mathrm{id}$. Thus $a_\sigma = 0$ for $\sigma \neq \mathrm{id}$, hence $x \in K$, so $C(K) \subseteq K$. The reverse inclusion is obvious. Finally, we prove that $Z(A) = k$. Obviously, $Z(A) \subseteq C(K) = K$. Now suppose $a \cdot e_1 \in K$ is in $Z(A)$. Then $(ae_1)e_\sigma = e_\sigma(ae_1)$ and therefore $aa_{1,\sigma}e_\sigma = \sigma(a)a_{\sigma,1}e_\sigma$. From there, we get $a \cdot a_{1,\sigma} = \sigma(a)a_{\sigma,1}$, which we can rewrite as

$$a \cdot a_{11} = \sigma(a)\sigma(a_{11}) = \sigma(aa_{11}).$$

From there, we get $aa_{11} \in K^G = k$ and

$$ae_1 = \underbrace{aa_{11}}_{\in k} \cdot (a_{11}^{-1}e_1) \in k.$$

Finally, we prove that A is simple. Suppose that $I \lhd A$ is a nontrivial ideal. 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 $a \in k$. As in the proof of the previous proposition, $(\overline{e_\sigma})_{\sigma\in G}$ are linearly independent in A/I. But then

$$\dim A/I \geq |G| = \dim A,$$

a contradiction. □

Definition 4.19. The algebra A is the crossed product of K and G relative to the factor set $(a_{\sigma,\tau})_{\sigma,\tau\in G}$. Notation: $A = (K, G, a)$.

Remark. Any finite set $(a_{\sigma,\tau})_{\sigma,\tau\in G}$ is the factor set of the csa (K, G, a) and (K, G, a) contains K as a self-centralizing subfield. A factor set of a csa isn't uniquely determined since x_σ are only uniquely determined up to multiplication in K^{-1}: if we choose some different $x'_\sigma = f_\sigma x_\sigma$, we get a factor set

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

We say that the factor sets $a_{\sigma,\tau} \sim b_{\sigma,\tau}$ are equivalent. This brings us to the following.

Remark. The crossed product algebra (K, G, a) from the above proof is isomorphic to the algebra S from the beginning of the section (the same vector basis for K and their multiplication).

Lemma 4.20. *The crossed algebras, generated by equivalent factor sets are isomorphic by map*

$$(K, G, b) \to (K, G, a), \quad x'_\sigma \mapsto f_\sigma x_\sigma.$$

Theorem 4.21.

Let K/k be a finite Galois extension with Galois group G. Then there is a bijective correspondence between $\mathrm{Br}(K/k)$ and equivalence classes of factor sets $(a_{\sigma,\tau})$. In other words, every element in $\mathrm{Br}(K/k)$ is of the form $[(K,G,a)]$ for some factor set a.

Proof. Given $x \in \mathrm{Br}(K/k)$, there exists a unique csa A such that $[A] = x$ and A contains K as a self-centralizing subfield. Then we get define a map

$$\mathrm{Br}(K/k) \xrightarrow{\psi_1} (a_{\sigma,\tau})/\sim, \quad A \mapsto [a_{\sigma,\tau}].$$

This map is well defined because A is unique and all factor sets in A relative to are $[A]$ into a factor set of A relative to K (such factor sets are all equivalent). Conversely, given a factor set $(a_{\sigma,\tau})$, the previous proposition constructs a csa (K,G,a) which has $(a_{\sigma,\tau})$ as a factor set. Since equivalent factor sets relative to K give rise to isomorphic crossed product algebras (the previous lemma), we have a well defined map

$$(a_{\sigma,\tau})/\sim \xrightarrow{\psi_2} \mathrm{Br}(K/k), \quad [(a_{\sigma,\tau})] \mapsto [(K,G,a)].$$

Now $\psi_2 \circ \psi_1$ maps $[A]$ into $[(K,G,a)]$, but by last remark, A and (K,G,a) are isomorphic, so $\psi_2 \circ \psi_1$ is an identity. Similarly, $\psi_1 \circ \psi_2$ maps a $[a_{\sigma,\tau}]$ into itself, so it is again an identity and ψ_1, ψ_2 are inverses. □

4.5 Group cohomology and Brauer group

Let G be a group and M an abelian group on which G acts[2]. Denote $C^0(G,M) := M$ and

$$C^n(G,M) := \{\text{functions } G^n \to M\}$$

for $n \in \mathbb{N}$. Clearly, $C^n(G,M)$ is an abelian group under pointwise addition of functions and the zero function as the identity element. In addition, G acts on $C^n(G,M)$ as

$$(g \cdot f)(g_1, \ldots, g_n) = g \cdot f(g_1, \ldots, g_n).$$

We call $C^n(G,M)$ the n-th cochain group. Its elements are n-cochains of G with coefficients in M. We define the maps

$$\delta_0 : C^0(G,M) \to C^1(G,M), \quad f \mapsto (g_1 \mapsto g_1 f - f)$$

and

$$\delta_n : C^n(G,M) \to C^{n+1}(G,M)$$

as

$$\begin{aligned}(\delta_n f)(g_1, \ldots, g_{n+1}) := {} & g_1 \cdot f(g_1, \ldots, g_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^n f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ & + (-1)^{n+1} f(g_1, \ldots, g_n).\end{aligned}$$

The map δ_n is called the n-th coboundary map. It is a group homomorphism.

Proposition 4.22. $\delta_{n+1} \circ \delta_n = 0$.

Proof. This is a routine calculation. □

[2]based on Brown: Cohomology of groups

With the above definitions, $(C^n(G,M),\delta_n)$ is called a cochain complex:

$$0 \to C^0 \xrightarrow{\delta_0} C^1 \xrightarrow{\delta_1} C^2 \xrightarrow{\delta_2} C^3 \to \cdots$$

Taking its homology, we get the n-cocycles $Z^n = \ker(\delta_n)$ and n-coboundaries $B^n = \mathrm{im}(\delta_{n-1})$. Since $\delta \circ \delta = 0$, we have $B^n \subseteq Z^n$. We define the n-th cohomology group of G with coefficients in M as $H^n(G,M) := Z^n / B^n$. The elements of $H^1(G,M)$ are group homomorphisms $G \to M$ and elements of $H^2(G,M)$ are called central extensions of G by M. We now restrict our attention to $G = \mathrm{Gal}\,(()K/k)$ and $M = K^{-1}$ for Galois extension K/k. Then $H^n(G,K^{-1})$ are Galois cohomology groups of the extension K/k with coefficients in K^{-1}. Elements $(f_\sigma)_\sigma : G \to K^{-1}$ are 1-cochains and $a : G \times G \to G^{-1}$ are 2-cochains.

Theorem 4.23 (Hilbert's theorem 90)**.**

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

Lemma 4.24. *If K is a field and $\sigma_1,\ldots,\sigma_n$ are distinct automorphisms of K, they are K-linearly independent.*

Proof. Suppose $\sum c_i\sigma_i = 0$ for $c_i \in K$, where $c_1,\ldots,c_r$ are nonzero and $c_{r+1} = \cdots = c_n = 0$. In addition, assume that r is the smallest possible. There exists Clearly, $r > 1$. There exists $a \in K$ such that $\sigma_1(a) \neq \sigma_r(a)$. Then

$$c_1\sigma_1(ax) + \cdots + c_r\sigma_r(ax) = 0,$$

which immediately gives us

$$c_1\sigma_1(a)\sigma_1(x) + \cdots + c_r\sigma_r(a)\sigma_r(x) = 0.$$

By subtracting

$$c_1\sigma_r(a)\sigma_1(x) + \cdots + c_r\sigma_r(a)\sigma_r(x) = 0,$$

we get

$$c_1(\sigma_1(a) - \sigma_r(a))\sigma_1(x) + \cdots + c_{r-1}(\sigma_{r-1}(a) - \sigma_r(a))\sigma_{r-1}(x) = 0$$

for all $x \in K$. But since $c_1(\sigma_1(a) - \sigma_r(a)) \neq 0$, this contradicts the minimality of r. □

Proof of the theorem.

1. The first part is a trivial calculation:

$$Z^0 = \ker\delta_0 = \{f \in K^{-1} \mid \forall g \in G,\ g \cdot f = f\} = k^{-1}.$$

2. Let $f \in Z^1$. Then $f : G \to K^{-1}$ and

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

From this we get $f(\sigma\tau) = \sigma(f(\tau))f(\sigma)$ or, written more compactly, $f_{\sigma\tau} = \sigma(f_\tau)f_\sigma$. Note that $f \in B^1$ is equivalent to

$$f(\tau) = \delta_0 g(\tau) = \tau(g) \cdot g^{-1}$$

for some $g \in K^{-1}$ This is what we're effectively proving. Consider

$$\sum_{\tau\in G} f_\tau \cdot \tau \neq 0$$

by the previous lemma. There exists $a \in K^{-1}$ such that $b = \sum_{\tau \in G} f_\tau \tau(a) \neq 0$. Finally, we have

$$\begin{aligned}\sigma(b) &= \sum_{\tau \in G} \sigma(f_\tau)\sigma\tau(a) = \sum_{\tau \in G} f_\tau^{-1} \cdot f_{\sigma\tau}(\sigma\tau)(a) \\ &= f_\sigma^{-1} \sum_{\sigma \in G} f_{\sigma\tau}(\sigma\tau)(a) = f_\sigma^{-1} \sum_{\mu \in G} f_\mu \cdot \mu(a) = f_\sigma^{-1} \cdot b,\end{aligned}$$

so $f_\sigma = b \,/\sigma(b) = \sigma(b^{-1}) \,/b^{-1}$ and $g = b^{-1}$ works. □

Elements of Z^2 are functions $a : G \times G \to K^{-1}$ such that $\delta_2(a) = 1$. Note that this is equivalent to

$$1 = \delta_2(\rho, \sigma, \tau) = \rho(a(\sigma, \tau))a(\rho\sigma, \tau)^{-1}a(\rho, \sigma\tau)a(\rho, \sigma)^{-1},$$

which is precisely the factor set (also: cocycle) condition (2). Therefore, 2-cocycles of $C^2(G, K^{-1})$ are just the factor sets relative to K. Likewise, B^2 are functions which are in the image of δ_1, so they are in the form $\delta_1(f)$ for some $f : G \to K^{-1}$:

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

Two cocycles give rise to the same element in $H^2(G, K^{-1})$ precisely when they differ by a coboundary. Hence $H^2(G, K^{-1})$ consists of all factor sets modulo the equivalence realtion in Z^2, which is

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

for some f. By one of the previous theorems, there exists a bijective map

$$\psi : H^2(G, K^{-1}) \to \mathrm{Br}(K\,/k), \quad a \mapsto [(K, G, a)].$$

Lemma 4.25. *As stated abobe, ψ is a group homomorphism. That is, if $K\,/k$ is Galois with the group G and a, b are factor sets, then*

$$[(K, G, a)][(K, G, b)] = [K, G, ab]$$

in $\mathrm{Br}(K\,/k)$.

Proof. Let $A = (K, G, a)$, $B = (K, G, B)$ and $C = (K, G, ab)$. We need to show that $A \otimes_k B \sim C$. We shall find a module on which both $A \otimes_k B$ and C act (on different sides). Define a left K-module $M := A^{\mathrm{op}} \otimes_K B$. Then M is a right $A \otimes_k B$ module with multiplication

$$(a' \otimes_K b') \cdot (a \otimes_k b) = (a'a \otimes_k b'b).$$

But M is also a left C module: indeed, if (u_σ), (v_σ) and (w_σ) are bases of A, B and C respectively, then we can define an action

$$(xw_\sigma)(a \otimes_K b) = (xu_\sigma a \otimes_K v_\sigma b).$$

This action makes M into a left C-module. We just verify associativity: take any $x, x' \in K$,

$\sigma, \tau \in G$, $a \in A$ and $b \in B$. Then

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

Therefore, M is a C-$A \otimes_k B$ bimodule. Define a k-algebra isomorphism

$$\Phi : (A \otimes_k B)^{\mathrm{op}} \to \mathrm{End}_C(M), \quad (a \otimes_k b) \to (m \to m \cdot (a \otimes_k b)).$$

Since $A \otimes_k B$ is a csa, so is $(A \otimes_k B)^{\mathrm{op}}$, hence Φ is injective. Now we have to show that it is onto. Denote

$$n = |G| = [A : K] = [B : K] = [C : K].$$

Then $[M : K] = n^2$ and $[M : k] = n^3 = n[C : k]$. Modules over a simple algebra are determined by the dimension over the base field: if $C \cong M_l(D)$ for some l and some division algebra D over k, then every C-module M is of the form D^{ls}. Therefore,

$$\frac{[M : k]}{[C : k]} = \frac{[D : k]s}{[D : k]l^2} = n,$$

so $M \cong D^{nl^2} \cong C^n$ as a C-module. Now

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

In the end,

$$\dim_k \mathrm{End}_C(M) = n^2 \dim_k C = n^4 = \dim_k A \cdot \dim_k B = \dim_k (A \otimes_k B),$$

so Φ is an isomorphism. As a result

$$(A \otimes_k B)^{\mathrm{op}} \cong C^{\mathrm{op}} \otimes_k M_n(k),$$

which implies $(A \otimes_k B)^{\mathrm{op}} \sim C^{\mathrm{op}}$ and finally $(A \otimes_k B) \sim C$. □

Everything proved so far culminates in the following statement.

Theorem 4.26.

For a Galois extension K/k, $\mathrm{Br}(K/k) \cong H^2(\mathrm{Gal}(K/k), K^{-1})$.

4.6 The Brauer group is torsion

Theorem 4.27.

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

Proof. Let $f \in Z^2$, so $\delta_2 f = 0$. We have

$$(\delta_2 f)(g_1, g_2, g_3) = g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0.$$

Rearrange to get

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

Summing over all $g_3 \in G$ and setting $h(g_2) := \sum_{g_3 \in G} f(g_2, g_3)$, we get

$$\begin{aligned} |G| \cdot f(g_1, g_2) &= \sum_{g_3 \in G} g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) \\ &= g_1 \cdot h(g_2) - h(g_1 g_2) + h(g_1) \\ &= (\delta_1 h)(g_1, g_2) \in B^2. \end{aligned}$$

So $|G| Z^2 \subseteq B^2$, which directly implies $|G| H^2(G, M) = |G| \frac{Z^2}{B^2} = 0$. □

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

Corollary 4.28. *For any field k, $\mathrm{Br}(k)$ is a torsion abelian group.*

Proof. We know that $\mathrm{Br}(k) = \bigcup_{K/k \text{ Galois}} \mathrm{Br}(K/k)$. But

$$\mathrm{Br}(K/k) \cong H^2(\mathrm{Gal}(K/k), K^{-1})$$

and $H^2(\mathrm{Gal}(K/k), K^{-1})$ is annihilated by $|G| = [K : k]$. □

As a result, if A is a csa over k, then there exists a $r \in \mathbb{N}$ such that

$$\underbrace{A \otimes \cdots \otimes A}_{r} \cong M_s(k)$$

for some $s \in \mathbb{N}$.

4.7 Primary decomposition for division algebras

Let D be a finite-dimensional central division algebra over k. Then $[D]$ has finite order in $\mathrm{Br}(k)$, say $\mathrm{order}([D]) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ for distinct primes p_j and $\alpha_j \in \mathbb{N}$. We will show that D decomposes as a tensor product of central division algebras D_j with $\mathrm{order}([D]) = p_j^{\alpha_j}$.

Let K be a splitting field for D: $D_K = D \otimes_k K \cong M_n(K)$ for some $n \in \mathbb{N}$. The degree of D is $\deg D = \sqrt{[D : k]} = n$: indeed,

$$[D_K : k] = [D : K] \cdot [K : k] = n^2 [K : k].$$

If A is a central simple algebra over k, then $A \cong M_m(D)$ for a unique central division algebra D. The index of A (denoted as $\mathrm{ind}(A)$) is defined to be the degree of D. The exponent of A (denoted as $\exp(A)$) is the order of $[A]$ in $\mathrm{Br}(k)$. This is the smallest $r \in \mathbb{N}$ such that $A^{\otimes r} \cong M_s(k)$ for some $s \in \mathbb{N}$.

Proposition 4.29. $[A]^{\mathrm{ind}(A)} = 1$ *in* $\mathrm{Br}(k)$*, that is to say that* $\exp(A) \mid \mathrm{ind}(A)$.

Proof. Let $[A] = [(K, G, a)]$ for some finite Galois extension K/k, where $G = \mathrm{Gal}(K/k)$ and $a \in Z^2(G, K^{-1})$. WLOG we can take A to be a unique representative csa over k such that K is its centralizing subfield and then $A = (K, G, a)$. Assume $A \cong M_r(D)$ for some central division algebra D over k where $[D : k] = m^2$ and $m = \mathrm{ind}(A)$. Assume $[A : k] = n^2 = r^2 m^2$. By an earlier lemma,

$$[A]^m = [(K, G, a)]^m = [(K, G, a^m)].$$

Lastly, it suffices to show $a^m \in B^2$. Let $V = (D^{\mathrm{op}})^r$. This is a left $\mathrm{End}_{D^{\mathrm{op}}}(V)$-module by $\phi \cdot v = \phi(v)$ for $v \in V$ and $\phi \in \mathrm{End}_{D^{\mathrm{op}}}(V)$ and V is also a left A-module. Since $K \subseteq A$, V is a K-vector space.

But since

$$\begin{aligned} r \cdot m^2 &= [V : D^{\mathrm{op}}][D^{\mathrm{op}} : k] \\ &= [V : k] = [V : K][K : k] \\ &= [V : K]n = [V : K]rm, \end{aligned}$$

we have $[V : K] = m$. Fix a basis $(v_1, \ldots, v_m)$ for V over K. For any $c \in A$, we have $cv_i = \sum_{j=1}^{m} c_{ij} v_j$ for some $c_{ij} \in K$. Written in matrix form:

$$c \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = [c_{ij}] \cdot \underbrace{\begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}}_{v}.$$

Take the distinguished basis $(x_\sigma)_{\sigma \in G}$ for $A = (K, G, a)$ over K. The above construction associates a matrix $X_\sigma \in M_m(K)$ to each x_σ. Notice that

$$\underbrace{x_\sigma (x_\tau \cdot v)}_{\text{module multiplication}} = x_\sigma X_\tau v = \sigma(X_\tau) X_\sigma v$$

and

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

This directly gives us

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

Taking the determinant of both sides (all matrices are invertible), we get

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

and

$$a_{\sigma,\tau}^m = \frac{\sigma(\det X_\tau) \det(X_\sigma)}{\det(X_{\sigma,\tau})} \in B^2$$

and we are done. □

Proposition 4.30. *Every prime divisor of the* $\mathrm{ind}(A)$ *divides* $\exp(A)$.

Proof. Let $(K, G, a) \cong M_n(D)$ be a crossed product algebra with

$$[A] = [(K, G, a)] = [M_n(D)] = [D],$$

where D is a central division algebra. Let $d = \mathrm{ind}(A) = \deg(D)$ and p be a prime divisor of d. First we notice that

$$|G|^2 = [(K, G, a) : k] = n^2 \cdot d^2,$$

which implies $|G| = n \cdot d$ and $p \mid |G|$. Let G_p be the p-Sylow subgroup of G and $K_p := K^{G_p} \subseteq K$. By the fundamental theorem of Galois theory,

$$[K : K_p] = |G_p| = p^r$$

for some $r \in \mathbb{N}$. Since G_p is p-Sylow, p does not divide $[K_p : k]$. If the field K_p split A, then it would split D. But by corollary 4.15 we'd have $\deg D \mid [K_p : k]$. Since p divides $\deg D$ but not $[K_p : k]$, we arrive at a contradiction, so K_p cannot split A. In particular, $\exp(A_{K_p}) \neq 1$. But now notice that

$$A \otimes_k K = (A \otimes_k K_p) \otimes_{K_p} K = A_{K_p} \otimes K,$$

which means that K splits A_{K_p}. Again using corollary 4.15, this means that the degree of its associated division ring (this is exactly $\mathrm{ind}(A_{K_p})$) divides $[K : K_p] = p^r$. By previous proposition, $\exp(A_{K_p})$ divides $\mathrm{ind}(A_{K_p})$ and therefore also divides p^r. But $\exp(A_{K_p}) \neq 1$, as we have already argued, so $p \mid \exp(A_{K_p})$. Since

$$\mathrm{Br}(k) \to \mathrm{Br}(K_p), \quad [S] \mapsto [S_{K_p}]$$

is a group homomorphism, $p \mid \exp(A_{K_p}) \mid \exp(A)$ and we're done. □

Proposition 4.31. *Suppose D_1, D_2 are central division algebras with coprime degrees. Then $D_1 \otimes D_2$ is a division algebra.*

Proof. By Wedderburn theory, $D_1 \otimes D_2 \cong M_n(D)$ for some $n \in \mathbb{N}$ and division algebra D. The identity $D_1^{\mathrm{op}} \otimes D_1 \cong M_n(k)$ implies

$$n^2[M_n(k) : k] = [D_1^{\mathrm{op}} \otimes D_1 : k] = [D_1 : k]^2,$$

which gives us $n = [D_1 : k]$. Consider the following calculation:

$$\begin{aligned} M_n(D_2) &\cong M_n(k) \otimes D_2 \cong D_1^{\mathrm{op}} \otimes D_1 \otimes D_2 \\ &\cong D_1^{\mathrm{op}} \otimes M_m(D) \cong M_m(D_1^{\mathrm{op}} \otimes D) \\ &\cong M_m(M_r(D')) \cong M_{mr} \end{aligned}$$

for some $r \in \mathbb{N}$ and a division algebra D'. By uniqueness (Wedderburn), we get $mr = n$ and $D' = D_2$, so $n \mid [D_1 : k]$. By symmetry, $m \mid [D_2 : k]$. But since D_1 and D_2 are of coprime degree, we have $m = 1$ and $D_1 \otimes D_2 \cong D$ is a division algebra. □

Theorem 4.32.

Let D be a finite-dimensional central division algebra over k and $\deg(D) = p_1^{n_1} \cdots p_r^{n_r}$, where p_j are distinct primes, $n_j \in \mathbb{N}$. Then there exists a unique decomposition (up to isomorphism)

$$D = D_1 \otimes D_2 \otimes \cdots \otimes D_r,$$

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

Proof. It's enough to show that if $\deg D = n_1 \cdot n_2$ and n_1, n_2 are coprime, then $D \cong D_1 \otimes D_2$ with $\deg(D_1) = n_1$ and $\deg(D_2) = n_2$. There exist $u, v \in \mathbb{Z}$ such that $un_1 + un_2 = 1$. Let D_1 be the unique central simple algebra with $[D_1] = [D]^{vn_2}$. Likewise, $[D_2] = [D]^{un_1}$. We have

$$[D_1 \otimes D_2] = [D]^{un_1 + vn_2} = [D].$$

This gives us

$$[D_1]^{n_1} = [D]^{vn_2 n_1} = [D]^{nv} = [k],$$

so $\exp(D_1) \mid n_1$. By symmetry, $\exp(D_2) \mid n_2$. From one of the above propositions, $\exp(D_i)$ and $\mathrm{ind}(D_i) = \deg(D_i)$ have the same prime factors. As $\gcd(n_1, n_2) = 1$, we get $\gcd(\deg D_1, \deg D_2) = 1$. So $D_1 \otimes D_2$ is a division algebra and since $[D_1][D_2] = [D]^{un_1 + vn_2} = [D]$, we get $D_1 \otimes D_2 \cong D$ and $\deg(D_j) = n_j$. Uniqueness is obviious. □

4.8 Miscellaneous and open problems

Theorem 4.33 (Merkurjev-Suslin)**.**

If $\operatorname{char} k = 0$ *and* k *contains all roots of unity, then* $\operatorname{Br}(k)$ *is generated by cyclic algebras.*

For $\deg A = 2$ and $\deg A = 3$, every division algebra A is cyclic. But for $\deg A = 4$, there exist non-cyclic division algebras. The following statement used to be an open problem: for a prime $p \geq 5$, construct a noncyclic division algebra of degree p. It has been shown that such division algebras do in fact exist. Another question we could ask ourself is whether all central division algebras of prime exponents are crossed algebras. So far, this problem has not yet been solved. Another open problem is whether every division algebra is split by an abelian field extension (i.e. $\operatorname{Gal}(K/k)$ is abelian). Finally, another topic of interest is whether for field h we can bound $\operatorname{ind}(A)$ in terms of $\exp(A)$.

We now turn our attention to a generic/universal division algebra. Let F be an infinite field and $n, r \in \mathbb{N}$, where $r \geq 2$. Define a polynomial ring

$$S := F[x_{ijk} \mid 1 \leq i, j \leq n,\ 1 \leq k \leq r]$$

and a matrix ring $M_n(S)$. We define a generic $n \times n$ matrix $X_k = [x_{ijk}]_{1 \leq i,j \leq n}$.

Let $GM_n(F, r)$ be an F-subalgebra of $M_n(S)$ generated by $X_1, \ldots, X_r$. We call this the ring of r generic $n \times n$ matrices. We have the following universal property: let A be a csa over L, where L/F is a field extension. Pick $a_1, \ldots, a_r \in A$. Then there exists a F-algebra homomorphism $GM_n(F, r) \to A$ such that $X_j \mapsto a_j,\ \forall j$.

Theorem 4.34.

$GM_n(F, r)$ is a domain (i.e. it has no zero divisors).

We denote $C := C(F, n, r)$ as the center of $GM_n(F, r)$.

Proposition 4.35. *$I \lhd GM_n$ implies $I \cap C = (0)$.*

Let Z be the quotient field of C. Then we define universal division algebra as

$$UD_n(F, r) := \frac{GM_n(F, r)}{C \setminus \{0\}},$$

so its elements are fractions with elements of C in denominator.

Theorem 4.36.

$UD_n(F, r)$ is a division algebra of degree n over its center Z.

Theorem 4.37 (Anitsur)**.**

If $p^3 \mid n$ and $p \neq \operatorname{char} F$, then $UD_n(F, r)$ is not a crossed product algebra.

The group of invertible matrices $GL_n(F)$ has center $F^{-1} \cdot I_n$. Define

$$PGL_n(F) := GL_n(F)/F^{-1}.$$

Notice that $PGL_n(F)$ acts on $S = F[x_{ijk}]$; by picking $A \in GL_n(F)$

$$\phi_A : S \to S, \quad x_{ijk} \mapsto (A^{-1} X_k A)_{ij}.$$

But $PGL_n(F)$ also acts on $M_n(S)$; for $B \in GL_n(F)$, we have

$$\psi_B M_n(S) \to M_n(S), \quad Y \mapsto B(M_n(\psi_B)(Y))B^{-1},$$

which means that ψ_B is applied elementwise to Y. Every generic matrix X_k is invariant under this action, which implies $GM_n(F,r) \subseteq M_n(S)^{PGL_n(F)}$. Now if we define $K := F(x_{ijk})$ as the quotient field of S, we have the following.

Theorem 4.38.

$UD_n(F,r) = M_n(K)^{PGL_n(F)}$ and $Z = K^{PGL_n(F)}$.

5 Local rings, idempotents and decompositions

Definition 5.1.
- R is a local ring if $R/\operatorname{rad} R$ is a division ring.
- R is a semilocal ring if $R/\operatorname{rad} R$ is semisimple.
- An element $e \in R$ is an idempotent if $e^2 = e$.

Example 5.2. *Left-artinian rings are semilocal.*

5.1 Semilocal rings

Theorem 5.3.

For a ring R, the following is equivalent:

1. *R has a unique maximal left ideal.*
2. *R has a unique maximal right ideal.*
3. *$R/\operatorname{rad} R$ is a division ring (R is local).*
4. *$R \setminus R^{-1} \lhd R$.*
5. *$R \setminus R^{-1}$ is a group.*
6. *If for some $a, b \in R$, we have $a + b \in R^{-1}$, then $a \in R^{-1}$ or $b \in R^{-1}$.*
7. *If for some $a_1, \ldots, a_n \in R$ we have $a_1 + \cdots + a_n \in R^{-1}$, then there exists an index i such that $a_i \in R^{-1}$.*

Proof. First, we tackle (3) $\Rightarrow$ (1), (2). By the basic properties of ideals, there is a bijective correspondence between left/right ideals in $R/\operatorname{rad} R$ and left/right ideals in R that contain $\operatorname{rad} R$. Since $R/\operatorname{rad} R$ is a division ring, any maximal left/right ideal M in R that contains $\operatorname{rad} R$ must be equal to $\operatorname{rad} R$. Next, (1) $\Rightarrow$ (3). The ring $R/\operatorname{rad} R$ has only two left ideals: (0) and $R/\operatorname{rad} R$. In particular, every nonzero element in $R/\operatorname{rad} R$ has a left inverse, so for $x \in R/\operatorname{rad} R$ there exists an x' such that $x'x$. Now let y be a left inverse of xx'. Then

$$1 \cdot xx' = (yxx') \cdot xx' = y \cdot (xx') = 1,$$

so x' is a right inverse of x as well. The implication (2) $\Rightarrow$ (3) is the same as the above. For (3) $\Rightarrow$ (4), recall that $a \in R$ is left/right invertible iff $\overline{a} = a + \operatorname{rad} R \in R/\operatorname{rad} R$ is left/right invertible. Since the image of any element $R \setminus \operatorname{rad} R$ is invertible in $R/\operatorname{rad} R$, we have $R \setminus R^{-1} = \operatorname{rad} R \lhd R$. The implications (4) $\Rightarrow$ (5), (5) $\Rightarrow$ (6) and (6) $\Leftrightarrow$ (7) are obvious. For (6) $\Rightarrow$ (3), let $a \in R/\operatorname{rad} R$. Then there exists a maximal left ideal M of R such that $a \notin M$. By maximality of M, $M + Ra = R$. In particular, there exists a $m \in M$ and $b \in R$ such that $m + ba = 1$. Then $ba \in R^{-1}$, so a is left invertible and $a + \operatorname{rad} R \in R/\operatorname{rad} R$ is left invertible. By the similar argument, $a + \operatorname{rad} R$ is right invertible, so it is invertible. Therefore, $R/\operatorname{rad} R$ is a division ring. □

Proposition 5.4. *Let R be a local ring.*

1. *R has a unique maximal ideal.*
2. *R has no nontrivial idempotents.*
3. *R is Dedekind-finite.*

Remark. The converse to (1) is not true: $M_n(k)$ has a unique maximal ideal (0), but is not a local ring.

Proof. 1. The unique maximal ideal is of course $\operatorname{rad} R$.
2. Suppose $e \in R$ is an idempotent. Then $1-e$ is also an idempotent, so by the previous theorem we have $e \in R^{-1}$ or $1-e \in R^{-1}$. But $e(1-e)=0$, so either $e=1$ or $e=0$.
3. If $ab=1$, then $(ba)^2 = b(ab)a = ba$ is an idempotent, so either $ba=0$ or $ba=1$. It it were the former, then $0=b(ab)=b$, so it has to be the latter. □

Proposition 5.5. *1. If each $a \in R \setminus R^{-1}$ is nilpotent, then R is local.*

2. Suppose R is a subring of a division ring D. If for each $d \in D$ we have $d \in R$ or $d^{-1} \in R$ (R is a valuation ring in D), then R is local.

Proof. 1. We prove that $R \setminus R^{-1} \subseteq \operatorname{rad} R$. Let $a \notin R^{-1}$ and $k \in \mathbb{N}$ be the smallest exponent such that $a^k = 0$. WLOG $a \neq 0$. Notice that $Ra \subseteq R \setminus R^{-1}$, otherwise there would exist $b \in R$ such that $ba \in R^{-1}$ and $ba \cdot a^{k-1} = 0$ would imply $a^{k-1}=0$, which is a contradiction. This means that $Ra \leq {}_R R$ and all its elements are nilpotent, so Ra is nil and so $Ra \subseteq \operatorname{rad} R$. This implies that $a \in \operatorname{rad} R$, so $R \setminus R^{-1} \subseteq \operatorname{rad} R$, but of course the inclusion also goes the other way around. Therefore $R \setminus R^{-1} = \operatorname{rad} R \lhd R$.
2. Let $a, b \in R$ such that $a+b \in R^{-1}$: WLOG $a+b=1$. Let $c := a^{-1}b \in D$. If $c \in R$, then

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

But if $c^{-1} \in R$, then

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

Example 5.6. *Every division ring is a local ring.*

Example 5.7. *If R is local, then $R[[X]] = A$ (a power series ring) is local. Recall that if $a = \sum_{i=0}^{\infty} a_i x^i$ is invertible in A iff $a_0 \in R^{-1}$. Hence*

$$\operatorname{rad} A = \{\sum_{0}^{\infty} a_i x^i \mid a_0 \in \operatorname{rad} R\}$$

and

$$R/\operatorname{rad} R = A/\operatorname{rad} A$$

is a division ring. Moreover, if $\sigma \in \operatorname{Aut}(R)$, then $R[[x,\sigma]]$ is local, too.

Example 5.8. *Let D be a division ring and R a ring of upper triangular $n \times n$ matrices with elements in D. Then* $\operatorname{rad} R$ *is a set of all strictly upper triangular matrices and*

$$R/\operatorname{rad} R = \underbrace{D \oplus \cdots \oplus D}_{n}.$$

Let A be the subring of R containing elements of the form

$$\begin{pmatrix} a & * & * \\ & \ddots & * \\ & & a \end{pmatrix},$$

where $a \in D$. Then $\operatorname{rad} R \subseteq A$ and $A/\operatorname{rad} R \cong D$, so A is local.

5.2 Intermezzo: commutative local rings: localization and fractions

In this subsection, all rings are considered commutative.

Definition 5.9.
- A set $A \subseteq R$ is multiplicative if $1 \in S$ and $\forall a, b \in S : \ ab \in S$.
- Let $S \subseteq R$ be multiplicative. Define an equivalence relation on $R \times S$ by

$$(a, s) \sim (a', s') \Leftrightarrow \exists u \in S : \ u \cdot (as' - a's) = 0.$$

Denote $\frac{a}{s} = [(a, s)]_\sim$. Then

$$S^{-1}R := \{a/s \mid a \in R, s \in S\}$$

is a localization of R at S. This is a ring via operations

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{as'}, \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}.$$

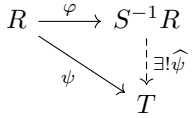
Remark.
- We have a homomorphism

$$\varphi : R \to S^{-1}R, \quad r \mapsto \frac{r}{1}.$$

If S has no zero-divisors, then φ is injective.

- 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 a quotient field of R.

Localizations satisfy the following universal property: suppose $S \subseteq R$ is multiplicative and $\psi : R \to T$ is a ring homomorphism. If $\psi(s) \in T^{-1}$ for all $s \in S$, then there exists a unique homomorphism $\widehat{\psi} : S^{-1}R \to T$ such that $\psi = \widehat{\psi} \circ \varphi$.



Example 5.10. *If $S = \{1\}$, then $S^{-1}R = R$.*

Example 5.11. *Let $P \lhd R$ be a prime proper ideal. Then $S := R \setminus P$ is multiplicative. The ring $R_P := S^{-1}R$ is called a localization of R at prime P.*

Example 5.12. *If we let $R = \mathbb{Z}$ and $S = \mathbb{Z} \setminus \{0\}$, then $S^{-1}\mathbb{Z} = \mathbb{Q}$. Now if $p \in \mathbb{Z}$ is a prime and*

$S = \{p^n \mid n \in \mathbb{N}_0\}$, *then*

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{p^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0 \right\} \subseteq \mathbb{Q}.$$

Finally, if we take a prime ideal $(p) \lhd \mathbb{Z}$*, we get*

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}, p \text{ does not divide } b \right\} \subseteq \mathbb{Q}$$

which is a valuation ring in $\mathbb{Q}$*, therefore a local ring.*

Proposition 5.13. *Let* $S \subseteq R$ *be multiplicative and*

$$\varphi : R \to S^{-1}R, \quad r \mapsto \frac{r}{1}.$$

Then there exists a bijective correspondence between prime ideals of $S^{-1}R$ *and prime ideals* $P \lhd R$ *such that* $P \cap S = \emptyset$*:*

$$Q \mapsto \varphi^{-1}(Q)$$

or inversely by

$$P \mapsto \left\{ \frac{a}{s} \mid a \in P, s \in S \right\}.$$

Corollary 5.14. *Let* $P \lhd R$ *be prime. Then there exists a bijection between prime ideals of* R_P *and prime ideals* $Q \lhd P$ *such that* $Q \subseteq P$*. In particular,* R_P *has a unique maximal ideal, namely* $P \cdot R_P$*. So* R_p *is a local ring.*

Remark. We can compare this to the correspondence between prime ideals of R/P and prime ideals $Q \lhd R$ such that $Q \supseteq P$.

5.3 Indecomposable modules

Definition 5.15. $M \in {}_R\mathrm{Mod}$ is indecomposable if it is not of the form $M = A \oplus B$ for some $(0) \neq A, B \subsetneq M$.

Lemma 5.16. *A module* M *is indecomposable iff* $E := \mathrm{End}(M)$ *has no nontrivial idempotents.*

Proof. ($\Leftarrow$) If M is decomposable, $M = A \oplus B$ for some $(0) \neq A, B \subsetneq M$. The projection $e : M \to A \leq M$ is an element of $E = \mathrm{End}(M)$ and $e^2 = e$ is neither zero nor identity. ($\Rightarrow$) If $e \in E$ is a nontrivial idempotent, then $1 - e \in E$ is idempotent. We can define $A := eM$ and $B := (1 - e)M$ and we get $M = A \oplus B$. □

Definition 5.17. We call $M \in {}_R\mathrm{Mod}$ strongly indecomposable if $\mathrm{End}(M)$ is a local ring.

Example 5.18. *If* M *is simple, then* $\mathrm{End}(M)$ *is a division ring by Schur's lemma, so* M *is strongly indecomposable.*

Example 5.19. *Let* $R = \mathbb{Z}$*.*

- *If* $M = \mathbb{Z}$*, then* $\mathrm{End}(M) \cong \mathbb{Z}$*, so* M *is indecomposable, but not strongly indecomposable.*
- *For a prime* p*, let* $M = \frac{\mathbb{Z}}{p^n\mathbb{Z}}$*. Then* $\mathrm{End}(M) = \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ *is a local ring, so it is strongly indecomposable.*

Definition 5.20. A module $M \in {}_R\,\mathrm{Mod}$ has finite length iff all of its chains of submodules

$$(0) = \mathbb{N}_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_s = M$$

have bounded length. The largest integer s for which there is such a chain is called the length of M.

Proposition 5.21. *Let $M \in {}_R\,\mathrm{Mod}$. The following statements are equivalent.*

1. *M has finite length;*
2. *M is noetherian and artinian;*
3. *M has a composition series chain*

$$(0) = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_s = M$$

such that $\frac{N_{j+1}}{N_j}$ (composition factors) are simple for all j;

4. *M is a direct sum of finitely many simple R-modules.*

Remark. By Jordan-Hölder, the composition factors are unique up to a permutation.

Lemma 5.22 (Fitting lemma)**.** *Let $M \in {}_R\,\mathrm{Mod}$ have finite length and let $f \in \mathrm{End}(M)$. Then there exists $r \in \mathbb{N}$ such that for all $n \geq r$ we have $M = \ker f^n \oplus \operatorname{im} f^n$.*

Proof. Clearly,

$$M \supseteq \operatorname{im} f \supseteq \operatorname{im} f^2 \supseteq \dots$$

and

$$(0) \subseteq \ker f \subseteq \ker f^2 \subseteq \dots$$

Since M is noetherian and artinian, both chains stabilize. In particular, there exists $r \in \mathbb{N}$ such that

$$\operatorname{im} f^r = \operatorname{im} f^{r+1} = \operatorname{im} f^{r+2} = \dots$$

and

$$\ker f^r = \ker f^{r+1} = \ker f^{r+2} = \dots$$

We now prove that $M = \ker f^r \oplus \operatorname{im} f^r$. Suppose $a \in \ker f^r \cap \operatorname{im} f^r$. Then there exists $b \in M$ such that $a = f^r(b)$, so $b \in \ker f^{2n} = \ker f^n$ and $a = 0$. Let $c \in M$. Then there exists $d \in M$ such that $f^r(c) = f^{2r}(d)$. Hence $f^r(c - f^r(d)) = 0$, so

$$c = \underbrace{(c - f^r(d))}_{\in \ker f^r} \oplus \underbrace{f^r(d)}_{\in \operatorname{im} f^r}$$

and we're done. □

Theorem 5.23.

Suppose $M \in {}_R\,\mathrm{Mod}$ is indecomposable and of finite length. Then $E := \mathrm{End}(M)$ is local and its maximal ideal $\operatorname{rad} E$ is nil. In particular, E is strongly indecomposable.

Proof. We prove that every $f \in E \setminus E^{-1}$ is nilpotent. By fitting, there exists $r \in \mathbb{N}$ such that $M = \ker f^r \oplus \operatorname{im} f^r$. By indecomposability of M, we either have $\ker f^r = (0)$ or $\operatorname{im} f^r = (0)$. If it were the former, then $\operatorname{im} f^r = M$, which would imply that f^r is both injective and surjective and

therefore invertible, which is a contradiction. So $\operatorname{im} f^r = (0)$ and f is nilpotent. □

Corollary 5.24. *A right artinian ring is local iff it has no nontrivial idempotents.*

Proof. The right implication ($\Rightarrow$) is obvious. Let us prove the other one ($\Leftarrow$). By Hopkins-Levitski (Pierre Antoine Grillet, theorem IX.6.4.), $M := R_R$ is of finite length. Hence $E = \operatorname{End}(M) \cong R$ is without nontrivial idempotents, so M is indecomposable. Then M is strongly indecomposable and $E = \operatorname{End}(M) = R$ is local. □

Proposition 5.25. *Suppose $M \in {}_R\operatorname{Mod}$ is noetherian or artinian. Then M admits a Krull-Schmidt decomposition, so M can be written as a finite direct sum of indecomposable submodules.*

Proof. We call $N \leq {}_R M$ tame if it admits a K-S decomposition and wild otherwise. Firstly, (0) is tame and so is any other indecomposable submodule. Furthermore, if $N, N' \leq {}_R M$ are tame and $N \cap N' = (0)$, then $N + N'$ is tame. Assume M is wild, so it is decomposable: $M = M_1 \oplus M_2$ and $M_1, M_2 \neq (0)$. WLOG M_1 is wild. Then $M_1 = M_{11} \oplus M_{12}$ for $M_{11}, M_{12} \neq (0)$. Again, WLOG M_{11} is wild. Repeat this process to get two chains of submodules:

$$M \supsetneq M_1 \supsetneq M_{11} \supsetneq \dots$$

and

$$(0) \subsetneq M_2 \subsetneq M_2 \oplus M_{12} \subsetneq M_2 \oplus M_{12} \oplus M_{112} \subsetneq \dots$$

So M is neither artinian nor noetherian, leading to a contradiction. So M is tame. □

Theorem 5.26 (Krull-Schmidt)**.**

Suppose $M \in {}_R\operatorname{Mod}$ is of finite length. If

$$M = M_1 \oplus \dots \oplus M_r = N_1 \oplus \dots \oplus N_s$$

are two decompositions of M into direct sums of indecomposables, then $r = s$ and there exists $\sigma \in S_r$ such that $M_i \cong N_{\sigma(i)}$.

Proof. Let $\alpha_i : M \to M_i$ and $\beta_j : M \to N_j$ be projections, so $\alpha_i, \beta_j \in \operatorname{End}(M)$. Then

$$\alpha_1 + \dots + \alpha_r = 1 = \beta_1 + \dots + \beta_s.$$

Then

$$\alpha_1 = \alpha_1\beta_1 + \dots + \alpha_1\beta_s,$$

which implies

$$\alpha_1\big|_{M_1} = \mathrm{id}_{M_1} = \sum_{j=1}^{s} \alpha_1\beta_j\big|_{M_1} \in \operatorname{End}(M_1).$$

Since M_1 is indecomposable and of finite length, $\operatorname{End}(M_1)$ is local. Hence there exists j such that $\alpha_1\beta_j\big|_{M_1}$ is invertible, WLOG $j = 1$. Then $\beta_1\big|_{M_1} : M_1 \to N_1$ is injective with left inverse. The short exact sequence

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

thus splits. In particular (by the short exact sequence lemma), $N_1 \cong M_1 \oplus N_1/M_1$. By indecomposability of N_1, $N_1 \cong M_1$. We claim that $M = M_1 \oplus N_2 \oplus \dots \oplus N_s$. Since $\beta_1\big|_{M_1} : M_1 \to N_1$ is an isomorphism, so

$$M_1 \cap \underbrace{\ker(\beta_1)}_{N_2 \oplus \dots \oplus N_s} = 0.$$

It then suffices to show that $N_1 \subseteq M_1 \oplus N_2 \oplus \cdots \oplus N_s$. Let $a \in N_1$. Then there exists $b \in M_1$ such that $\beta_1(b) = a$. Then $\beta_1(a-b) = 0$. Hence

$$a = b + (a-b) \in M_1 \oplus N_2 \oplus \cdots \oplus N_s,$$

so by quotienting we get

$$M_2 \oplus \cdots \oplus M_r = M/M_1 = N_1 \oplus \cdots \oplus N_s$$

and induction does the rest. □

Remark. Krull-Schmidt theorem can fail if M is only noetherian or only artinian.

5.4 Semilocal rings

Proposition 5.27. *If R has only finitely many maximal left ideals, then it is semilocal.*

Proof. WLOG $\operatorname{rad} R = (0)$. Let $M_1, \ldots, M_r \leq {}_R R$ be all the maximal left ideals. Consider R-module map

$$\Phi : R \to \bigoplus_{i=1}^{r} R/M_i, \quad x \mapsto (x + M_1, \ldots, x + M_r),$$

then $\ker \Phi = \bigcap_{i=1}^{r} M_i = \operatorname{rad} R = (0)$. By maximality, each R/M_i is simple, so $\bigoplus_{i=1}^{r} R/M_i$ is semisimple. Hence ${}_R R$ is (via Φ) a submodule of this semisimple module, so semisimple. Thus R is a semisimple ring. □

Remark. The converse of this proposition holds if $R/\operatorname{rad} R$ is commutative.

Example 5.28. *1. Every (left) artinian ring is semilocal.*
2. If R is semilocal, then so is $M_n(R)$. Indeed, $\operatorname{rad} M_n(R) = M_n(\operatorname{rad} R)$, so

$$M_n(R)/\operatorname{rad} M_n(R) = M_n(R)/M_n(\operatorname{rad} R) = M_n(R/\operatorname{rad} R).$$

3. A finite product of local rings is semilocal.

5.5 Idempotents

if R is commutative and $e \in R$ is an idempotent, then $R \cong Re \times R(1-e)$. If $e \neq 0, 1$, then such a ring R is not indecomposable. The same holds true in the noncommutative setting if $e \in Z(R)$ (e is a central idempotent).

Definition 5.29. A ring R is indecomposable if it cannot be written as a direct product of nontrivial rings.

Proposition 5.30. *R is indecomposable iff R does not have nontrivial central idempotent.*

Lemma 5.31. *Let $e \in R$ be an idempotent and $f := 1 - e$. Then e is a central idempotent iff $eRf = fRe = (0)$.*

Proof. The implication ($\Rightarrow$) is trivial: $erf = ref = 0$ and $fre = fer = 0$. The reverse ($\Leftarrow$) follows from

$$erf = er(1-e) = er - ere = 0$$

and

$$fre = (1-e)re = re - ere = 0. \qquad \square$$

Let R be a ring, $e \in R$ idempotent and $f = 1 - e$. Then $R = Re \oplus Rf$ in ${}_R\mathrm{Mod}$ and $R = eR \oplus fR$ in Mod_R. As abelian groups, we have

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

where eRf and fRe are abelian groups and

$$eRe = \{r \in R \mid er = r = re\}, \quad fRf = \{r \in R \mid fr = r = rf\}$$

are corner rings.

Example 5.32. *Let A be some ring and $R = M_n(A)$. Let*

$$e = \begin{pmatrix} I_k & 0 \\ 0 & 0_{n-k} \end{pmatrix}, \quad f = \begin{pmatrix} 0_k & 0 \\ 0 & I_{n-k} \end{pmatrix}.$$

Then

$$eRe = \underbrace{\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}}_{M_k(A)}, \quad eRf = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}, \quad fRe = \begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix}, \quad fRf = \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix}}_{M_{n-k}(A)}.$$

Proposition 5.33. *Suppose $e, e' \in R$ are idempotents and $M \in \mathrm{Mod}_R$.*

1. *There exists an isomorphism of abelian groups $\mathrm{Hom}(eR, M) \to Me$.*
2. *There exists an isomorphism of abelian groups $\mathrm{Hom}(eR, e'R) \cong e'Re$.*

Proof. 1. Let $\theta : eR \to M$ be a homomorphism of right R-modules and $m := \theta(e) \in M$. Then

$$m \cdot e = \theta(e) \cdot e = \theta(e^2) = \theta(e) = m \in Me.$$

Define

$$\lambda : \mathrm{Hom}(eR, M) \to Me, \quad \theta \mapsto \theta(e).$$

This is a homomorphism of abelian groups. First we show that λ is injective. Since $\theta(er) = \theta(e)r$, θ is uniquely determined by $\theta(e)$. Now surjectivity: take $m \in Me$ and set $\theta(er) := mr$. This θ is well defined; indeed, if $er = 0$, then $mr \in Mer = (0)$. Hence $\theta \in \mathrm{Hom}(eR, M)$ and $\lambda(\theta) = \theta(e) = m$.

2. Apply the previous item to $M = e'R$.

$\square$

Corollary 5.34. *For each idempotent $e \in R$, there is a canonical isomorphism of rings $\mathrm{End}(eR) \cong eRe$.*

Proof. Apply previous proposition (b) to get an isomorphism of abelian groups $\lambda : \mathrm{End}(eR) \to eRe$. We only have to check that λ is multiplicative: for $\theta, \theta' \in \mathrm{End}(eR)$, we get

$$\begin{aligned} \lambda(\theta\theta') = (\theta\theta')(e) &= \theta(\underbrace{\theta'(e)}_{=:m \in eR}) \\ &= \theta(m) = \theta(em) \\ &= \theta(e) \cdot m = \theta(e)\theta'(e) \\ &= \lambda(\theta)\lambda(\theta'). \end{aligned}$$

$\square$

Definition 5.35. Idempotents $\alpha, \beta \in R$ are orthogonal if $\alpha\beta = \beta\alpha = 0$.

Proposition 5.36. *For an element $0 \neq e \in R$. The following is equivalent:*

1. *eR is an indecomposable right R-module;*
2. *Re is an indecomposable left R-module;*
3. *eRe has no nontrivial idempotents;*
4. *e does not decompose as $e = \alpha + \beta$ for some nonzero orthogonal $\alpha, \beta \in R$.*

Such an idempotent is called primitive.

Proof. The points (1) and (2) are left-right symmetric, so it suffices to prove the equivalence of (1), (3) and (4). The equivalence (1) $\Leftrightarrow$ (3) is a direct consequence of the least corollary, since $\mathrm{End}(eR) \cong eRe$ is without nontrivial elements iff eR is indecomposable. For (4) $\Rightarrow$ (3), suppose that $\alpha \in eRe$ is a nontrivial idempotent. Then $\beta := e - \alpha$ is its complementary idempotent in eRe, thus $\alpha\beta = \beta\alpha = 0$ and $e = \alpha + \beta$. Lastly, we prove (3) $\Rightarrow$ (4). Let $e = \alpha + \beta$ for orthogonal idempotents $\alpha, \beta \neq 0$. Then

$$e\alpha = (\alpha + \beta)\alpha = \alpha^2 + \beta\alpha = \alpha$$

and

$$\alpha e = \alpha(\alpha + \beta) = \alpha^2 + \alpha\beta = \alpha$$

imply that $\alpha \in eRe$ is a nontrivial idempotent. □

Corollary 5.37. *For an idempotent $0 \neq e \in R$, the following is equivalent:*

1. *eR is a strongly indecomposable right R-module;*
2. *Re is a strongly indecomposable left R-module;*
3. *eRe is a local ring.*

Such an idempotent is called local.

Remark. Every local idempotent is primitive.

Proof. The module eR is strongly indecomposible iff $\mathrm{End}(eR) \cong eRe$ is a local ring. Equivalence between (1) and (2) is, again, due to symmetry. □

Theorem 5.38.

Suppose $e \in R$ is an idempotent and $J := \operatorname{rad} R$. Then

1. $\operatorname{rad}(eRe) = J \cap eRe = eJe$;
2. $eRe / \operatorname{rad}(eRe) \cong \overline{e}\overline{R}\overline{e}$.

Proof. 1. First, we prove that if $r \in \operatorname{rad}(eRe)$, then $r \in J$. It suffices to show that $1 - yr$ has aleft inverse for an arbitrary $y \in R$. From $r \in \operatorname{rad}(eRe)$ it follows that there exists $b \in eRe$ such that $b(e - eyer) = e$. But since $b, y \in eRe$, we have $b(1 - yr) = e$ and

$$yrb(1 - yr) = yre = yr.$$

Adding $(1-yr)$ to both sides, we get

$$(yrb+1)(1-yr)=1.$$

Next, if $r \in J \cap eRe$, then $r = ere \in eJe$. Finally, we show that if $r \in eJe$, then $r \in \operatorname{rad}(eRe)$. Take any $y \in eRe$. since $r \in eJe \subseteq J$, we have an $x \in R$ such that $x(1-yr)=1$. Then

$$e = ex(1-yr)e = ex(e-yre) = exe(e-yr).$$

2. Define the map
$$eRe \to \overline{e}\overline{R}\overline{e}, \quad ere \mapsto \overline{ere}.$$
This is a surjective ring homomorphism with kernel $\operatorname{rad}(eRe)$, which implies $eRe/\operatorname{rad}(eRe) \cong \overline{e}\overline{R}\overline{e}$. □

Theorem 5.39.

Let $e \in R$ be an idempotent.

1. *If $I \subseteq eRe$ is a left ideal, then $RI \cap eRe = I$ and the map*
$$\{\text{left ideals in } eRe\} \to \{\text{left ideals in } R\}, \quad I \mapsto R \cdot I$$
is injective.
2. *If $I \lhd eRe$ is a left ideal, then $e(RIR)e = I$ and the map*
$$\{\text{ideals in } eRe\} \to \{\text{ideals in } R\}, \quad I \mapsto RIR$$
is injective.
3. *If e satisfies ReR (i.e. it is a full idempotent), then the map in (2) in onto.*

Proof. 1. Define $I_0 := RI \cap eRe \supseteq I$. Then
$$I_0 \subseteq eI_0 \subseteq eRI = eReI = I$$
and $I = I_0$.
2. From $I \lhd eRe$ it follows that
$$e(RIR)e = (eRe)I(eRe) = I.$$
3. Suppose e is a full idempotent. Let $J \lhd R$ and set $I = eJe \lhd eRe$. Then
$$RIR = R(eJe)R = (ReR)J(ReR) = RJR = J.$$ □

Corollary 5.40. *Let $e \neq 0$ be an idempotent in R. If R is J-semisimple, semisimple, left/right noetherian or left/right artinian, then so is eRe.*

Example 5.41. *Let A be a ring, $R = M_n(A)$ and $e = E_{11}$ an idempotent. It is easy to see that $ReR = R$, so e is full. Furthermore, $eRe = A$. As a result, all ideals of R are of the form RIR, where $I \lhd A$.*

Remark. 1. Mod_R and $\operatorname{Mod}_{M_n(R)}$ are equivalent categories.

2. Suppose $e \in R$ is a full idempotent. Then Mod_R and Mod_{eRe} are equivalent categories.

3. If Mod_R is equivalent to Mod_S, then $S = eM_n(R)e$ for some $n \in \mathbb{N}$ and a full idempotent $e \in M_n(R)$.

Theorem 5.42.

Suppose $I \lhd R$ is nil and $a \in R$ is such that $\overline{a} = a + I \in R/I$ is idempotent. Then there exists an idempotent $e \in aR$ such that $\overline{e} = \overline{a}$.

Proof. Suppose $b := 1 - a$. Then $ab = ba = a - a^2 \in I$ since $\overline{a}$ is an idempotent. Since I is nil, there exists $m \in \mathbb{N}$ such that $(ab)^m = 0$. Consider

$$\begin{aligned} 1 = (a+b)^{2m} &= \sum_{k=0}^{2m} \binom{2m}{k} a^k b^{2m-k} \\ &= \underbrace{a^{2m} + \binom{2m}{1} a^{2m-1}b + \cdots + \binom{2m}{m} a^m b^m}_{e} \\ &\quad + \underbrace{\binom{2m}{m-1} a^{m-1}b^{m+1} + \cdots + \binom{2m}{2m-1} ab^{2m-1} + b^{2m}}_{f}. \end{aligned}$$

Then $e \in aR$ and $ef = 0$ since $(ab)^m = 0$ and a, b commute. As a result,

$$e = e \cdot 1 = e(e+f) = e^2 + ef = e^2$$

is an idempotent. Finally,

$$e \equiv a^{2m} \equiv a^{2m-1} \equiv \cdots \equiv a(\mod I).$$ □

5.6 Block decomposition

If $R = I \oplus J$ for ideals $I, J \lhd R$, then $1 = e + f \in I + J$ and $e, f \in Z(R)$ are central idempotents. Then $I = eR$, $J = fR$ and $R \cong eR \times fR$ is decomposable.

Definition 5.43. An element $c \in R$ is a centrally primitive idempotent if it is a central idempotent that cannot be written as a sum of two nonzero orthogonal central idempotents.

If $c = \alpha + \beta \in Z(R)$ is an idempotent and α, β are orthogonal central idempotents, then $c \cdot \alpha = (\alpha + \beta)\alpha = \alpha^2 + \beta\alpha = \alpha$, so $\alpha, \beta \in cR$.

Proposition 5.44. *Suppose $1 \in R$ decomposes as $1 = c_1 + \cdots + c_r$, where c_j are orthogonal centrally primitive idempotents.*

1. *Every central idempotent $c \in R$ is of the form $c = \sum_{i \in I} c_i$ for some $I \subseteq \{1, 2, \ldots, r\}$.*
2. *The elements $c_1, \ldots, c_r$ are the only centrally primitive idempotents. In particular, any two centrally primitive idempotents are orthogonal.*
3. *The decomposition $1 = c_1 + \cdots + c_r$ as a sum of orthogonal centrally primitive idempotents is unique.*

Proof. It suffices to prove (1). Take any i so that $c \cdot c_i \neq 0$ (by assumption, there must exist at least one). Since c_i is centrally primitive, it is the only central nontrivial idempotent in Rc_i (mimicking

the proof of (4) ⇒ (3) in 5.36). This implies that $c \cdot c_i = c_i$ and

$$c = c \cdot 1 = c \cdot \sum c_i = \sum cc_i = \sum_{i \in I} c_i. \qquad \square$$

If such a decomposition $1 = c_1 + \cdots + c_r$ exists, then

$$R = c_1 R \times \cdots \times c_r R$$

is a block decomposition.

Theorem 5.45.

If R is left noetherian or left artinian, then such a block decomposition exists.

Proof. Same as in Krull-Schmidt. $\square$

6 Free algebras and polynomial identities

6.1 Basic definitions

Take a nonempty set $X = \{x_i \mid i \in I\}$ of variables. A finite sequence of its elements $x_{i_1} x_{i_2} \dots x_{i_r}$ is a word (an empty sequence is 1). Then we denote $\langle X \rangle$ as the set of all words. We define multiplication by concatenating words:

$$(x_{i_1} \dots x_{i_r}) \cdot (x_{j_1} \dots x_{j_s}) = x_{i_1} \dots x_{i_r} x_{j_1} \dots x_{j_s}.$$

Then $\langle X \rangle$ becomes a monoid: in fact, it is a free monoid on X (i.e. a free object in Mon). Simplifying the notation a bit, we see that every $w \in \langle X \rangle$ can be written as

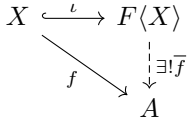
$$w = x_{i_1}^{k_1} x_{i_2}^{k_2} \dots x_{i_r}^{k_r},$$

where $k_j \in \mathbb{N}$, $i_j \in I$ and $i_j \neq i_{j+1}$.

Definition 6.1. Let F be a field and $X \neq 0$. The free algebra on X over F (denote it $F\langle X \rangle$) is the monoid algebra of $\langle X \rangle$ over F. Its elements are noncommutative polynomials.

Remark. We can also form $R\langle X \rangle$ for a ring R.

The free algebra $F\langle X \rangle$ satisfies the following universal property: for any F-algebra A, the homomorphisms $F\langle X \rangle \to A$ are uniquely determined by its image of X. Conversely, any function $X \xrightarrow{f} A$ extends uniquely to a homomorphism $F\langle X \rangle \to A$. We say that $F\langle X \rangle$ is the free object in Alg_F.



Noncommutative polynomials can be evaluated in algebras. Suppose $f \in F\langle X \rangle$, where $f = f(x_{i_1}, \dots, x_{i_m})$. If A is an F-algebra and $a_1, \dots, a_{\in} A$, then $f(a_1, \dots, a_m)$ is the element of A obtained by replacing variable x_{i_j} with a_j. We call a monomial a scalar multiple of of a word, i.e. $\lambda \cdot w$ for $\lambda \in F$ and $w \in \langle X \rangle$. Every nonzero polynomial is a unique sum of monomials $f = \lambda_1 w_1 + \cdots + \lambda_s w_s$, where $w_j \in \langle X \rangle$ are distinct and $\lambda_j \in F$ are nonzero. The degree of a word $w = x_{i_1} \dots x_{i_m}$ is $\deg(w) = m$. It follows that $\deg(1) = 0$ and $\deg(0) := -\infty$. The degree of a polynomial $f = \lambda_1 w_1 + \cdots + \lambda_s w_s$ is $\deg f = \max_{j=1,\dots,s} \deg w_j$. If $\deg w_1 = \cdots = \deg w_s$, then f is homogenous. Additionally, f is

multilinear if each variable $x_1, \ldots, x_n$ appears in every monomial of $f = f(x_1, \ldots, x_n)$ exactly once. Equivalently, f is multilinear if

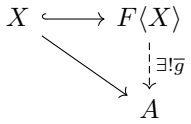
$$f = \sum_{\sigma \in S_n} \lambda_\sigma x_{\sigma(1)} \ldots x_{\sigma(n)}.$$

It is trivial to check that $\deg(fg) = \deg(f) + \deg(g)$. A direct corollary is that $F\langle X \rangle$ has no zero divisors and is therefore a domain.

Remark. As a ring, $F\langle X \rangle$ is primitive if $|X| \geq 2$.

6.2 Algebras defined by generators and relations

Let A be an F-algebra and $X \subseteq A$ any generating set. Consider $F\langle X \rangle$. Then



where g is onto. Hence $A \cong F\langle X \rangle / I$ for $I = \ker g \lhd F\langle X \rangle$. We have shown that every algebra is the quotient of a free algebra. Given $S \subseteq F\langle X \rangle$, we can construct $F\langle X \rangle / (S)$. If $S = \{f_j = f_j(x_{i_1}, \ldots, x_{i_{k_j}}) \mid j \in J\}$, then we can write $F\langle X \rangle / (S)$ as

$$F\langle x_i, i \in I \mid f_j(x_{i_1}, \ldots, x_{i_{k_j}}),\ j \in J \rangle.$$

This is an algebra defined by the generators $x_i,\ i \in I$ for and relations $f_j,\ j \in J$.

Example 6.2. *Let*

$$A = F\langle x, y \mid x^2 = 0, y^2 = 0, xy + yx = 1 \rangle.$$

Since $xyx = x$ and $yxy = y$, this algebra is spanned by $\{1, x, y, xy\}$ and so its dimension is at most 4. It turns out that $A \cong M_2(F)$ by mapping $x \mapsto E_{12}$ and $y \mapsto E_{21}$.

Example 6.3. *The exterior (Grassman) algebra is*

$$G := F\langle x_i, i \in \mathbb{N} \mid x_i^2 = 0, x_i x_j + x_j x_i = 0,\ \forall i, j \in \mathbb{N} \rangle.$$

First, notice that $x_1 x_2 x_1 = -x_1^2 x_2 = 0$. More generally, $x_i G x_i = (0)$. Therefore, G is spanned by 1 and all sorted words. We can prove that this is also a basis for G. Indeed, suppose $\sum_{i=1}^n \lambda_i b_i = 0$, where $\lambda_i \in F$ and b_i's are either 1 or sorted words. Assume b_i's are distinct. Then there exists a $k \in \mathbb{N}$ such that x_k appears in b_n but not in b_i. Then $\sum_{i=1}^{n-1} \lambda_i b_i x_k = 0$. To complete the induction, we need to prove that all sorted words are nonzero. If $x_1 x_2 \ldots x_n = 0$, consider $F\langle y_1, y_2, \ldots \rangle$ and

$$I = \langle y_i^2, y_i y_j + y_j y_i \mid i, j \in \mathbb{N} \rangle \lhd F\langle y_1, y_2, \ldots \rangle.$$

Hence $G = \frac{F\langle y_1, y_2, \ldots \rangle}{I}$. Since $y_1 \ldots y_n \in I$, so $y_1 \ldots y_n$ is a sum of terms of the form $m y_i^2 m'$ and $q(y_i y_j + y_j y_i) q'$ for monomials m, m', q, q'. Since a linear combination of non-multilinear monomials is a non-multilinear polynomial, so $y_1 \ldots y_n \in I$ is a linear combination of the polynomials of the form

$$y_{\sigma(1)} \cdots y_{\sigma(j-1)} (y_{\sigma(j)} y_{\sigma(j+1)} + y_{\sigma(j+1)} y_{\sigma(j)}) y_{\sigma(j+1)} \cdots y_{\sigma(n)}$$

for $\sigma \in S_n$. In such a sum, the sum of coefficients corresponding to even permutations is the sum of coefficients corresponding to odd permutations, a contradiction. The center of the Grassman algebra is spanned by 1 and all sorted words of even length. We denote it $Z(G) := G_0$. If G_1 is the span of all odd length sorted words, then $G = G_1 \oplus G_2$ as a vector space.

6.3 Alternating polynomials

Definition 6.4. A multilinear polynomial $f = f(x_1, \dots, x_m, y_1, \dots, y_n) \in F\langle X, Y\rangle$ is alternating in $x_1, \dots, x_m$ if f becomes zero whenever one replaces x_i by x_j for $1 \leq i < j \leq m$.

If we replace x_1, x_2 by $x_1 + x_2$ in such a polynomial, then $f(x_1 + x_2, x_1 + x_2, x_3, \dots, y_n) = 0$ and so

$$f(x_1, x_2, \dots, y_n) = -f(x_2, x_1, \dots, y_n).$$

Hence f changes sign if we swap two of its x variables.

Proposition 6.5. *Let A be an F-algebra and assume that $a_1, \dots, a_m \in A$ are linearly dependent. If $f = f(x_1, \dots, x_m, y_1, \dots, y_n)$ is alternating in $x_1, \dots, x_m$, then*

$$f(a_1, \dots, a_m, b_1, \dots, b_n) = 0, \quad \forall b_j \in A.$$

Proof. WLOG $a_m = \sum_{i=1}^{m-1} \lambda_i a_i$ for some $\lambda_i \in F$. Then

$$f(a_1, \dots, a_m, b_1, \dots, b_n) = \sum_{i=1}^{m-1} \lambda_i f(a_1, \dots, a_{m-1}, a_i, b_1, \dots, b_n) = 0. \qquad \square$$

Example 6.6. *For $n \geq 2$ let*

$$s_n = s_n(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) x_{\sigma(1)} \dots x_{\sigma(n)}$$

define the standard polynomial of degree n. For $n = 2$, $s_2 = [x_1, x_2]$ and for $n = 3$, $s_3 = h(x_1, x_2, x_3, 1)$ with the above notation. For every $n \in \mathbb{N}$, s_n is alternating in all of its variables.

Example 6.7. *For $n \geq 2$ let*

$$c_n(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) x_{\sigma(1)} y_1 x_{\sigma(2)} y_2 \dots y_{n-1} x_{\sigma(n)}$$

be th n-th Capelli polynomial. It is alternating in $x-1, \dots, x_n$ and satisfies the following identities:

- $c_n(x_1, \dots, x_n, 1, \dots, 1) = s_n(x_1, \dots, x_n)$;
- $c_n = \sum_{i=1}^{n} (-1)^{i-1} x_i y_1 c_{n-1}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n, y_2, \dots, y_{n-1})$ *for $n \geq 3$;*
- $c_n = \sum_{i=1}^{n-1} (-1)^{i-1} x_i s_{n-1}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ *for $n \geq 3$.*

6.4 Polynomial identities (PI)

Definition 6.8. A polynomial $f = f(x_1, \dots, x_n) \in F\langle X\rangle$ is a PI of an F-algebra A if $f(a_1, \dots, a_n) = 0$ for all $a_j \in A$. We also say that A satisfies f. Furthermore, A is a PI-algebra if there exists $f \in F\langle X\rangle \setminus \{0\}$ that is a PI of A.

Example 6.9. *Commutative algebras are PI-algebras: A is commutative iff A satisfies the identity $[x_1, x_2]$.*

Example 6.10. *Every finite-dimensional algebra A is a PI-algebra. Suppose $[A : F] = d$. Then every polynomial alternating in $d + 1$ variables is a PI of A. In particular, A satisfies S_{d+1}. For example $M_n(F)$ satisfies S_{n^2+1}, so it is a PI-algebra. If C is a commutative F-algebra, then $M_n(C)$ is a PI-algebra.*

Example 6.11. *Consider the Grassman algebra G. We prove that for all $f, g \in G$, we have $[f, g] \in G_0 = Z(G)$. WLOG let f, g be words*