Leandro Vendramin

Associative algebras

Notes

Monday 21st November, 2022

Preface

The notes correspond to the master course *Associative Algebra* of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences. The course is divided into twelve or thirteen two-hours lectures.

The material is heavily based on [2], [5] and [14].

Prerequisites: An undergraduate "abstract algebra" course. See for example my notes on Rings and modules.

This version was compiled on Monday 21$^{\text{st}}$ November, 2022 at 10:59. Please send comments and corrections to me at `Leandro.Vendramin@vub.be`.

Leandro Vendramin
Brussels, Belgium

Contents

List of topics

Lecture 1

§1. Semisimple algebras

We will devote two lectures to the study of finite-dimensional semisimple algebras. The main goal is to prove Artin–Wedderburn theorem.

Definition 1.1. An **algebra** (over the field K) is a vector space (over K) with an associative multiplication $A \times A \to A$ such that $a(\lambda b + \mu c) = \lambda(ab) + \mu(ac)$ and $(\lambda a + \mu b)c = \lambda(ac) + \mu(bc)$ for all $a, b, c \in A$, and that contains an element $1_A \in A$ such that $1_A a = a 1_A = a$ for all $a \in A$.

Note that an algebra over K is a ring A that is a vector space (over K) such that the map $K \to A$, $\lambda \mapsto \lambda 1_A$, is injective.

Definition 1.2. An algebra A is **commutative** if $ab = ba$ for all $a, b \in A$.

The **dimension** of an algebra A is the dimension of A as a vector space. This is why we want to consider algebras, as they are a linear version of rings. Often, our arguments will use the dimension of the underlying vector space.

Example 1.3. The field $\mathbb{R}$ is a real algebra and $\mathbb{C}$ is a complex algebra. Moreover, $\mathbb{C}$ is a real algebra.

Any field K is an algebra over K.

Example 1.4. If K is a field, then $K[X]$ is an algebra over K.

Similarly, the polynomial ring $K[X, Y]$ and the ring $K[[X]]$ of power series are examples of algebra over K.

Example 1.5. If A is an algebra, then $M_n(A)$ is an algebra.

Example 1.6. The set of continuous maps $[0, 1] \to \mathbb{R}$ is a real algebra with the usual point-wise operations $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$.

Example 1.7. Let $n \in \mathbb{Z}_{>0}$. Then $K[X]/(X^n)$ is a finite-dimensional algebra. It is the **truncated polynomial algebra**.

Example 1.8. Let G be a finite group. The vector space $\mathbb{C}[G]$ with basis $\{g : g \in G\}$ is an algebra with multiplication

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{h\in G} \mu_h h\right) = \sum_{g,h\in G} \lambda_g \mu_h (gh).$$

Note that $\dim \mathbb{C}[G] = |G|$ and $\mathbb{C}[G]$ is commutative if and only G is abelian. This is the **complex group algebra** of G.

If G is an infinite group, the complex group algebra $\mathbb{C}[G]$ is defined as the set of finite linear combinations of elements of G with the usual operations.

Definition 1.9. An algebra **homomorphism** is a ring homomorphism $f\colon A \to B$ that is also a linear map.

The complex conjugation map $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$, is a ring homomorphism that is not an algebra homomorphism over $\mathbb{C}$.

Exercise 1.10. Let G be a non-trivial finite group. Then $\mathbb{C}[G]$ has zero divisors.

If A is an algebra, then $\mathcal{U}(A)$ is the set of units of A.

Exercise 1.11. Let A be a K-algebra and G be a finite group. If $f\colon G \to \mathcal{U}(A)$ is a group homomorphism, then there exists an algebra homomorphism $\varphi\colon K[G] \to A$ such that $\varphi|_G = f$.

Definition 1.12. An **ideal** of an algebra is an ideal of the underlying ring.

Similarly, one defines left and right ideals of an algebra.

If A is an algebra, then every left ideal of the ring A is a vector space. Indeed, if I is a left ideal of A and $\lambda \in K$ and $x \in I$, then

$$\lambda x = \lambda(1_A x) = (\lambda 1_A)x.$$

Since $\lambda 1_A \in A$, it follows that $\lambda I = (\lambda 1_A)I \subseteq I$. Similarly, every right ideal of the ring A is a vector space.

If A is an algebra and I is an ideal of A, then the quotient ring A/I has a unique algebra structure such that the canonical map $A \to A/I$, $a \mapsto a + I$, is a surjective algebra homomorphism with kernel I.

Definition 1.13. Let A be an algebra over the field K. An element $a \in A$ is **algebraic** over K if there exists a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$.

If every element of A is algebraic, then A is said to be algebraic

In the algebra $\mathbb{R}$ over $\mathbb{Q}$, the element $\sqrt{2}$ is algebraic, as $\sqrt{2}$ is a root of the polynomial $X^2 - 2 \in \mathbb{Q}[X]$. A famous theorem of Lindemann proves that π is not algebraic over $\mathbb{Q}$. Every element of the real algebra $\mathbb{R}$ is algebraic.

Proposition 1.14. *Every finite-dimensional algebra is algebraic.*

Proof. Let A be an algebra with $\dim A = n$ and let $a \in A$. Since $\{1, a, a^2, \dots, a^n\}$ has $n+1$ elements, it is a linearly dependent set. Thus there exists a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$. $\square$

Definition 1.15. A **module** over an algebra A is a module over the ring A.

Similarly, one defines submodules and module homomorphisms. It is a straightforward exercise to prove the isomorphism theorems.

Example 1.16. If V is a module over an algebra A, one defines $\mathrm{End}_A(V)$ as the set of module homomorphisms $V \to V$. The set $\mathrm{End}_A(V)$ is indeed an algebra with

$$(f+g)(v) = f(v) + g(v), \quad (\lambda f)(v) = \lambda f(v) \quad \text{and} \quad (fg)(v) = f(g(v))$$

for all $f, g \in \mathrm{End}_A(V)$, $\lambda \in K$ and $v \in V$.

Let A be a finite-dimensional algebra. If M is a module over the ring A, then M is a vector space with

$$\lambda m = (\lambda 1_A) \cdot m,$$

where $\lambda \in K$ and $m \in M$. Moreover, M is finitely generated if and only if M is finite-dimensional.

Example 1.17. An algebra A is a module over A with left multiplication, that is $a \cdot b = ab$, $a, b \in A$. This module is the (left) **regular representation** of A and it will be denoted by ${}_AA$.

Definition 1.18. Let A be an algebra and M be a module over A. Then M is **simple** if $M \neq \{0\}$ and $\{0\}$ and M are the only submodules of M.

Definition 1.19. Let A be a finite-dimensional algebra and M be a finite-dimensional module over A. Then M is **semisimple** if M is a direct sum of finitely many simple submodules.

A finite direct sum of semisimples is semisimple.

Lemma 1.20 (Schur). *Let A be an algebra. If S and T are simple modules and $f \colon S \to T$ is a non-zero module homomorphism, then f is an isomorphism.*

Proof. Since $f \neq 0$, $\ker f$ is a proper submodule of S. Since S is simple, it follows that $\ker f = \{0\}$. Similarly, $f(S)$ is a non-zero submodule of T and hence $f(S) = T$, as T is simple. $\square$

Proposition 1.21. *If A is a finite-dimensional algebra and S is a simple module, then S is finite-dimensional.*

Proof. Let $s \in S \setminus \{0\}$. Since S is simple, $\varphi \colon A \to S$, $a \mapsto a \cdot s$, is a surjective module homomorphism. In particular, by the first isomorphism theorem, $A/\ker\varphi \simeq S$ and hence $\dim S = \dim(A/\ker\varphi) \leq \dim A$. $\square$

Proposition 1.22. *Let M be a finite-dimensional module. The following statements are equivalent.*

1) *M is semisimple.*
2) *$M = \sum_{i=1}^{k} S_i$, where each S_i is a simple submodule of M.*
3) *If S is a submodule of M, then there is a submodule T of M such that $M = S \oplus T$.*

Proof. We first prove that 2) $\implies$ 3). Let $N \neq \{0\}$ be a submodule of M. Since $N \neq \{0\}$ and $\dim M < \infty$, there exists a submodule T of M of maximal dimension such that $N \cap T = \{0\}$. If $S_i \subseteq N \oplus T$ for all $i \in \{1, \dots, k\}$, then, as M is the sum of the S_i, it follows that $M = N \oplus T$. If, however, there exists $i \in \{1, \dots, k\}$ such that $S_i \not\subseteq N \oplus T$, then $S_i \cap (N \oplus T) \subsetneq S_i$. Since the module S_i is simple, it follows that $S_i \cap (N \oplus T) = \{0\}$. Thus $N \cap (S_i \oplus T) = \{0\}$, a contradiction to the maximality of $\dim T$.

The implication 1) $\implies$ 2) is trivial.

Finally, we prove that 3) $\implies$ 1). We proceed by induction on $\dim M$. The result is clear if $\dim M = 1$. Assume that $\dim M \geq 2$ and let S be a non-zero submodule of M of minimal dimension. In particular, S is simple. By assumption, there exists a submodule T of M such that $M = S \oplus T$. We claim that T satisfies the assumptions. If X is a submodule of T, then, since T is also a submodule of M, there exists a submodule Y of M such that $M = X \oplus Y$. Thus

$$T = T \cap M = T \cap (X \oplus Y) = X \oplus (T \cap Y),$$

as $X \subseteq T$. Since $\dim T < \dim M$ and $T \cap Y$ is a submodule of T, the inductive hypothesis implies that T is a direct sum of simple submodules. Hence M is a direct sum of simple submodules. □

Proposition 1.23. *If M is a semisimple module and N is a submodule, then N and M/N are semisimple.*

Proof. Assume that $M = S_1 + \cdots + S_k$, where each S_i is a simple submodule. If $\pi \colon M \to M/N$ is the canonical map, Schur's lemma implies that each restriction $\pi|_{S_i}$ is either zero or an isomorphism with the image. Since

$$M/N = \pi(M) = \sum_{i=1}^{k} (\pi|_{S_i})(S_i),$$

it follows that M/N is a direct sum of finitely many simples.

We now prove that N is semisimple. By assumption, there exists a submodule T such that $M = N \oplus T$. The quotient M/T is semisimple by the previous paragraph, so it follows that

$$N \simeq N/\{0\} = N/(N \cap T) \simeq (N \oplus T)/T = M/T$$

is also semisimple. □

Lecture 2

Definition 1.24. An algebra A is **semisimple** if every finitely generated A-module is semisimple.

Proposition 1.25. *Let A be a finite-dimensional algebra. Then A is semisimple if and only if the regular representation of A is semisimple.*

Proof. Let us prove the non-trivial implication. Let M be a finitely generated module, say $M = (m_1, \dots, m_k)$. The map

$$\bigoplus_{i=1}^{k} A \to M, \quad (a_1, \dots, a_k) \mapsto \sum_{i=1}^{k} a_i \cdot m_i,$$

is a surjective homomorphism of modules, where A is considered as a module with the regular representation. Since A is semisimple, it follows that $\oplus_{i=1}^{k} A$ is semisimple. Thus M is semisimple, as it is isomorphic to the quotient of a semisimple module. □

Theorem 1.26. *Let A be a finite-dimensional semisimple algebra. Assume that the regular representation can be decomposed as ${}_A A = \oplus_{i=1}^{k} S_i$ where each S_i is a simple submodule. If S is a simple module, then $S \simeq S_i$ for some $i \in \{1, \dots, k\}$.*

Proof. Let $s \in S \setminus \{0\}$. The map $\varphi \colon A \to S$, $a \mapsto a \cdot s$, is a surjective module homomorphism. Since $\varphi \neq 0$, there exists $i \in \{1, \dots, k\}$ such that some restriction $\varphi|_{S_i} \colon S_i \to S$ is non-zero. By Schur's lemma, it follows that $\varphi|_{S_i}$ is an isomorphism. □

As a corollary, a finite-dimensional semisimple algebra admits only finitely many isomorphism classes of simple modules. When we say that the $S_1, \dots, S_k$ are the simple modules of an algebra, this means that the S_i are the representatives of isomorphism classes of all simple modules of the algebra, that is that each simple module is isomorphic to some S_i and, moreover, $S_i \not\simeq S_j$ whenever $i \neq j$.

Exercise 1.27. If A and B are algebras, M is a module over A and N is a module over B, then $M \oplus N$ is a module over $A \times B$ with

$$(a, b) \cdot (m, n) = (a \cdot m, b \cdot n).$$

A **division algebra** D is an algebra such that every non-zero element is invertible, that is for all $x \in D \setminus \{0\}$ there exists $y \in D$ such that $xy = yx = 1$. Modules over division algebras are very much like vector spaces. For example, every finitely generated module M over a division algebra has a basis. Moreover, every linearly independent subset of M can be extended into a basis of M.

Proposition 1.28. *Let D be a division algebra, and V be a finitely generated module over D. Then V is a simple module over* $\operatorname{End}_D(V)$ *and there exits $n \in \mathbb{Z}_{>0}$ such that* $\operatorname{End}_D(V) \simeq nV$ *is semisimple.*

Sketch of the proof. Let $\{v_1, \dots, v_n\}$ be a basis of V. A direct calculation shows that the map

$$\operatorname{End}_D(V) \to \bigoplus_{i=1}^{n} V = nV, \quad f \mapsto (f(v_1), \dots, f(v_n)),$$

is an injective homomorphism of $\operatorname{End}_D(V)$-modules. Since

$$\dim \operatorname{End}_D(V) = n^2 = \dim(nV),$$

it follows that the map is an isomorphism. Thus

$$\operatorname{End}_D(V) \simeq \bigoplus_{i=1}^{n} V.$$

It remains to show that V is simple. It is enough to prove that $V = (v)$ for all $v \in V \setminus \{0\}$. Let $v \in V \setminus \{0\}$. If $w \in V$, then there exists $f \in \operatorname{End}_D(V)$ such that $f \cdot v = f(v) = w$. Thus $w \in (v)$ and therefore $V = (v)$. □

The proposition states that if D is a division algebra, then D^n is a simple $M_n(D)$-module and that $M_n(D) \simeq nD^n$ as $M_n(D)$-modules.

Exercise 1.29. Let M, N, and X be modules. Prove that

$$\operatorname{Hom}_A(M \oplus N, X) \simeq \operatorname{Hom}_A(M, X) \times \operatorname{Hom}_A(N, X). \tag{2.1}$$

Theorem 1.30. *Let A be a finite-dimensional algebra and let $S_1, \dots, S_k$ be the simple modules over A. If*

$$M \simeq n_1 S_1 \oplus \cdots \oplus n_k S_k,$$

then each n_j is uniquely determined.

Proof. Since each S_j is simple and $S_i \not\simeq S_j$ if $i \neq j$, Schur's lemma implies that $\operatorname{Hom}_A(S_i, S_j) = \{0\}$ whenever $i \neq j$. For each $j \in \{1, \dots, k\}$, routine calculations show that

$$\operatorname{Hom}_A(M, S_j) \simeq \operatorname{Hom}_A\left(\bigoplus_{i=1}^{k} n_i S_i, S_j\right) \simeq n_j \operatorname{Hom}_A(S_j, S_j).$$

Since M and S_j are finite-dimensional vector spaces, it follows that $\mathrm{Hom}_A(M,S_j)$ and $\mathrm{Hom}_A(S_j,S_j)$ are both finite-dimensional vector spaces. Moreover, the identity $\mathrm{id}\colon S_j \to S_j$ is a module homomorphism and hence $\dim \mathrm{Hom}_A(S_j,S_j) \geq 1$. Thus each n_j is uniquely determined, as

$$n_j = \frac{\dim \mathrm{Hom}_A(M,S_j)}{\dim \mathrm{Hom}_A(S_j,S_j)}. \qquad \square$$

If A is an algebra, the **opposite algebra** A^{op} is the vector space A with multiplication $A \times A \to A$, $(a,b) \mapsto ba = a \cdot_{\mathrm{op}} b$. Clearly, A is commutative if and only if $A = A^{\mathrm{op}}$.

Lemma 1.31. *If A is an algebra, then $A^{\mathrm{op}} \simeq \mathrm{End}_A(A)$ as algebras.*

Proof. Note that $\mathrm{End}_A(A) = \{\rho_a : a \in A\}$, where $\rho_a\colon A \to A$, $x \mapsto xa$. Indeed, if $f \in \mathrm{End}_A(A)$, then $f(1) = a \in A$. Moreover, $f(b) = f(b1) = bf(1) = ba$ and hence $f = \rho_a$. The map $A^{\mathrm{op}} \to \mathrm{End}_A(A)$, $a \mapsto \rho_a$, is bijective and it is an algebra homomorphism, as

$$\rho_a\rho_b(x) = \rho_a(\rho_b(x)) = \rho_a(xb) = x(ba) = \rho_{ba}(x). \qquad \square$$

Lemma 1.32. *If A is an algebra and $n \in \mathbb{Z}_{>0}$, then $M_n(A)^{\mathrm{op}} \simeq M_n(A^{\mathrm{op}})$ as algebras.*

Proof. Let $\psi\colon M_n(A)^{\mathrm{op}} \to M_n(A^{\mathrm{op}})$, $X \mapsto X^T$, where X^T is the transpose matrix of X. Since ψ is a bijective linear map, it is enough to see that ψ is a homomorphism. If $i,j \in \{1,\dots,n\}$, $a = (a_{ij})$ and $b = (b_{ij})$, then

$$\begin{aligned}(\psi(a)\psi(b))_{ij} &= \sum_{k=1}^n \psi(a)_{ik}\psi(b)_{kj} = \sum_{k=1}^n a_{ki} \cdot_{\mathrm{op}} b_{jk} \\ &= \sum_{k=1}^n b_{jk}a_{ki} = (ba)_{ji} = ((ba)^T)_{ij} = \psi(a \cdot_{\mathrm{op}} b)_{ij}. \qquad \square\end{aligned}$$

Lemma 1.33. *If S is a simple module and $n \in \mathbb{Z}_{>0}$, then*

$$\mathrm{End}_A(nS) \simeq M_n(\mathrm{End}_A(S))$$

as algebras.

Proof. Let (φ_{ij}) be a matrix with entries in $\mathrm{End}_A(S)$. We define a map $nS \to nS$ as follows:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \dots & \ddots & \vdots \\ \varphi n1 & \cdots & \varphi_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \varphi_{11}(x_1) + \cdots + \varphi_{1n}(x_n) \\ \vdots \\ \varphi_{n1}(x_1) + \cdots + \varphi_{nn}(x_n) \end{pmatrix}.$$

The reader should prove that the map

$$M_n(\mathrm{End}_A(S)) \to \mathrm{End}_A(nS)$$

is an injective algebra homomorphism. It is surjective. Indeed, if $\psi \in \operatorname{End}_A(nS)$ and $i, j \in \{1, \dots, n\}$ one defines ψ_{ij} by

$$\psi \begin{pmatrix} x \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \psi_{11}(x) \\ \psi_{21}(x) \\ \vdots \\ \psi_{n1}(x) \end{pmatrix}, \dots, \psi \begin{pmatrix} 0 \\ 0 \\ \vdots \\ x \end{pmatrix} = \begin{pmatrix} \psi_{1n}(x) \\ \psi_{2n}(x) \\ \vdots \\ \psi_{nn}(x) \end{pmatrix}. \qquad \square$$

Exercise 1.34. Let M, N, and X be modules. Prove that

$$\operatorname{Hom}_A(X, M \oplus N) \simeq \operatorname{Hom}_A(X, M) \times \operatorname{Hom}_A(X, N). \tag{2.2}$$

Theorem 1.35 (Artin–Wedderburn). *Let A be a finite-dimensional semisimple algebra with k isomorphism classes of simple modules. Then*

$$A \simeq M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

for some $n_1, \dots, n_k \in \mathbb{Z}_{>0}$ and some division algebras $D_1, \dots, D_k$.

Proof. Decompose the regular representation as a sum of simple modules and gather the simples by isomorphism classes to get

$$A = \bigoplus_{i=1}^{k} n_i S_i,$$

where each S_i is simple and $S_i \not\simeq S_j$ whenever $i \neq j$. Schur's lemma implies that

$$\operatorname{End}_A(A) \simeq \operatorname{End}_A\left(\bigoplus_{i=1}^{k} n_i S_i\right) \simeq \prod_{i=1}^{k} \operatorname{End}_A(n_i S_i) \simeq \prod_{i=1}^{k} M_{n_i}(\operatorname{End}_A(S_i)),$$

where each $D_i = \operatorname{End}_A(S_i)$ is a division algebra. Thus

$$\operatorname{End}_A(A) \simeq \prod_{i=1}^{k} M_{n_i}(D_i).$$

Since $\operatorname{End}_A(A) \simeq A^{\mathrm{op}}$, it follows that

$$A = (A^{\mathrm{op}})^{\mathrm{op}} \simeq \prod_{i=1}^{k} M_{n_i}(D_i)^{\mathrm{op}} \simeq \prod_{i=1}^{k} M_{n_i}(D_i^{\mathrm{op}}).$$

Since each D_i is a division algebra, each D_i^{op} is also a division algebra. $\square$

Corollary 1.36 (Mollien). *If A is a finite-dimensional complex semisimple algebra with k isomorphism classes of simple modules, then*

$$A \simeq \prod_{i=1}^{k} M_{n_i}(\mathbb{C})$$

for some $n_1, \dots, n_k \in \mathbb{Z}_{>0}$.

Proof. By Wedderburn's theorem,

$$A \simeq \prod_{i=1}^{k} M_{n_i}(\operatorname{End}_A(S_i)^{\mathrm{op}}),$$

where $S_1, \dots, S_k$ are representatives of the isomorphism classes of simple modules and each $\operatorname{End}_A(S_i)$ is a division algebra. We claim that

$$\operatorname{End}_A(S_i) = \{\lambda \operatorname{id} : \lambda \in \mathbb{C}\} \simeq \mathbb{C}$$

for all $i \in \{1, \dots, k\}$. If $f \in \operatorname{End}_A(S_i)$, then f has an eigenvalue $\lambda \in \mathbb{C}$. Since $f - \lambda \operatorname{id}$ is not an isomorphism, Schur's lemma implies that $f - \lambda \operatorname{id} = 0$, that is $f = \lambda \operatorname{id}$. Thus $\operatorname{End}_A(S_i) \longrightarrow \mathbb{C}$, $f \mapsto \lambda$, is an algebra isomorphism. In particular,

$$A \simeq \prod_{i=1}^{k} M_{n_i}(\mathbb{C}). \qquad \square$$

Maschke's theorem states that, if G is a finite group, then the group algebra $\mathbb{C}[G]$ is semisimple. By Mollien's theorem,

$$\mathbb{C}[G] \simeq \prod_{i=1}^{k} M_{n_i}(\mathbb{C}),$$

where k is the number of (isomorphism classes of) simple $\mathbb{C}[G]$-modules. Moreover,

$$|G| = \dim \mathbb{C}[G] = \sum_{i=1}^{k} n_i^2.$$

Theorem 1.37. *Let G be a finite group. The number of simple modules of $\mathbb{C}[G]$ coincides with the number of conjugacy classes of G.*

Proof. By Mollien's theorem, $\mathbb{C}[G] \simeq \prod_{i=1}^{k} M_{n_i}(\mathbb{C})$. Thus

$$Z(\mathbb{C}[G]) \simeq \prod_{i=1}^{k} Z(M_{n_i}(\mathbb{C})) \simeq \mathbb{C}^k.$$

In particular, $\dim Z(\mathbb{C}[G]) = k$. If $\alpha = \sum_{g \in G} \lambda_g g \in Z(\mathbb{C}[G])$, then $h^{-1}\alpha h = \alpha$ for all $h \in G$. Thus

$$\sum_{g \in G} \lambda_{hgh^{-1}} g = \sum_{g \in g} \lambda_g h^{-1} g h = \sum_{g \in G} \lambda_g g$$

and hence $\lambda_g = \lambda_{hgh^{-1}}$ for all $g, h \in G$. A basis for $Z(\mathbb{C}[G])$ is given by elements of the form

$$\sum_{g \in K} g,$$

where K is a conjugacy class of G. Therefore $\dim Z(\mathbb{C}[G])$ is equal to the number of conjugacy classes of G. $\square$

Example 1.38. Let $G = C_4$ be the cyclic group of order four. Then G has four simple modules and $\mathbb{C}[G] \simeq \mathbb{C}^4$.

Example 1.39. Let $G = \mathbb{S}_3$. Then G has three simple modules and

$$\mathbb{C}[G] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}).$$

Open problem 1.1 (Brauer). Which algebras are group algebras?

This question might be impossible to answer, but it is extremely interesting. Examples 1.38 and 1.39 show that $\mathbb{C}^4$ and $\mathbb{C}^2 \times M_2(\mathbb{C})$ are complex group algebras.

Exercise 1.40. Is $\mathbb{C}^2 \times M_2(\mathbb{C}) \times M_3(\mathbb{C})$ a complex group algebra?

Lecture 3

Definition 1.41. An algebra A is **simple** if $A \neq \{0\}$ and $\{0\}$ and A are the only ideals of A.

Proposition 1.42. *Let A be a finite-dimensional simple algebra. There exists a non-zero left ideal I of minimal dimension. This ideal is a simple A-module, and every simple A-module is isomorphic to I.*

Proof. Since A is finite-dimensional and A is a left ideal of A, there exists a non-zero left ideal of minimal dimension. The minimality of $\dim I$ implies that I is a simple A-module.

Let M be a simple A-module. In particular, $M \neq \{0\}$. Since

$$\operatorname{Ann}_A(M) = \{a \in A : a \cdot M = \{0\}\}$$

is an ideal of A and $1 \in A \setminus \operatorname{Ann}_A(M)$, the simplicity of A implies that $\operatorname{Ann}_A(M) = \{0\}$ and hence $I \cdot M \neq \{0\}$ (because $I \cdot m = 0$ for all $m \in M$ yields $I \subseteq \operatorname{Ann}_A(M)$ and I is non-zero, a contradiction). Let $m \in M$ be such that $I \cdot m \neq \{0\}$. The map

$$\varphi\colon I \longrightarrow M, \quad x \mapsto x \cdot m,$$

is a module homomorphism. Since $I \cdot m \neq \{0\}$, the map φ is non-zero. Since both I and M are simple, Schur's lemma implies that φ is an isomorphism. □

If D is a division algebra, then $M_n(D)$ is a simple algebra. The previous proposition implies that the algebra $M_n(D)$ has a unique isomorphism class of simple modules. Each simple module is isomorphic to D^n.

Proposition 1.43. *Let A be a finite-dimensional algebra. If A is simple, then A is semisimple.*

Proof. Let S be the sum of the simple submodules appearing in the regular representation of A. We claim that S is an ideal of A. We know that S is a left ideal, as the submodules of the regular representation are exactly the left ideals of A. To show that $Sa \subseteq S$ for all $a \in A$ we need to prove that $Ta \subseteq S$ for all simple submodule T of A and $a \in A$. If $T \subseteq A$ is a simple submodule and $a \in A$, let $f\colon T \to Ta$, $t \mapsto ta$. Since f is a surjective module homomorphism and T is simple, it follows that either $\ker f = \{0\}$ or $\ker T = T$. If $\ker T = T$, then $f(T) = Ta = \{0\} \subseteq S$. If $\ker f = \{0\}$, then $T \simeq f(T) = Ta$ and hence Ta is simple. Hence $Ta \subseteq S$.

Since S is an ideal of A and A is a simple algebra, it follows either $S = \{0\}$ or $S = A$. Since $S \neq \{0\}$, because there exists a non-zero left ideal I of A such that $I \neq \{0\}$ is of minimal dimension, it follows that $S = A$, that is, the regular representation of A is semisimple (because it is a sum of simple submodules). Therefore A is semisimple. □

Theorem 1.44 (Wedderburn). *Let A be a finite-dimensional algebra. If A is simple, then $A \simeq M_n(D)$ for some $n \in \mathbb{Z}_{>0}$ and some division algebra D.*

Proof. Since A is simple, it follows that A is semisimple. Artin–Wedderburn theorem implies that $A \simeq \prod_{i=1}^{k} M_{n_i}(D_i)$ for some $n_1, \dots, n_k$ and some division algebras $D_1, \dots, D_k$. Moreover, A has k isomorphism classes of simple modules. Since A is simple, A has only one isomorphism class of simple modules. Thus $k = 1$ and hence $A \simeq M_n(D)$ for some $n \in \mathbb{Z}_{>0}$ and some division algebra D. □

§2. Primitive rings

We will consider (possibly non-unitary) rings. Thus a **ring** is an abelian group R with an associative multiplication $(x, y) \mapsto xy$ such that $(x + y)z = xz + yz$ and $x(y+z) = xy+xz$ for all $x, y, z \in R$. If there is an element $1 \in R$ such that $x1 = 1x = x$ for all $x \in R$, we say that R is a **unitary ring**. A **subring** S of R is an additive subgroup of R closed under multiplication.

Example 2.1. $\mathbb{Z}$ is a (unitary) ring and $2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$ is a (non-unitary) ring.

A **left ideal** (resp. **right ideal**) is a subring I of R such that $rI \subseteq I$ (resp. $Ir \subseteq I$) for all $r \in R$. An **ideal** (also two-sided ideal) of R is a subring I of R that is both a left and a right ideal of R.

Example 2.2. If I and J are both ideals of R, then the sum $I+J = \{x+y : x \in I, y \in J\}$ and the intersection $I \cap J$ are both ideals of R. The product IJ, defined as the additive subgroup of R generated by $\{xy : x \in I, y \in J\}$, is also an ideal of R.

Example 2.3. If R is a ring, the set $Ra = \{xa : x \in R\}$ is a left ideal of R. Similarly, the set $aR = \{ax : x \in R\}$ is a right ideal of R. The set RaR, which is defined as the additive subgroup of R generated by $\{xay : x, y \in R\}$, is a ideal of R.

Example 2.4. Ir R is a unitary ring, then Ra is the left ideal generated by a, aR is the right ideal generated by a and RaR is the ideal generated by a. If R is not unitary, the left ideal generated by a is $Ra+\mathbb{Z}a$, the right ideal generated by a is $aR+\mathbb{Z}a$ and the ideal generated by a is $RaR+Ra+aR+\mathbb{Z}a$.

Definition 2.5. A ring R is said to be **simple** if $R^2 \neq \{0\}$ and the only ideals of R are $\{0\}$ and R.

The condition $R^2 \neq \{0\}$ is trivially satisfied in the case of rings with identity, as $1 \in R^2 = \{r_1 r_2 : r_1, r_2 \in R\}$.

Example 2.6. Division rings are simple.

Let S be a unitary ring. Recall that $M_n(S)$ is the ring of $n \times n$ square matrices with entries in S. If $A = (a_{ij}) \in M_n(S)$ y E_{ij} is the matrix such that $(E_{ij})_{kl} = \delta_{ik}\delta_{jl}$, then

$$E_{ij} A E_{kl} = a_{jk} E_{il} \tag{3.1}$$

for all $i, j, k, l \in \{1, \dots, n\}$.

Example 2.7. If D is a division ring, then $M_n(D)$ is simple.

Let R be a ring. A left R-module (or module, for short) is an abelian group M together with a map $R \times M \to M$, $(r, m) \mapsto r \cdot m$, such that

$$(r+s) \cdot m = r \cdot m + s \cdot m, \qquad r \cdot (m+n) = r \cdot m + r \cdot s, \qquad r \cdot (s \cdot m) = (rs) \cdot m$$

for all $r, s \in R$, $m, n \in M$. If R has an identity 1 and $1 \cdot m = m$ holds for all $m \in M$, the module M is said to be **unitary**. If M is a unitary module, then $M = R \cdot M$.

Exercise 2.8. Let R be a simple unitary ring.
Prove that the center $Z(R)$ of R is a field.
Prove that R is an algebra over $Z(R)$.

Definition 2.9. A module M is said to be **simple** if $R \cdot M \neq \{0\}$ and the only submodules of M are $\{0\}$ and M. If M is a simple module, then $M \neq \{0\}$.

If R is a unitary ring and M is a simple module, then M is unitary.

Lemma 2.10. *Let M be a non-zero module. Then M is simple if and only if $M = R \cdot m$ for all $0 \neq m \in M$.*

Proof. Assume that M is simple. Let $m \neq 0$. Since $R \cdot m$ is a submodule of the simple module M, either $R \cdot m = \{0\}$ or $R \cdot m = M$. Let $N = \{n \in M : R \cdot n = \{0\}\}$. Since N is a submodule of M and $R \cdot M \neq \{0\}$, $N = \{0\}$. Therefore $R \cdot m = M$, as $m \neq 0$. Now assume that $M = R \cdot m$ for all $m \neq 0$. Let L be a non-zero submodule of M and let $0 \neq x \in L$. Then $M = L$, as $M = R \cdot x \subseteq L$. □

Example 2.11. Let D be a division ring and let V be a non-zero vector space (over D). If $R = \mathrm{End}_D(V)$, then V is a simple R-module with $fv = f(v)$, $f \in R$. $v \in V$.

Example 2.12. Let $n \geq 2$. If D is a division ring and $R = M_n(D)$, then each

$$I_k = \{(a_{ij}) \in R : a_{ij} = 0 \text{ for } j \neq k\}$$

is an R-module isomorphic to D^n. Thus $M_n(D)$ is a simple ring that is not a simple $M_n(D)$-module.

Definition 2.13. A left ideal L of a ring R is said to be **minimal** if $L \neq \{0\}$ and L does not strictly contain other left ideals of R.

Similarly one defines right minimal ideals and minimal ideals.

Example 2.14. Let D be a division ring and let $R = M_n(D)$. Then $L = RE_{11}$ is a minimal left ideal.

Example 2.15. Let L be a non-zero left ideal. If $RL \neq \{0\}$, then L is minimal if and only if L is a simple R-module.

Definition 2.16. A left (resp. right) ideal L of R is said to be **regular** if there exists $e \in R$ such that $r - re \in L$ (resp. $r - er \in L$) for all $r \in R$.

If R is a ring with identity, every left (or right) ideal is regular.

Definition 2.17. A left (resp. right) ideal I of R is said to be **maximal** if $I \neq R$ and I is not properly contained in any other left (resp. right) ideal of R.

Similarly, one defines maximal ideals.

A standard application of Zorn's lemma proves that every unitary ring contains a maximal left (or right) ideal.

Proposition 2.18. *Let R be a ring and M be a module. Then M is simple if and only if $M \simeq R/I$ for some maximal regular left ideal I.*

Proof. Assume that M is simple. Then $M = R \cdot m$ for some $m \neq 0$ by Lemma 2.10. The map $\phi\colon R \to M$, $r \mapsto r \cdot m$, is a surjective homomorphism of R-modules, so the first isomorphism theorem implies that $M \simeq R/\ker\phi$. Since $\ker\phi$ is an ideal of R, it is in particular a left ideal of R.

We claim that $I = \ker\phi$ is a maximal left ideal. The correspondence theorem and the simplicity of M imply that I is a maximal left ideal (because each left ideal J such that $I \subseteq J$ yields a submodule of R/I).

We claim that I is regular. Since $M = R \cdot m$, there exists $e \in R$ such that $m = e \cdot m$. If $r \in R$, then $r - re \in I$ since $\phi(r - re) = \phi(r) - \phi(re) = r \cdot m - r \cdot (e \cdot m) = 0$.

Now assume that I is a maximal left ideal that is regular. The correspondence theorem implies that R/I has no non-zero proper submodules.

We claim that $R \cdot (R/I) \neq 0$. If $R \cdot (R/I) = \{0\}$ and $r \in R$, then the regularity of I implies that there exists $e \in R$ such that $r - re \in I$. Hence $r \in I$, as

$$0 = r \cdot (e + I) = re + I = r + I,$$

a contradiction to the maximality of I. $\square$

Let R be a ring and M be a left R-module. For a subset $N \subseteq M$ we define the **annihilator** of N as the subset

$$\mathrm{Ann}_R(N) = \{r \in R : r \cdot n = 0 \text{ for all } n \in N\}.$$

Example 2.19. $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/n) = n\mathbb{Z}$.

Exercise 2.20. Let R be a ring and M be a module. If $N \subseteq M$ is a subset, then $\mathrm{Ann}_R(N)$ is a left ideal of R. If $N \subseteq M$ is a submodule of R, then $\mathrm{Ann}_R(N)$ is an ideal of R.

Definition 2.21. A module M is said to be **faithful** if $\mathrm{Ann}_R(M) = \{0\}$.

Example 2.22. If K is a field, then K^n is a faithful unitary $M_n(K)$-module.

Example 2.23. If V is vector space over a field K, then V is faithful unitary $\mathrm{End}_K(V)$-module.

Definition 2.24. A ring R is said to be **primitive** if there exists a faithful simple R-module.

Since we are considering left modules, our definition of primitive rings is that of left primitive rings. By convention, a primitive ring will always mean a left primitive ring. The use of right modules yields to the notion of right primitive rings.

Exercise 2.25. If R is a simple unitary ring, then R is primitive.

Exercise 2.26. If R is a commutative ring (maybe without identity), then R is primitive if and only if R is a field.

Example 2.27. The ring $\mathbb{Z}$ is not primitive.

Lecture 4

Definition 2.28. An ideal P of a ring R is said to be **primitive** if $P = \operatorname{Ann}_R(M)$ for some simple R-module M.

Lemma 2.29. *Let R be a ring and P be an ideal of R. Then P is primitive if and only if R/P is a primitive ring.*

Proof. Assume that $P = \operatorname{Ann}_R(M)$ for some R-module M. Then M is a simple (R/P)-module with

$$(r+P)\cdot m = r\cdot m,$$

$r \in R$, $m \in M$. This operation is well-defined, as $P = \operatorname{Ann}_R(M)$. Since M is a simple R-module, it follows that M is a simple (R/P)-module. Moreover, $\operatorname{Ann}_{R/P} M = \{0\}$. Indeed, if $(r+P)\cdot M = \{0\}$, then $r \in \operatorname{Ann}_R M = P$ and hence $r+P = P$.

Assume now that R/P is primitive. Let M be a faithful simple (R/P)-module. Then $r\cdot m = (r+P)\cdot m$, $r \in R$, $m \in M$, turns M into an R-module. It follows that M is simple and that $P = \operatorname{Ann}_R(M)$. □

Example 2.30. Let $R_1, \dots, R_n$ be primitive rings and $R = R_1 \times \cdots \times R_n$. Then each $P_i = R_1 \times \cdots \times R_{i-1} \times \{0\} \times R_{i+1} \times \cdots \times R_n$ is a primitive ideal of R since $R/P_i \simeq R_i$.

Lemma 2.31. *Let R be a ring. If P is a primitive ideal, there exists a maximal left ideal I such that $P = \{x \in R : xR \subseteq I\}$. Conversely, if I is a regular maximal left ideal, then $\{x \in R : xR \subseteq I\}$ is a primitive ideal.*

Proof. Assume that $P = \operatorname{Ann}_R(M)$ for some simple R-module M. By Proposition 2.18, there exists a regular maximal left ideal I such that $M \simeq R/I$. Then $P = \operatorname{Ann}_R(R/I) = \{x \in R : xR \subseteq I\}$.

Conversely, let I be a regular maximal left ideal. By Proposition 2.18, R/I is a simple R-module. Then

$$\operatorname{Ann}_R(R/L) = \{x \in R : xR \subseteq I\}$$

is a primitive ideal. □

Exercise 2.32. Maximal ideals of unitary rings are primitive.

Exercise 2.33. Prove that every primitive ideal of a commutative ring is maximal.

Exercise 2.34. Prove that $M_n(R)$ is primitive if and only if R is primitive.

§3. Jacobson's radical

Definition 3.1. Let R be a ring. The **Jacobson radical** $J(R)$ is the intersection of all the annihilators of simple left R-modules. If R does not have simple left R-modules, then $J(R) = R$.

From the definition, it follows that $J(R)$ is an ideal. Moreover,

$$J(R) = \bigcap \{P : P \text{ left primitive ideal}\}.$$

If I is an ideal of R and $n \in \mathbb{Z}_{>0}$, I^n is the additive subgroup of R generated by the set $\{y_1 \dots y_n : y_j \in I\}$.

Definition 3.2. An ideal I of R is **nilpotent** if $I^n = \{0\}$ for some $n \in \mathbb{Z}_{>0}$.

Similarly, one defines right or left nilpotent ideals. Note that an ideal I is nilpotent if and only if there exists $n \in \mathbb{Z}_{>0}$ such that $x_1 x_2 \cdots x_n = 0$ for all $x_1, \dots, x_n \in I$.

Definition 3.3. An element x of a ring is said to be **nil** (or nilpotent) if $x^n = 0$ for some $n \in \mathbb{Z}_{>0}$.

Definition 3.4. An ideal I of a ring is said to be nil if every element of I is nil.

Similarly, one defines right or left nil ideals. Note that every nilpotent ideal is nil, as $I^n = 0$ implies $x^n = 0$ for all $x \in I$.

Example 3.5. Let $R = \mathbb{C}[X_1, X_2, \dots]/(X_1, X_2^2, X_3^3, \dots)$. The ideal $I = (X_1, X_2, X_3, \dots)$ is nil in R, as it is generated by nilpotent element. However, it is not nilpotent. Indeed, if I is nilpotent, then there exists $k \in \mathbb{Z}_{>0}$ such that $I^k = 0$ and hence $x_i^k = 0$ for all i, a contradiction since $x_{k+1}^k \neq 0$.

Proposition 3.6. *Let R be a ring. Then every nil left ideal (resp. right ideal) is contained in $J(R)$.*

Proof. Assume that there is a nil left ideal (resp. right ideal) I such that $I \not\subseteq J(R)$. There exists a simple R-module M such that $n = xm \neq 0$ for some $x \in I$ and some $m \in M$. Since M is simple, $Rn = M$ and hence there exists $r \in R$ such that

$$(rx) \cdot m = r \cdot (x \cdot m) = r \cdot n = m \quad (\text{resp. } (xr) \cdot n = x \cdot (r \cdot n) = x \cdot m = n).$$

Thus $(rx)^k \cdot m = m$ (resp. $(xr)^k \cdot n = n$) for all $k \geq 1$, a contradiction since $rx \in I$ (resp. $xr \in I$) is a nilpotent element. $\square$

Definition 3.7. Let R be a ring. An element $a \in R$ is said to be **left quasi-regular** if there exists $r \in R$ such that $r+a+ra=0$. Similarly, a is said to be **right quasi-regular** if there exists $r \in R$ such that $a+r+ar=0$.

Let R be a ring. A direct calculation shows that

$$R \times R \to R, \quad (r,s) \mapsto r \circ s = r+s+rs,$$

is an associative operation with neutral element 0. To show an explicit example let $R = \mathbb{Z}/3 = \{0,1,2\}$. The multiplication table for the circle operation is

$\circ$	0	1	2
0	0	1	2
1	1	0	2
2	2	2	2

If R is unitary, an element $x \in R$ is left quasi-regular (resp. right quasi-regular) if and only if $1+x$ is left invertible (resp. right invertible). In fact, if $r \in R$ is such that $r+x+rx=0$, then $(1+r)(1+x) = 1+r+x+rx = 1$. Conversely, if there exists $y \in R$ such that $y(1+x)=1$, then

$$(y-1) \circ x = y-1+x+(y-1)x = 0.$$

Example 3.8. If $x \in R$ is a nilpotent element, then $y = \sum_{n \geq 1} x^n \in R$ is left quasi-regular. In fact, if there exists N such that $x^N = 0$, then the sum defining y is finite and $y+(-x)+y(-x)=0$. Is right quasi-regular?

Definition 3.9. A left ideal I of R is said to be **left quasi-regular** (resp. right quasi-regular) if every element of I is left quasi-regular (resp. right quasi-regular). A left ideal is said to be **quasi-regular** if it is left and right quasi-regular.

Similarly one defines right quasi-regular ideals and quasi-regular ideals.

Lemma 3.10. *Let I be a left ideal of R. If I is left quasi-regular, then I is quasi-regular.*

Proof. Let $x \in I$. Let us prove that x is right quasi-regular. Since I is left quasi-regular, there exists $r \in R$ such that $r \circ x = r+x+rx = 0$. Since $r = -x-rx \in I$, there exists $s \in R$ such that $s \circ r = s+r+sr = 0$. Then s is right quasi-regular and

$$x = 0 \circ x = (s \circ r) \circ x = s \circ (r \circ x) = s \circ 0 = s. \qquad \square$$

Let $(A, \leq)$ be a **partially order set**, this means that A is a set together with a reflexive, transitive, and anti-symmetric binary relation R en $A \times A$, where $a \leq b$ if and only if $(a,b) \in R$. Recall that the relation is reflexive if $a \leq a$ for all $a \in A$, the relation is transitive if $a \leq b$ and $b \leq c$ imply that $a \leq c$ and the relation is anti-symmetric if $a \leq b$ and $b \leq a$ imply $a = b$. The elements $a, b \in A$ are said to be

comparable if $a \leq b$ or $b \leq a$. An element $a \in A$ is said to be **maximal** if $c \leq a$ for all $c \in A$ that is comparable with a. An **upper bound** for a non-empty subset $B \subseteq A$ is an element $d \in A$ such that $b \leq d$ for all $b \in B$. A **chain** in A is a subset B such that every pair of elements of B are comparable. **Zorn's lemma** states the following property:

> If A is a non-empty partially ordered set such that every chain in A contains an upper bound in A, then A contains a maximal element.

Our application of Zorn's lemma:

Lemma 3.11. *Let R be a ring, and $x \in R$ be an element that is not left quasi-regular Then there exists a maximal left ideal M such that $x \notin M$. Moreover, R/M is a simple R-module and $x \notin \mathrm{Ann}_R(R/M)$.*

Proof. Let $T = \{r + rx : r \in R\}$. A straightforward calculation shows that T is a left ideal of R such that $x \notin T$ (if $x \in T$, then $r + rx = -x$ for some $r \in R$, a contradiction since x is not left quasi-regular).

The only left ideal of R containing $T \cup \{x\}$ is R. Indeed, if there exists a left ideal U containing T, then $x \notin U$, since otherwise every $r \in R$ could be written as $r = (r + rx) + r(-x) \in U$.

Let $\mathcal{S}$ be the set of proper left ideals of R containing T partially ordered by inclusion. If $\{K_i : i \in I\}$ is a chain in $\mathcal{S}$, then $K = \cup_{i \in I} K_i$ is an upper bound for the chain (K is a proper, as $x \notin K$). Zorn's lemma implies that $\mathcal{S}$ admits a maximal element M. Thus M is a maximal left ideal such that $x \notin M$. Moreover, M is regular since $r - r(-x) \in T \subseteq M$ for all $r \in R$. Therefore R/M is a simple R-module by Proposition 2.18. Since $x \cdot (x + M) \neq 0$ (if $x^2 \in M$, then $x \in M$, as $x + x^2 \in T \subseteq M$), it follows that $x \notin \mathrm{Ann}_R(R/M)$. □

If $x \in R$ is not left quasi-regular, the lemma implies that there exists a simple R-module M such $x \notin \mathrm{Ann}_R(M)$. Thus $x \notin J(R)$.

Theorem 3.12. *Let R be a ring and $x \in R$. The following statements are equivalent:*

1) *The left ideal generated by x is quasi-regular.*
2) *Rx is quasi-regular.*
3) *$x \in J(R)$.*

Proof. The implication (1) $\implies$ (2) is trivial, as Rx is included in the left ideal generated by x.

We now prove (2) $\implies$ (3). If $x \notin J(R)$, then Lemma 3.11 implies that there exists a simple R-module M such that $xm \neq 0$ for some $m \in M$. The simplicity of M implies that $R(xm) = M$. Thus there exists $r \in R$ such that $rxm = -m$. There is an element $s \in R$ such that $s + rx + s(rx) = 0$ and hence

$$-m = rxm = (-s - srx)m = -sm + sm = 0,$$

a contradiction.

Finally, to prove (3) $\implies$ (1), it is enough to note that x is left quasi-regular. If $x \in J(R)$, then x is left quasi-regular by the previous lemma. Thus the left ideal generated by x is quasi-regular by Lemma 3.10. □

The theorem immediately implies the following corollary.

Corollary 3.13. *If R is a ring, then $J(R)$ is a quasi-regular ideal that contains every left quasi-regular ideal.*

The following result is somewhat what we all had in mind.

Theorem 3.14. *Let R be a ring such that $J(R) \neq R$. Then*

$$J(R) = \bigcap \{I : I \textit{ regular maximal left ideal of } R\}.$$

Proof. We only prove the non-trivial inclusion. Let

$$K = \bigcap \{I : I \text{ regular maximal left ideal of } R\}.$$

By Proposition 2.18,

$$J(R) = \bigcap \{\mathrm{Ann}_R(R/I) : I \text{ regular maximal left ideal of } R\}.$$

Let I be a regular maximal left ideal. If $r \in J(R) \subseteq \mathrm{Ann}_R(R/I)$, then, since I is regular, there exists $e \in R$ such that $r - re \in I$. Since

$$re + I = r(e + I) = \{0\},$$

$re \in I$ and hence $r \in I$. Thus $J(R) \subseteq K$. □

Example 3.15. Each maximal ideals of $\mathbb{Z}$ is of the form $p\mathbb{Z} = \{pm : m \in \mathbb{Z}\}$ for some prime number p. Thus $J(\mathbb{Z}) = \cap_p p\mathbb{Z} = \{0\}$.

We now review some basic results useful to compute radicals.

Proposition 3.16. *Let $\{R_i : i \in I\}$ be a family of rings. Then*

$$J\left(\prod_{i \in I} R_i\right) = \prod_{i \in I} J(R_i).$$

Proof. Let $R = \prod_{i \in I} R_i$ and $x = (x_i)_{i \in I} \in R$. The left ideal Rx is quasi-regular if and only if each left ideal $R_i x_i$ is quasi-regular in R_i, as x is quasi-regular in R if and only if each x_i is quasi-regular in R_i. Thus $x \in J(R)$ if and only if $x_i \in J(R_i)$ for all $i \in I$. □

For the next result, we shall need a lemma.

Lemma 3.17. *Let R be a ring and $x \in R$. If $-x^2$ is a left quasi-regular element, then so is x.*

Proof. Let $r \in R$ be such that $r + (-x^2) + r(-x^2) = 0$ and $s = r - x - rx$. Then x is left quasi-regular, as

$$\begin{aligned} s + x + sx &= (r - x - rx) + x + (r - x - rx)x \\ &= r - x - rx + x + rx - x^2 - rx^2 = r - x^2 - rx^2 = 0. \end{aligned}$$ □

Proposition 3.18. *If I is an ideal of R, then $J(I) = I \cap J(R)$.*

Proof. Since $I \cap J(R)$ if an ideal of I, if $x \in I \cap J(R)$, then x is left quasi-regular in R. Let $r \in R$ be such that $r + x + rx = 0$. Since $r = -x - rx \in I$, x is left quasi-regular in I. Thus $I \cap J(R) \subseteq J(I)$.

Let $x \in J(I)$ and $r \in R$. Since $-(rx)^2 = (-rxr)x \in I(J(I)) \subseteq J(I)$, the element $-(rx)^2$ is left quasi-regular in I. Thus rx is left quasi-regular by Lemma 3.17. □

Lecture 5

Definition 3.19. A ring R is said to be **radical** if $J(R) = R$.

Example 3.20. If R is a ring, then $J(R)$ is a radical ring, by Proposition 3.18.

Example 3.21. The Jacobson radical of $\mathbb{Z}/8$ is $\{0, 2, 4, 6\}$.

There are several characterizations of radical rings.

Theorem 3.22. *Let R be a ring. The following statements are equivalent:*

1) *R is radical.*
2) *R admits no simple R-modules.*
3) *R does not have regular maximal left ideals.*
4) *R does not have primitive left ideals.*
5) *Every element of R is quasi-regular.*
6) *$(R, \circ)$ is a group.*

Exercise 3.23. Prove Theorem 3.22.

Example 3.24. Let

$$A = \left\{ \frac{2x}{2y+1} : x, y \in \mathbb{Z} \right\}.$$

Then A is a radical ring, as the inverse of the element $\frac{2x}{2y+1}$ with respect to the circle operation $\circ$ is

$$\left(\frac{2x}{2y+1} \right)' = \frac{-2x}{2(x+y)+1}.$$

Definition 3.25. A ring R is said to be **nil** if for every $x \in R$ there exists $n = n(x)$ such that $x^n = 0$.

Exercise 3.26. Prove that a nil ring is a radical ring.

Exercise 3.27. Let $\mathbb{R}[[X]]$ be the ring of power series with real coefficients. Prove that the ideal $X\mathbb{R}[[X]]$ consisting of power series with zero constant term is a radical ring that is not nil.

Theorem 3.28. *If R is a ring, then $J(R/J(R)) = \{0\}$.*

Proof. If R is radical, the result is trivial. Suppose then that $J(R) \neq R$. Let M be a simple R-module. Then M is a simple module over $R/J(R)$ with

$$(x+J(R))\cdot m = x\cdot m, \quad x \in R, m \in M.$$

If $x+J(R) \in J(R/J(R))$, then $x\cdot M = (x+J(R))\cdot M = \{0\}$. Then $x \in J(R)$, as x annihilates any simple module over R. □

Theorem 3.29. *Let R be a ring and $n \in \mathbb{Z}_{>0}$. Then $J(M_n(R)) = M_n(J(R))$.*

Proof. We first prove that $J(M_n(R)) \subseteq M_n(J(R))$. If $J(R) = R$, the theorem is clear. Let us assume that $J(R) \neq R$ and let $J = J(R)$. If M is a simple R-module, then M^n is a simple $M_n(R)$-module with the usual multiplication. Let $x = (x_{ij}) \in J(M_n(R))$ and $m_1,\dots,m_n \in M$. Then

$$x\begin{pmatrix} m_1\\ \vdots\\ m_n\end{pmatrix} = 0.$$

In particular, $x_{ij} \in \mathrm{Ann}_R(M)$ for all $i,j \in \{1,\dots,n\}$. Hence $x \in M_n(J)$.

We now prove that $M_n(J) \subseteq J(M_n(R))$. Let

$$J_1 = \begin{pmatrix} J & 0 & \cdots & 0\\ J & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ J & 0 & \cdots & 0\end{pmatrix} \quad \text{and} \quad x = \begin{pmatrix} x_1 & 0 & \cdots & 0\\ x_2 & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ x_n & 0 & \cdots & 0\end{pmatrix} \in J_1.$$

Since x_1 es quasi-regular, there exists $y_1 \in R$ such that $x_1+y_1+x_1y_1 = 0$. If

$$y = \begin{pmatrix} y_1 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 0\end{pmatrix},$$

then $u = x+y+xy$ is lower triangular, as

$$u = \begin{pmatrix} 0 & 0 & \cdots & 0\\ x_2y_1 & 0 & \cdots & 0\\ x_3y_1 & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ x_ny_1 & 0 & \cdots & 0\end{pmatrix}.$$

Since $u^n = 0$, the element

$$v = -u+u^2-u^3+\cdots+(-1)^{n-1}u^{n-1}$$

is such that $u+v+uv=0$. Thus x is right quasi-regular, as

$$x+(y+v+yv)+x(y+v+yv)=0,$$

and therefore J_1 is right quasi-regular. Similarly one proves that each J_i is right quasi-regular and hence $J_i \subseteq J(M_n(R))$ for all $i \in \{1,\dots,n\}$. In conclusion,

$$J_1+\cdots+J_n \subseteq J(M_n(R))$$

and therefore $M_n(J) \subseteq J(M_n(R))$. □

Exercise 3.30. Let R be a unitary ring. Then

$$J(R) = \bigcap \{M : M \text{ is a left maximal ideal}\}.$$

Exercise 3.31. Let R be a unitary ring. The following statements are equivalent:

1) $x \in J(R)$.
2) $x \cdot M = \{0\}$ for all simple R-module M.
3) $x \in P$ for all primitive left ideal P.
4) $1+rx$ is invertible for all $r \in R$.
5) $1+\sum_{i=1}^{n} r_i x s_i$ is invertible for all n and all $r_i, s_i \in R$.
6) x belongs to every maximal ideal maximal.

The following exercise is entirely optional. It somewhat shows a recent application of radical rings to solutions of the celebrated Yang–Baxter equation.

Exercise 3.32. A pair (X,r) is a **solution** to the Yang–Baxter equation if X is a set and $r\colon X \times X \to X \times X$ is a bijective map such that

$$(r \times \mathrm{id}) \circ (\mathrm{id} \times r) \circ (r \times \mathrm{id}) = (\mathrm{id} \times r) \circ (r \times \mathrm{id}) \circ (\mathrm{id} \times r).$$

The solution (X,r) is said to be **involutive** if $r^2 = \mathrm{id}$. By convention, we write

$$r(x,y) = (\sigma_x(y), \tau_y(x)).$$

The solution (X,r) is said to be **non-degenerate** $\sigma_x\colon X \to X$ and $\tau_x\colon X \to X$ are bijective for all $x \in X$.

1) Let X be a set and $\sigma\colon X \to X$ be a bijective map. Prove that the pair (X,r), where $r(x,y) = (\sigma(y), \sigma^{-1}(x))$, is an involutive non-degenerate solution.

Let R be a radical ring. For $x, y \in R$ let

$$\lambda_x(y) = -x + x \circ y = xy + y,$$
$$\mu_y(x) = \lambda_x(y)' \circ x \circ y = (xy+y)'x + x$$

Prove the following statements:

2) $\lambda\colon (R,\circ) \to \mathrm{Aut}(R,+)$, $x \mapsto \lambda_x$, is a group homomorphism.

3) $\mu\colon (R,\circ) \to \operatorname{Aut}(R,+)$, $y \mapsto \mu_y$, is a group antihomomorphism.
4) The map

$$r\colon R\times R \to R\times R, \quad r(x,y) = (\lambda_x(y), \mu_y(x)),$$

is an involutive non-degenerate solution to the Yang–Baxter equation.

Exercise 3.33. If D is a division ring and $R = D[X_1,\dots,X_n]$, then $J(R) = \{0\}$.

Example 3.34. A commutative and unitary ring R is **local** if it contains only one maximal ideal. If R is a local ring and M is its maximal ideal, then $J(R) = M$. Some particular cases:

1) If K is a field and $R = K[[X]]$, then $J(R) = (X)$.
2) If p is a prime number and $R = \mathbb{Z}/p^n$, then $J(R) = (p)$.

We finish the discussion on the Jacobson radical with some results in the case of unitary algebras. We first need an application of Zorn's lemma.

Exercise 3.35. Let I be a proper left ideal that is left regular. Prove that I is contained in a maximal left ideal which is regular.

Proposition 3.36. *Let A be a K-algebra and I be a subset of A. Then I is a regular maximal left ideal of the algebra A if and only if I is a regular maximal left ideal of the ring A.*

Proof. Let I be a left regular maximal ideal of the ring A. We claim that $\lambda I \subseteq I$ for all $\lambda \in K$. Assume that $\lambda I \not\subseteq I$ for some λ. Then $I + \lambda I$ is an ideal of the ring A that contains I, as

$$a(I+\lambda I) = aI + a(\lambda I) \subseteq I + \lambda(aI) \subseteq I + \lambda I.$$

Since I is maximal, it follows that $I + \lambda I = A$. The left regularity of I implies that there exists $e \in A$ such that $a - ae \in I$ for all $a \in A$. Write $e = x + \lambda y$ for $x, y \in I$. Then

$$e^2 = e(x+\lambda y) = ex + e(\lambda y) = ex + (\lambda e)y \in I.$$

Since $e - e^2 \in I$ and $e^2 \in I$, it follows that $e \in I$. Thus $A = I$, as $a - ae \in I$ for all $a \in A$, a contradiction.

Conversely, if I is a left regular maximal ideal of the algebra A, then I is a left regular ideal of the ring A. We claim that I is a maximal left ideal of the ring of A. There exists a regular maximal left ideal M of the ring A that contains I. Since M is regular, it follows that M is a regular maximal ideal of the algebra A. Thus $M = I$ because I is a maximal left ideal of the algebra A. $\square$

Exercise 3.37. Let A be an algebra. Prove that the Jacobson radical of the ring A coincides with the Jacobson radical of the algebra A.

§4. Amitsur's theorem

We now prove an important result of Amitsur that has several interesting applications. We first need a lemma.

Lemma 4.1. *Let A be an algebra with one and let $x \in J(A)$. Then x is algebraic if and only if x is nilpotent.*

Proof. Since x is algebraic, there exist $a_0, \dots, a_n \in K$ not all zero such that

$$a_0 + a_1 x + \cdots + a_n x^n = 0.$$

Let r be the smallest integer such that $a_r \neq 0$. Then

$$x^r(1 + b_1 x + \cdots + b_m x^m) = 0,$$

for some $b_1, \dots, b_m \in K$. Since $1 + b_1 x + \cdots + b_m x^m$ is a unit by Exercise 3.31, it follows that $x^r = 0$. $\square$

An application:

Proposition 4.2. *If A is an algebraic algebra with one, then $J(A)$ is the largest nil ideal of A.*

Proof. The previous lemma implies that $J(A)$ is a nil ideal. Proposition 3.6 now implies that $J(A)$ is the largest nil ideal of A. $\square$

Theorem 4.3 (Amitsur). *Let A be a K-algebra with one such that* $\dim_K A < |K|$ *(as cardinals). Then $J(A)$ is the largest nil ideal of A.*

Proof. If K is finite, then A is a finite-dimensional algebra. In particular, A is algebraic and hence $J(A)$ is a nil ideal by Proposition 4.2.

Assume that K is infinite and let $a \in J(A)$. Exercise 3.31 implies that every element of the form $1 - \lambda^{-1} a$, $\lambda \in K \setminus \{0\}$, is invertible. Thus

$$a - \lambda = -\lambda(1 - \lambda^{-1} a)$$

is invertible for all $\lambda \in K \setminus \{0\}$. Let $S = \{(a - \lambda)^{-1} : \lambda \in K \setminus \{0\}\}$. Since

$$(a - \lambda)^{-1} = (a - \mu)^{-1} \iff \lambda = \mu,$$

it follows that $|S| = |K \setminus \{0\}| = |K| > \dim_K A$. Then S is linearly dependent, so there are $\beta_1, \dots, \beta_n \in K$ not all zero and distinct elements $\lambda_1, \dots, \lambda_n \in K$ such that

$$\sum_{i=1}^{n} \beta_i (a - \lambda_i)^{-1} = 0. \tag{5.1}$$

Multiplying (5.1) by $\prod_{i=1}^{n}(a - \lambda_i)$ we get

$$\sum_{i=1}^{n} \beta_i \prod_{j \neq i} (a - \lambda_j) = 0.$$

We claim that a is algebraic over K. Indeed,

$$f(X) = \sum_{i=1}^{n} \beta_i \prod_{j \neq i} (X - \lambda_j)$$

is non-zero, as, for example, if $\beta_1 \neq 1$, then $f(\lambda_1) = \beta_1(\lambda_1 - \lambda_2) \cdots (\lambda_1 - \lambda_n) \neq 0$ and $f(a) = 0$. Since $a \in J(A)$ is algebraic, it follows a is nilpotent by Lemma 4.1. $\square$

Amitsur's theorem implies the following result.

Corollary 4.4. *Let K be a non-countable field. If A is an algebra over K with a countable basis, then $J(A)$ is the largest nil ideal of A.*

§5. Jacobson's conjecture

We now conclude the lecture with two big open problems related to the Jacobson radical. The first one is Jacobson's conjecture.

Open problem 5.1 (Jacobson). Let R be a noetherian ring. Is then

$$\bigcap_{n \geq 1} J(R)^n = \{0\}?$$

Open problem 5.1 was originally formulated by Jacobson in 1956 [7] for one-sided noetherian rings. In 1965 Herstein [4] found a counterexample in the case of one-sided noetherian rings and reformulated the conjecture as it appears here.

Exercise 5.2 (Herstein). Let D be the ring of rationals with odd denominators. Let $R = \begin{pmatrix} D & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$. Prove that R is right noetherian and $J(R) = \begin{pmatrix} J(D) & \mathbb{Q} \\ 0 & 0 \end{pmatrix}$. Prove that $J(R)^n \supseteq \begin{pmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{pmatrix}$ and hence $\bigcap_n J(R)^n$ is non-zero.

§6. Köthe's conjecture

The following problem is maybe the most important open problem in non-commutative ring theory.

Open problem 6.1 (Köthe). Let R be a ring. Is the sum of two arbitrary nil left ideals of R is nil?

Open problem 6.1 is the well-known Köthe's conjecture. The conjecture was first formulated in 1930, see [8]. It is known to be true in several cases. In full generality, the problem is still open. In [9] Krempa proved that the following statements are equivalent:

1) Köthe's conjecture is true.
2) If R is a nil ring, then $R[X]$ is a radical ring.
3) If R is a nil ring, then $M_2(R)$ is a nil ring.
4) Let $n \geq 2$. If R is a nil ring, then $M_n(R)$ is a nil ring.

In 1956 Amitsur formulated the following conjecture, see for example [1]: If R is a nil ring, then $R[X]$ is a nil ring. In [16] Smoktunowicz found a counterexample to Amitsur's conjecture. This counterexample suggests that Köthe's conjecture might be false. A simplification of Smoktunowicz's example appears in [13]. See [17, 18] for more information on Köthe's conjecture and related topics.

Lecture 6

§7. Gilmer's theorem

Hilbert's theorem states that if R is a noetherian commutative unitary ring, then $R[X]$ is noetherian. Following [3], we now present the converse of Hilbert's theorem.

Theorem 7.1 (Gilmer). *Let R be a commutative ring. If $R[X]$ is noetherian, then R is unitary.*

Proof. Let $a \in R$. For $m \geq 0$, let

$$\begin{aligned} I_m &= (a, aX, aX^2, \dots, aX^m) \\ &= R[X]a + R[X]aX + \cdots + aX^m + \mathbb{Z}a + \mathbb{Z}aX + \cdots + \mathbb{Z}aX^m. \end{aligned}$$

Then $I_0 \subseteq I_1 \subseteq \cdots I_m \subseteq I_{m+1} \subseteq \cdots$ is a sequence of ideals of $R[X]$. Since $R[X]$ is noetherian, $I_n = I_{n+1}$ for some n. In particular, $aX^{n+1} \in I_{n+1} = I_n$. Thus

$$aX^{n+1} = \sum_{i=1}^{n+1} aX^{i-1} f_i(X) + \sum_{i=1}^{n+1} k_i aX^{i-1}$$

for some $f_1(X), \dots, f_n(X) \in R[X]$ and $k_1, \dots, k_n \in \mathbb{Z}$. Comparing the coefficient of X^{n+1} one gets that $a = ar$ for some $r \in R$. Thus

$$\text{for every } a \in R \text{ there exists } r \in R \text{ such that } a = ra. \tag{6.1}$$

Claim. For every $a_1, \dots, a_n \in R$ there exists $r \in R$ such that $a_i = ra_i$ for all i.

We proceed by induction on n. The case $n = 1$ is (6.1). Assume that the result holds for $n - 1 \geq 1$. By the inductive hypothesis, there exists $r_1 \in R$ such that $a_i = r_1 a_i$ for all $i \in \{1, \dots, n-1\}$. Moreover, there exists $r_2 \in R$ such that $a_n = ra_n$. Let $r = r_1 + r_2 - r_1 r_2$. Then

$$ra_n = r_1 a_n + r_2 a_n - r_1 r_2 a_n = r_1 a_n + a_n - r_1 a_n = a_n.$$

Moreover, for $i \in \{1, \dots, n-1\}$,

$$ra_i = r_1a_i + r_2a_i - r_1r_2a_i = a_i + r_2a_i - r_2r_1a_i = a_i + r_2a_i - r_2a_i = a_i.$$

We now finish the proof of the theorem. Let $R[X] \to R$, $f(X) \mapsto f(0)$, be an evaluation map. Since it is a surjective ring homomorphism, R is noetherian. In particular, R is finitely generated, say

$$R = (a_1, \dots, a_n) = Ra_1 + \cdots + Ra_n + \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$$

for some $a_1, \dots, a_n \in R$.

We now prove that the element r from the claim we proved turns R into a unitary ring, that is $r = 1_R$. We need to show that $rb = b$ for all $b \in R$. If $b \in R$, then

$$b = t_1a_1 + \cdots + t_na_n + m_1a_1 + \cdots + m_na_n$$

for some $t_1, \dots, t_n \in R$ and $m_1, \dots, m_n \in \mathbb{Z}$. Since $a_i = ra_i$ for all $i \in \{1, \dots, n\}$, it immediately follows that $rb = b$. $\square$

Example 7.2. The polynomial ring $(2\mathbb{Z})[X]$ is not noetherian, as the ring $2\mathbb{Z}$ is not unitary.

§8. Artinian modules

Definition 8.1. Let R be a ring. A module N is **artinian** if every decreasing sequence $N_1 \supseteq N_2 \supseteq \cdots$ of submodules of N stabilizes, that is there exists $n \in \mathbb{Z}_{>0}$ such that $N_n = N_{n+k}$ for all $k \in \mathbb{Z}_{\geq 0}$.

Let X be a set and $\mathcal{S}$ be a set of subsets of X. We say that $A \in \mathcal{S}$ is a **minimal element** of $\mathcal{S}$ if there is no $Y \in \mathcal{S}$ such that $Y \subsetneq A$.

Proposition 8.2. *A module N is artinian if and only if every non-empty subset of submodules of N contains a minimal element.*

Proof. Assume that N is artinian. Let $\mathcal{S}$ be a non-empty set of submodules of N. Suppose that $\mathcal{S}$ has no minimal element and let $N_1 \in \mathcal{S}$. Since N_1 is not minimal, there exists $N_2 \in \mathcal{S}$ such that $N_1 \supsetneq N_2$. Now assume the submodules

$$N_1 \supsetneq N_2 \supseteq \cdots \supsetneq N_k$$

we chosen. Since N_k is not minimal, there exists N_{k+1} such that $N_k \supsetneq N_{k+1}$. This procedure produces a sequence $N_1 \supsetneq N_2 \supsetneq \cdots$ that cannot stabilize, a contradiction.

If $N_1 \supseteq N_2 \supseteq \cdots$ is a sequence of submodules, then $\mathcal{S} = \{N_j : j \geq 1\}$ has a minimal element, say N_n. Then $N_n = N_{n+k}$ for all k. $\square$

A module N is **noetherian** if for every sequence $N_1 \subseteq N_2 \subseteq \cdots$ of submodules of N there exists $n \in \mathbb{Z}_{>0}$ such that $N_n = N_{n+k}$ for all $k \in \mathbb{Z}_{\geq 0}$.

Exercise 8.3. Let M be a module. The following statements are equivalent:

1) M is noetherian.
2) Every submodule of M is finitely generated.
3) Every non-empty subset $\mathcal{S}$ of submodules of M contains a maximal element, that is an element $X \in \mathcal{S}$ such that there is no $Z \in \mathcal{S}$ such that $X \subsetneq Z$.

Exercise 8.4. Prove that a ring R is left noetherian if every sequence of left ideals $I_1 \subseteq I_2 \subseteq \cdots$ stabilizes.

Exercise 8.5. Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence of modules. Prove that B is noetherian (resp. artinian) if and only if A and C are noetherian (resp. artinian).

Definition 8.6. A ring R is **left artinian** if the module ${}_RR$ is artinian.

Similarly one defines right artinian rings.

Example 8.7. The ring $\mathbb{Z}$ is noetherian. It is not artinian, as the sequence

$$2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq \cdots$$

does not stabilize.

Exercise 8.8. Prove that a ring R is left artinian if every sequence of left ideals $I_1 \supseteq I_2 \supseteq \cdots$ stabilizes.

Definition 8.9. A **composition series** of the module M is a sequence

$$\{0\} = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

of submodules of M such that each M_i/M_{i-1} is non-zero and has no non-zero proper submodules. In this case n is the length of the composition series.

The previous definition makes sense also for non-unitary rings. That is why it is required that each quotient M_i/M_{i-1} has no proper submodules.

Theorem 8.10. *A non-zero module admits a composition series if and only if it is artinian and noetherian.*

Proof. Let M be a non-zero module and let $\{0\} = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ be a composition series for M. We claim that each M_i is artinian and noetherian. We proceed by induction on i. The case $i = 0$ is trivial. Let us assume that M_i is artinian and noetherian. Since M_i/M_{i+1} has no proper submodules and the sequence

$$0 \longrightarrow M_i \longrightarrow M_{i+1} \longrightarrow M_{i+1}/M_i \longrightarrow 0$$

is exact, it follows that M_{i+1} is artinian and noetherian, see Exercise 8.5.

Conversely, let M be a non-zero artinian and noetherian module. Let $M_0 = \{0\}$ and M_1 be minimal among the non-zero submodules of M (it exists by Proposition 8.2). If $M_1 \neq M$, let M_2 be minimal among those submodules of M such that $M_1 \subsetneq M_2$. This procedure produces a sequence

$$\{0\} = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$$

of submodules of M, where each M_{i+1}/M_i is non-zero and admits no proper submodules. Since M is noetherian, the sequence stabilizes and hence it follows that $M_n = M$ for some n. □

Definition 8.11. Let M be a module. We say that the composition series

$$M = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_k = \{0\}, \quad M = W_0 \supsetneq W_1 \supsetneq \cdots \supsetneq W_l = \{0\},$$

are **equivalent** if $k = l$ and there exists $\sigma \in \mathbb{S}_k$ such that $V_i/V_{i-1} \simeq W_{\sigma(i)}/W_{\sigma(i)-1}$ for all $i \in \{1, \dots, k\}$.

Exercise 8.12. Find all composition series for the $\mathbb{Z}$-module $\mathbb{Z}/6$.

Theorem 8.13 (Jordan–Hölder). *Any two composition series for a module are equivalent.*

Proof. Let M be a module and

$$M = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_k = \{0\}, \quad M = W_0 \supsetneq W_1 \supsetneq \cdots \supsetneq W_l = \{0\},$$

be composition series of M. We claim that these composition series are equivalent. We proceed by induction on k. The case $k = 1$ is trivial, as in this case M has no proper submodules and $M \supsetneq \{0\}$ is the only possible composition series for M. So assume the result holds for modules with composition series of length $< k$. If $V_1 = W_1$, then V_1 has composition series of lengths $k-1$ and $l-1$. The inductive hypothesis implies that $k = l$ and we are done. So assume that $V_1 \neq W_1$. Since V_1 and W_1 are submodules of M, the sum $V_1 + W_1$ is also a submodule of M. Moreover, M/V_1 has no non-zero proper submodules and hence $V_1 + W_1 = V$. Then

$$M/V_1 = \frac{V_1 + W_1}{V_1} \simeq \frac{V_1}{V_1 \cap W_1}.$$

Since V_1 has a composition series, V_1 is artinian and noetherian by Theorem 8.10. The submodule $U = V_1 \cap W_1$ is also artinian and noetherian and hence, by Theorem 8.10, it admits a composition series

$$U = U_0 \supsetneq U_1 \supsetneq \cdots \supsetneq U_r = \{0\}.$$

Thus $V_1 \supsetneq \cdots \supsetneq V_k = \{0\}$ and $V_1 \supsetneq U \supsetneq U_1 \supsetneq \cdots \supsetneq U_r = \{0\}$ are both composition series for V_1. The inductive hypothesis implies that $k - 1 = r + 1$ and that these composition series are equivalent. Similarly,

$$W_1 \supsetneq W_2 \supsetneq \cdots \supsetneq W_l = \{0\}, \quad W_1 \supsetneq U \supsetneq U_1 \supsetneq \cdots \supsetneq U_r = \{0\},$$

are both composition series for W_1 and hence $l-1 = r+1$ and these composition series are equivalent. Therefore $l = k$ and the proof is completed. □

Jordan–Hölder theorem allows us to define the length of modules that admit a composition series.

Definition 8.14. Let M be a module with a composition series. The **length** $\ell(M)$ of M is defined as the length of any composition series of M.

A module is said to be of finite length if it admits a composition series.

Exercise 8.15. If N and Q are modules with composition series and

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} Q \longrightarrow 0$$

is an exact sequence of modules, then $\ell(M) = \ell(N) + \ell(Q)$.

Exercise 8.16. If A and B are finite-length submodules of M, then

$$\ell(A+B) + \ell(A \cap B) = \ell(A) + \ell(B).$$

Theorem 8.17. *If R is a left artinian ring, then $J(R)$ is nilpotent.*

Proof. Let $J = J(R)$. Since R is a left artinian ring, the sequence $(J^m)_{m \in \mathbb{Z}_{>0}}$ of left ideals stabilizes. There exists $k \in \mathbb{Z}_{>0}$ such that $J^k = J^l$ for all $l \geq k$. We claim that $J^k = \{0\}$. If $J^k \neq \{0\}$ let $\mathcal{S}$ the set of left ideals I such that $J^k I \neq \{0\}$. Since

$$J^k J^k = J^{2k} = J^k \neq \{0\},$$

the set $\mathcal{S}$ is non-empty. Since R is left artinian, $\mathcal{S}$ has a minimal element I_0. Since $J^k I_0 \neq \{0\}$, let $x \in I_0 \setminus \{0\}$ be such that $J^k x \neq \{0\}$. Moreover, $J^k x$ is a left ideal of R contained in I_0 and such that $J^k x \in \mathcal{S}$, as $J^k(J^k x) = J^{2k} x = J^k x \neq \{0\}$. The minimality of I_0 implies that, $J^k x = I_0$. In particular, there exists $r \in J^k \subseteq J$ such that $rx = x$. Since $-r \in J(R)$ is left quasi-regular, there exists $s \in R$ such that $s - r - sr = 0$. Thus

$$x = rx = (s - sr)x = sx - s(rx) = sx - sx = 0,$$

a contradiction. □

Corollary 8.18. *Let R be a left artinian ring. Each nil left ideal is nilpotent and $J(R)$ is the unique maximal nilpotent ideal of R.*

Proof. Let L be a nil left ideal of R. By Proposition 3.6, L is contained in $J(R)$. Thus L is nilpotent, as $J(R)$ is nilpotent by Theorem 8.17. □

§9. Akizuki's theorem

We now prove that if R is a unitary commutative artinian ring, then R is noetherian.

Exercise 9.1. Let R be a unitary commutative ring, I be an ideal of R and M be an R-module such that $I \cdot M = \{0\}$. Prove that if M is finitely generated, then M is a finitely generated (R/I)-module with

$$(r+I)\cdot m = r\cdot m, \quad r \in R, m \in M.$$

Recall that an ideal I of a commutative ring R is said to be **prime** if $xy \in I$ implies that $x \in I$ or $y \in I$.

Exercise 9.2. Let R be an unitary commutative artinian ring.

1) Prove that if R is a domain, then R is a field.
2) Prove that prime ideals of R are maximal.

Theorem 9.3 (Akizuki). *Let R be a unitary commutative ring. If R is artinian, then R is noetherian.*

Proof. Assume that the result is not true, so there exists an ideal of R that is not finitely generated. Let X be the set of ideals of R that are not finitely generated. Since $X \neq \emptyset$ and R is artinian, there exists a minimal element $I \in X$. The minimality of I implies that if J is an ideal of R such that $J \subsetneq I$, then J is finitely generated.

Claim. Either $RI = \{0\}$ or $RI = I$.

If not, let $r \in R$ be such that $rI \neq \{0\}$ and $rI \neq I$. Since rI is an ideal of R and $rI \subsetneq I$, the minimality of I implies that rI is finitely generated. Let $f\colon I \to rI$, $x \mapsto rx$. Then f is a surjective module homomorphism. Since $RI \neq \{0\}$, f is non-zero. In particular, $\ker f$ is finitely generated, again by the minimality of I. By the first isomorphism theorem, $I/\ker f \simeq rI$ as R-modules. Since $\ker f$ and $I/\ker f \simeq rI$ are finitely generated, I is finitely generated, a contradiction.

Claim. $M = \{r \in R : rI = \{0\}\}$ is a maximal ideal of R.

Routine calculations show that M is an ideal. Since R is artinian, it is enough to show that M is a prime ideal. Let $rs \in M$. Then $(rs)I = \{0\}$. If $r \notin M$, then $rI \neq \{0\}$. By the previous claim, $rI = I$. Thus

$$\{0\} = (rs)I = s(rI) = sI$$

and hence $s \in M$.

Since M is maximal, $K = R/M$ is a field. Since $MI = \{0\}$, I is an (R/M)-module, that is I is a K-vector space. By Exercise 9.1, $\dim_K I = \infty$. Let B be a basis of I (as a K-vector space) and $x_0 \in B$. Let J be the subspace of I generated by $B \setminus \{x_0\}$. A direct calculation shows that J is an ideal of R. Since $\dim_K J = \infty$, it follows that J is not a finitely generated ideal of R (Exercise 9.1). This is a contradiction, because J is an ideal of R such that $J \subsetneq I$. □

Lecture 7

§10. Semiprime and semiprimitive rings

Definition 10.1. A ring R is **semiprimitive** (or Jacobson semisimple) if $J(R) = \{0\}$.

In Lecture 3 we defined primitive rings as those rings that have a faithful simple module. We claim that primitive rings are semiprimitive. If R is primitive, then $\{0\}$ is a primitive ideal. Since $J(R)$ is the intersection of primitive ideals, it follows that $J(R) = \{0\}$.

Example 10.2. If $R = \prod_{i \in I} R_i$ is a direct product of semiprimitive rings, then R is semiprimitive, as

$$J(R) = J\left(\prod_{i \in I} R_i\right) = J\left(\prod_{i \in I} J(R_i)\right) = \{0\}.$$

Example 10.3. $\mathbb{Z}$ is semiprimitive, as $J(\mathbb{Z}) = \cap_p p\mathbb{Z} = \{0\}$.

Example 10.4. Let $R = C[a,b]$ be the ring of continuous maps $f\colon [a,b] \to \mathbb{R}$. In this case $J(R)$ is the intersection of all maximal ideals of R. Note that each maximal ideal of R is of the form

$$U_c = \{f \in C[a,b] : f(c) = 0\}$$

for some $c \in [a,b]$. Thus $J(R) = \cap_{a \leq c \leq b} U_c = \{0\}$.

We proved in Theorem 3.28 (Lecture 4) that $R/J(R)$ is semiprimive.

Definition 10.5. Let $\{R_i : i \in I\}$ be an arbitrary family of rings. For each $j \in I$, let $\pi_j\colon \prod_{i \in I} R_i \to R_j$ be the canonical map. We say that R is a **subdirect product** of $\{R_i : i \in I\}$ if the following conditions hold:

1) There exists an injective ring homomorphism $R \to \prod_{i \in I} R_i$.
2) For each j, the composition $\pi_j f\colon R \to R_j$ is injective.

Direct products and direct sums of rings are all examples of subdirect products of rings.

Exercise 10.6. Write (if possible) $\mathbb{Z}$ as a non-trivial subdirect product.

Example 10.7. Let R be a ring, $\{I_j : j\}$ be a collection of ideals of R and

$$f\colon R \to \prod_i R/I_i, \quad r \mapsto (r+I_i)_i.$$

For each i, let $R_i = R/I_i$. Then R is a subdirect product of the R_i if and only if f is injective.

Theorem 10.8. *Let R be a non-zero ring. Then R is semiprimitive if and only if R is isomorphic to a subdirect product of primitive rings.*

Proof. Suppose first that R is semiprimitive and let $\{P_i : i \in I\}$ be the collection of primitive ideals of R. Each R/P_j is primitive and $\{0\} = J(R) = \cap_{i\in I} P_i$. For j let $\lambda_j\colon R \to R/P_j$ and $\pi_j\colon \prod_{i\in I} R/P_i \to R/P_j$ be canonical maps. The ring homomorphism

$$\phi\colon R \to \prod_{i\in I} R/P_i, \quad r \mapsto \{\lambda_i(r) : i \in I\},$$

is injective and satisfies $\pi_j\phi(R) = R/P_j$ for all j.

Assume now that R is isomorphic to a subdirect product of primitive rings R_j and let $\varphi\colon R \to \prod_{i\in I} R_i$ be an injective homomorphism such that $\pi_j(\varphi(R)) = R_j$ for all j. For j let $P_j = \ker \pi_j\varphi$. Since $R/P_j \simeq R_j$, each P_j is a primitive ideal. If $x \in \cap_{i\in I} P_i$, then $\varphi(x) = 0$ and thus $x = 0$. Hence $J(R) \subseteq \cap_{i\in I} P_i = 0$. □

Example 10.9. The ring $C[a,b]$ of Example 10.4 is isomorphic to a subdirect product of the fields $C[a,b]/U_c \simeq \mathbb{R}$.

Definition 10.10. A ring R **semiprime** if $aRa = \{0\}$ implies $a = 0$.

Proposition 10.11. *Let R be a ring. The following statements are equivalent:*

1) *R is semiprime.*
2) *If I is a left ideal such that $I^2 = \{0\}$, then $I = \{0\}$.*
3) *If I is an ideal such that $I^2 = \{0\}$, then $I = \{0\}$.*
4) *R does not contain non-zero nilpotent ideals.*

Proof. We first prove that 1) $\implies$ 2). If $I^2 = \{0\}$ y $x \in I$, then $xRx \subseteq I^2 = \{0\}$ and thus $x = 0$. The implications 2) $\implies$ 3) and 4) $\implies$ 3) are both trivial. Let us prove that 3) $\implies$ 4). If I is a non-zero nilpotent ideal, let $n \in \mathbb{Z}_{>0}$ be minimal such that $I^n = \{0\}$. Since $(I^{n-1})^2 = \{0\}$, it follows that $I^{n-1} = \{0\}$, a contradiction. Finally, we prove that 3) $\implies$ 1). Let $a \in R$ be such that $aRa = \{0\}$. Then $I = RaR$ is an ideal of R such that $I^2 = \{0\}$. Thus $RaR = \{0\}$. This means that Ra and aR are ideals such that $(Ra)R = R(aR) = \{0\}$ (for example, $R(aR) \subseteq RaR = \{0\} \subseteq aR$). Moreover, since $(Ra)(Ra) = \{0\}$ and $(aR)(aR) = \{0\}$, it follows that $aR = Ra = \{0\}$. This implies that $\mathbb{Z}a$ is an ideal of R, as $R(\mathbb{Z}a) \subseteq \mathbb{Z}(Ra) = \{0\}$ and $(\mathbb{Z}a)R \subseteq aR = \{0\}$. Now $(\mathbb{Z}a)(\mathbb{Z}a) \subseteq (\mathbb{Z}a)R = \{0\}$ and hence $a = 0$, as $\mathbb{Z}a = \{0\}$. □

Two consequences:

Exercise 10.12. A commutative ring is semiprime if and only if it does not contain non-zero nilpotent elements.

We will prove in Lecture 9 (Corollary 16.13) that the if G is a group, then the ring $\mathbb{C}[G]$ is semiprime.

Exercise 10.13. Let D be a division ring.

1) $D[X]$ is semiprime.
2) $D[[X]]$ is semiprime and it is not semiprimitive.

§11. Jacobson's density theorem

At this point, it is convenient to recall that modules over division rings are pretty much as vector spaces over fields. Modules over division rings are usually called vector spaces over division rings.

Definition 11.1. Let D be a division ring, and V be a vector space over D. A subring $R \subseteq \operatorname{End}_D(V)$ is a **dense ring of linear operators** of V (or simple, **dense** in V) if for every $n \in \mathbb{Z}_{>0}$, every linearly independent set $\{u_1, \dots, u_n\} \subseteq V$ and every (not necessarily linearly independent) subset $\{v_1, \dots, v_n\} \subseteq V$ there exists $f \in R$ such that $f(u_j) = v_j$ for all $j \in \{1, \dots, n\}$.

Proposition 11.2. *Let D be a division ring and V be a finite-dimensional D-vector space. Then* $\operatorname{End}_D(V)$ *is the only dense ring of V.*

Proof. Let R be dense in V and let $\{v_1, \dots, v_n\}$ be a basis of V. By definition, $R \subseteq \operatorname{End}_D(V)$. If $g \in \operatorname{End}_D(V)$ then, since R is dense in V, there exists $f \in R$ such that $f(v_j) = g(v_j)$ for all $j \in \{1, \dots, n\}$. Hence $g = f \in R$. □

Theorem 11.3 (Jacobson). *A ring R is primitive if and only if it is isomorphic to a dense ring on a vector space over a division ring.*

We shall need the following lemma.

Lemma 11.4. *Let D be a division ring and V be a D-vector space. If R is dense in V and I is a non-zero ideal of R, then I is dense on V.*

Proof. Fix $n \in \mathbb{Z}_{>0}$. Let $\{u_1, \dots, u_n\} \subseteq V$ be a linearly independent set and let $\{v_1, \dots, v_n\} \subseteq V$. We want to find $\gamma \in I$ such that $\gamma(u_i) = v_i$ for all i. Since $I \neq \{0\}$, there exists $h \in I \setminus \{0\}$. This means that $h(u) = v \neq 0$ for some $u \neq 0$. Since R is dense on V, there exist $g_1, \dots, g_n \in R$ such that

$$g_i(u_j) = \begin{cases} u & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Further, since $\{v\}$ is a linearly independent subset of V, there exist $f_1,\dots,f_n \in R$ such that $f_i(v) = v_i$ for all i. Thus $\gamma = \sum_{i=1}^n f_i h g_i \in I$ is such that $\gamma(u_j) = v_j$ for all $j \in \{1,\dots,n\}$. □

Now we are ready to prove Jacobson's density theorem.

Proof of Theorem 11.3. If R is isomorphic to a dense ring in V, where V is a D-vector space for some division ring D, then R is primitive, as V is a simple and faithful R-module. Why faithful? If $f \in \mathrm{Ann}_R(V)$, then $f = 0$ since $f(v) = 0$ for all $v \in V$. Why simple? If $W \subseteq V$ is a non-zero submodule, let $v \in V$ and $w \in W \setminus \{0\}$. There exists $f \in R$ such that $v = f(w) \in W$.

Now assume that R is primitive. Let V be a simple faithful module. Schur's lemma implies that $D = \mathrm{End}_R(V)$ is a division ring. Thus V is a D-vector space with

$$D \times V \to V, \quad (\delta, v) \mapsto \delta v = \delta(v),$$

For $r \in R$ let

$$\gamma_r : V \to V, \quad v \mapsto rv.$$

A straightforward calculation shows that $\gamma_r \in \mathrm{End}_D(V)$ and that $R \to \mathrm{End}_D(V)$, $r \mapsto \gamma_r$, is a ring homomorphism. Since V is faithful, $R \simeq \gamma(R) = \{\gamma_r : r \in R\}$. In fact, if $\gamma_r = \gamma_s$, then $rv = \gamma_r(v) = \gamma_s(v) = sv$ for all $v \in V$ and hence $r = s$, as $(r-s)v = 0$ for all $v \in V$.

Claim. If U is a finite-dimensional submodule of V, for each $w \in V \setminus U$ there exists $r \in R$ such that $\gamma_r(U) = \{0\}$ and $\gamma_r(w) \neq 0$.

Suppose the claim is not true. Let U be a counterexample of minimal dimension. Then $\dim_D U \geq 1$, as the claim holds for the zero submodule. Let U_0 be a submodule of U such that $\dim U_0 = \dim U - 1$ and let

$$L = \{l \in R : \gamma_l(U_0) = \{0\}\}.$$

The minimality of the dimension of U shows that the claim is true for U_0, so any $v \in V \setminus U_0$ is such that $Lv = V$. Since there exists $l \in L$ such that $lv = \gamma_l(v) \neq 0$ and L is a left ideal of R, it follows that $Lv \subseteq V$ is a submodule and the claim follows from the simplicity of V.

Let $w \in V \setminus U$ be such that the claim is not true. Let $u \in U \setminus U_0$. The map

$$\delta : V \to V, \quad v \mapsto lw,$$

where $v = lu \in Lu = V$ (that depends both on u and w) is well-defined: if $l_1, l_2 \in L$ are such that $v = l_1 u = l_2 u$, then $(l_1 - l_2)u = 0$ and thus

$$0 = \delta(0) = \delta((l_1 - l_2)u) = (l_1 - l_2)w = l_1 w - l_2 w.$$

Further, δ is a homomorphism of modules over R, as if $l \in L$ is such that $v = lu$, then

$$\delta(rv) = \delta(r(lu)) = \delta((rl)u) = (rl)w = r(lw) = r\delta(v)$$

for all $r \in R$.

For every $l \in L$,

$$l(\delta(u) - w) = l\delta(u) - lw = \delta(lu) - lw = 0.$$

Thus $L(\delta(u) - w) = \{0\}$. This implies that $\delta(u) - w \notin V \setminus U_0$, that is $\delta(u) - w \in U_0$. Therefore

$$w = xu - (xu - w) \in Du + U_0 = U,$$

a contradiction.

Now the theorem follows from the claim. Let $u_1, \dots, u_n \in V$ be linearly independent vectors and let $v_1, \dots, v_n \in V$ arbitrary vectors. Fix $i \in \{1, \dots, n\}$. The previous claim with

$$U = \langle u_1, \dots, u_{i-1}, u_{i+1}, \dots, u_n \rangle$$

and $w = u_i$ implies that there exists $r_i \in R$ such that $\gamma_{r_i}(u_j) = 0$ if $j \neq i$ and $\gamma_{r_i}(u_i) \neq 0$. Since there exists $s_i \in R$ such that $\gamma_{s_i}\gamma_{r_i}(u_i) = v_i$, it follows that $r = \sum_{j=1}^{n} s_j r_j \in R$ is such that $\gamma_r(u_i) = v_i$ for all $i \in \{1, \dots, n\}$. □

Corollary 11.5. *If R is a primitive ring, then either there exists a division ring D such that $R \simeq \operatorname{End}_D(V)$ for some finite-dimensional module V over D or for all $m \in \mathbb{Z}_{>0}$ there exists a subring R_m of R and a surjective ring homomorphism $R_m \to \operatorname{End}_D(V_m)$ for some module V_m over D such that* $\dim_D V_m = m$.

Proof. The ring R admits a simple faithful module V. Furthermore, by Jacobson's density theorem we may assume that there exists a division ring D such that R is dense in a module V over D. Let $\gamma\colon R \to \operatorname{End}_D(V)$, $r \mapsto \gamma_r$, where $\gamma_r(v) = rv$. Since V is faithful, γ is injective. Thus $R \simeq \gamma(R)$.

If $\dim_D V < \infty$, the result follows from Proposition 11.2. Assume that $\dim_D V = \infty$ and let $\{u_1, u_2, \dots\}$ be a linearly independent set. For each $m \in \mathbb{Z}_{>0}$ let V_m be the subspace generated by $\{u_1, \dots, u_m\}$ and $R_m = \{r \in R : rV_m \subseteq V_m\}$. Then R_m is a subring of R. Since R is dense in V, the map

$$R_m \to \operatorname{End}_D(V_m), \quad r \mapsto \gamma_r|_{V_m}$$

is a surjective ring homomorphism. □

Lecture 8

§12. Prime rings

In commutative algebra, domains play a fundamental role. In non-commutative algebra, certain things could be quite different. For example, the ring $M_n(\mathbb{C})$ is not a domain. We need a non-commutative generalization of domains.

Definition 12.1. Let R be a ring (not necessarily with one). Then R is **prime** if for $x, y \in R$ such that $xRy = \{0\}$ it follows that $x = 0$ or $y = 0$.

A ring R is a **domain** if $xy = 0$ implies $x = 0$ or $y = 0$. Each domain is trivially a prime ring.

Example 12.2. A commutative ring is prime if and only if it is a domain, as $ab = 0$ if and only if $aRb = \{0\}$.

Example 12.3. A non-zero ideal of a prime ring is a prime ring.

Exercise 12.4. A ring is a domain if and only if it is both prime and reduced.

A characterization of prime rings:

Proposition 12.5. *Let R be a ring. The following statements are equivalent:*

1) *R is prime.*
2) *If I and J are left ideals such that $IJ = \{0\}$, then $I = \{0\}$ or $J = \{0\}$.*
3) *If I and J are ideals such that $IJ = \{0\}$, then $I = \{0\}$ or $J = \{0\}$.*

Proof. We first prove that 1) $\implies$ 2). Let I and J be left ideals such that $IJ = \{0\}$. Then $IRJ = I(RJ) \subseteq IJ = \{0\}$. If $J \neq \{0\}$, $u \in I$ and $v \in J \setminus \{0\}$, then $uRv \in IRJ = \{0\}$. Hence $u = 0$.

The implication 2) $\implies$ 3) is trivial.

Let us prove that 3) $\implies$ 1). Let $x, y \in R$ be such that $xRy = \{0\}$. Let $I = RxR$ and $J = RyR$. Since $IJ = (RxR)(RyR) = R(xRy)R = \{0\}$, we may assume that $I = \{0\}$. In particular, Rx and xR are ideals, as $R(xR) = (Rx)R = \{0\}$. Then $\mathbb{Z}x$ is an ideal of R such that $(\mathbb{Z}x)R = \{0\}$. Thus $x = 0$. $\square$

Simple rings are trivially prime. The converse is not true. For example, $\mathbb{Z}$ is a domain, so it is a prime ring but is not simple.

Example 12.6. If R_1 and R_2 are rings, $R = R_1 \times R_2$ is not prime, as $I = R_1 \times \{0\}$ and $J = \{0\} \times R_2$ are non-zero ideals such that $IJ = \{0\}$.

Theorem 12.7 (Connel). *Let K be a field of characteristic zero and G be a group. Then $K[G]$ is prime if and only if G does not contain non-trivial finite normal subgroups.*

Proof. See for example [14, Theorem 2.10 of Chapter 4]. $\square$

Lemma 12.8. *Let R be a prime ring and L be a minimal left ideal of R. Then R is primitive.*

Proof. Since L is a minimal left ideal, it is simple as a module over R. We claim that L is faithful. Let $y \in L \setminus \{0\}$ and $x \in \mathrm{Ann}_R(L)$. Since $xRy \in xRL \subseteq xL = \{0\}$, it follows that $x = 0$. $\square$

Lemma 12.9. *Let D be a division ring and R be a dense ring in a module V over D. If R is left artininian, then* $\dim_D V < \infty$.

Proof. Assume that $\dim_D V = \infty$ and let $\{u_1, u_2, \dots,\}$ be linearly independent. Since $R \subseteq \mathrm{End}_D(V)$, it follows that V is a module over R with $f \cdot v = f(v)$, where $f \in R$ y $v \in V$. For $n \in \mathbb{Z}_{>0}$ let

$$I_n = \mathrm{Ann}_R(\{u_1, \dots, u_n\}).$$

Each I_j is a left ideal of R and $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$. Let $n \in \mathbb{Z}_{>0}$ and $v \in V \setminus \{0\}$. Since R is dense in V, there exists $f \in R$ such that $f(u_j) = 0$ for all $j \in \{1, \dots, n\}$ and $f(u_{n+1}) = v \neq 0$. Thus $I_1 \supsetneq I_2 \supsetneq \cdots \supsetneq I_n \supsetneq \cdots$, a contradiction. $\square$

Theorem 12.10 (Wedderburn). *Let R be a left artinian ring. The following statements are equivalent:*

1) *R is simple.*
2) *R is prime.*
3) *R is primitive.*
4) *$R \simeq M_n(D)$ for some n and some division ring D.*

Proof. The implication 1) $\implies$ 2) is trivial.

To show that 2) $\implies$ 3) first note that R contains a minimal left ideal, as R is left artinian. By Lemma 12.8, R is primitive.

Now we prove that 3) $\implies$ 4). If R is primitive, Jacobson's density theorem implies that there exists a division ring D such that R is isomorphic to a ring S that is dense in a vector space V over D. Since R is left artinian, Lemma 12.9 implies that $R = \mathrm{End}_D(V) \simeq M_n(D)$, as $\dim_D V < \infty$.

Finally, 4) $\implies$ 1) is trivial, as $M_n(D)$ is simple. $\square$

We now prove Artin–Wedderburn theorem. We will assume that our ring is a unitary left artinian ring. One could prove Artin–Wedderburn's theorem for arbitrary rings –see for example [6]– but when dealing with unitary rings, the proof is simpler. We will prove that left artinian semiprimitive unitary rings are isomorphic to a direct product of finitely many matrix rings. The idea of the proof goes as follows. We know that if R is semiprimitive, then R is a subdirect product of primitive rings; that is there exists an injective map

$$R \to \prod_{i \in I} R/I_i$$

where each I_i is a primitive ideal. Since R is left artinian, the set I will be finite. Moreover, by Wedderburn's theorem, $R/I_i \simeq M_{n_i}(D_i)$ for some division ring D_i. Finally, a non-commutative version of the Chinese remainder theorem implies that the map is fact surjective.

Definition 12.11. An ideal I of R is **prime** if $xRy \subseteq I$ implies $x \in I$ or $y \in I$.

Note that a ring R is prime if and only if $\{0\}$ is a prime ideal. Moreover, an ideal I of R is prime if and only if the ring R/I is prime.

Lemma 12.12. *If R is left artinian and I is a primitive ideal, then I is prime.*

Proof. Since I is primitive, then R/I is primitive. By Wedderburn theorem, R/I is prime and hence I is prime. □

Theorem 12.13 (Artin–Wedderburn). *Let R be a semiprimitive left artinian unitary ring. Then $R \simeq \prod_{i=1}^{k} M_{n_i}(D_i)$ for finitely many division rings $D_1, \dots, D_k$.*

We shall need the following lemmas.

Lemma 12.14. *Let R be a left artinian ring and I be a primitive ideal. Then I is maximal.*

Proof. If I is a primitive ideal of R, then R/I is a primitive ring by Lemma 2.29. By Wedderburn's theorem, R/I is simple. Thus I is maximal by Proposition 2.18. □

Lemma 12.15. *Let $I_1, \dots, I_k$ be finitely many distinct maximal ideals of R. Then $I_2 \cdots I_k \not\subseteq I_1$.*

Proof. Suppose the result is not true and let k be minimal such that $I_2 \cdots I_k \subseteq I_1$. Since the result is clearly true for two distinct maximal ideals, $k \geq 3$. Let $I = I_2 \cdots I_{k-1}$. Since $I \not\subseteq I_1$, there exists $x \in I \setminus I_1$. Moreover, there exists $y \in I_k \setminus I_1$, as $I_k \neq I_1$. Then $(xR)y \subseteq II_k \subseteq I_1$. Since I_1 is prime, it follows that either $x \in I_1$ or $y \in I_1$, a contradiction. □

Lemma 12.16. *Let R be a left artinian ring. Then R has only finitely many primitive ideals.*

Proof. If $I_1, I_2 \dots$ are infinitely many primitive ideals. Since R is left artinian, the sequence $I_1 \supseteq I_1 I_2 \supseteq \cdots$ stabilizes, so there exists n such that

$$I_1 I_2 \cdots I_n = I_1 I_2 \cdots I_n I_{n+1} \subseteq I_{n+1}.$$

This contradicts the previous lemma, as each I_j is a maximal ideal. □

Now we are ready to prove the theorem.

Proof of Theorem 12.13. Let $I_1, \dots, I_k$ be the (distinct) primitive ideals of R. We know that each I_i is a maximal ideal. Thus $I_i + I_j = R$ for $i \neq j$. Since R is semiprimitive, $I_1 \cap \cdots \cap I_k = J(R) = \{0\}$. Let

$$\varphi\colon R \to \prod_{i=1}^{k} R/I_i, \quad x \mapsto (x + I_1, \dots, x + I_k).$$

Then φ is a ring homomorphism with kernel $I_1 \cap \cdots \cap I_k = \{0\}$, so φ is injective. We need to prove that φ is surjective.

We first claim that $I_1 + (I_2 \cdots I_k) = R$. In fact, since $I_1, \dots, I_k$ are maximal ideals, $I_2 \cdots I_k \nsubseteq I_1$. This implies that $I_1 + (I_2 \cdots I_k)$ is an ideal of R that contains I_1. Since I_1 is maximal, $I_1 + (I_2 \cdots I_k) = R$.

Since $I_1 + (I_2 \cdots I_k) = R$, there exists $x_1 \in \prod_{j=2}^{k} I_j$ such that $1 \in x_1 + I_1$. Note that $x_1 = (1 + I_1) \cap (I_2 \cdots I_k) \subseteq I_j$ for all $j \in \{2, \dots, k\}$. Thus

$$\varphi(x_1) = (x + I_1, x + I_2, \dots, x + I_k) = (1 + I_1, I_2, \dots, I_k).$$

Similarly, there exists $x_2 \in 1 + I_2, \dots, x_k \in 1 + I_k$ such that

$$\begin{aligned} \varphi(x_2) &= (I_1, 1 + I_2, \dots, I_k), \\ &\vdots \\ \varphi(x_k) &= (I_1, I_2, \dots, 1 + I_k). \end{aligned}$$

From this, it follows that φ is surjective. Each R/I_i is primitive and hence isomorphic to $M_{n_i}(D_i)$ for some n_i and some division ring D_i. Therefore

$$R \simeq R/I_1 \times \cdots \times R/I_k \simeq \prod_{i=1}^{k} M_{n_i}(D_i).$$ □

§13. Semisimple modules

In the first lectures, we studied semisimple modules over finite-dimensional algebras. Let us now review the theory of semisimple modules over rings. A (finitely generated) module M (over a ring R) is **semisimple** if it is isomorphic to a (finite) direct sum of simple modules.

Definition 13.1. Let R be a ring. A left ideal L is said to be **minimal** if $L \neq \{0\}$ and there is no left ideal L_1 such that $\{0\} \subsetneq L_1 \subsetneq L$.

The ring $\mathbb{Z}$ contains no minimal left ideals. If I is a non-zero left ideal of $\mathbb{Z}$, then $I = (n)$ for some $n > 0$ and $I = (n) \supsetneq (2n)$.

Proposition 13.2. *Let R be a left artinian ring. Then every non-zero left ideal contains a minimal left ideal.*

Proof. Let X be the family of non-zero left ideals contained in I. Then X is non-empty, as $I \in X$. Then X contains a minimal element by Proposition 8.2. $\square$

Definition 13.3. A ring R with identity is **semisimple** if it is a direct sum of (finitely many) minimal left ideals.

Why finitely many minimal left ideals? Suppose that $R = \oplus_{i \in I} L_i$, where $\{L_i : i \in I\}$ is a collection of minimal left ideals of R. Since R is unitary, $1 = \sum_{i \in I} e_i$ (finite sum) for some $e_i \in L_i$. This means that the set $J = \{i \in I : e_i \neq 0\}$ is finite. Note that $R = \oplus_{j \in J} L_j$, as if $x \in R$, then

$$x = x1 = \sum_{j \in J} x e_j \in \bigoplus_{j \in J} L_j.$$

Note that ${}_R R$ is finitely generated by $\{1\}$. Minimal left ideals of R are exactly the simple submodules of ${}_R R$. This means that the ring R is semisimple if and only if the module ${}_R R$ is semisimple.

Proposition 13.4. *Let R be a semisimple ring. Then R is noetherian and artinian.*

Proof. Write R as a direct sum $R = L_1 \oplus \cdots \oplus L_n$ of minimal left ideals. Since each L_j is a simple submodule of ${}_R R$, it follows that

$$L_1 \oplus \cdots \oplus L_n \supsetneq L_2 \oplus \cdots \oplus L_n \supsetneq \cdots \supsetneq L_n \supsetneq \{0\}$$

is a composition series for ${}_R R$ with composition factors $L_1, \dots, L_n$. Since the module ${}_R R$ admits a composition series, it is artinian and noetherian by Theorem 8.10. It follows from the definitions that R is left artinian and left noetherian. $\square$

Exercise 13.5. If R is a semisimple ring, every R-module is semisimple.

Exercise 13.6. Prove that if D is a division ring, then $M_n(D)$ is semisimple.

To see a concrete example, note that $M_2(\mathbb{R})$ is semisimple, as

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\} = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \right\} \oplus \left\{ \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} \right\} \simeq D \oplus D$$

and D is a minimal left ideal of $M_2(\mathbb{R})$.

Theorem 13.7. *Let R be a unitary ring. Then R is semisimple if and only if R is left artinian and $J(R) = \{0\}$.*

Proof. If R is semisimple, then R is left artinian by the previous proposition. Moreover, there are finitely many minimal left ideals $L_1, \dots, L_k$ of R such that $R \simeq L_1 \oplus \cdots \oplus L_k$. We claim that for each $i \in \{1, \dots, k\}$, the ideal $M_i = \sum_{j \neq i} L_j$ of R is maximal. For example, let us prove that M_1 is maximal. If not, there exists a left ideal I of R such that $M_1 \subsetneq I$. Let $x \in I \setminus M_1$ and write

$$x = x_1 + x_2 + \cdots + x_k$$

for $x_j \in L_j$. Since $x_2 + \cdots + x_k \in M_1 \subseteq I$, it follows that $x_1 \in I \cap L_1$, a contradiction.

Conversely, if R is left artinian and $J(R) = \{0\}$, then $R \simeq M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ for division rings $D_1, \dots, D_k$, this is Artin–Wedderburn theorem. Since each $M_{n_j}(D_j)$ is semisimple, it follows that R is semisimple. □

§14. Hopkins–Levitski theorem

Theorem 14.1 (Hopkins–Levitszki). *Let R be a unitary left artinian ring. Then R is left noetherian.*

Proof. Let $J = J(R)$. Since R is left artinian, J is a nilpotent ideal by Theorem 8.17. Let n be such that $J^n = \{0\}$. Now consider the sequence

$$R \supsetneq J \supsetneq J^2 \supsetneq \cdots \supsetneq J^{n-1} \supsetneq J^n = \{0\}.$$

Each J^i/J^{i+1} is a module over R annihilated by J, that is $J \cdot (J^i/J^{i+1}) = \{0\}$, as

$$x \cdot (y + J^{i+1}) = xy + J^{i+1} \subseteq JJ^i + J^{i+1} = J^{i+1}$$

if $x \in J$ and $y \in J^i$. Thus each J^i/J^{i+1} is a module over R/J. Since R/J is left artinian and $J(R/J) = \{0\}$ by Theorem 3.28, it follows that R/J is semisimple. In particular, since every R/J-module is semisimple, each J^i/J^{i+1} is semisimple and hence it is left noetherian.

Now suppose that R is not left noetherian. Let m be the largest non-negative integer such that J^m is not left noetherian. Note that $0 \leq m < n$. The sequence

$$0 \longrightarrow J^{m+1} \longrightarrow J^m \longrightarrow J^m/J^{m+1} \longrightarrow 0$$

is exact. Since J^{m+1} is left noetherian by the definition of m and J^m/J^{m+1} is left noetherian, it follows that J^m is noetherian, a contradiction. □

Theorem 14.2 (Connel). *Let K be a field of characteristic zero and G be a group. Then $K[G]$ is left artinian if and only if G is finite.*

Proof. It follows from Theorem 12.7 and Hopkins–Levitzky theorem; see [14, Theorem 1.1 of Chapter 10]. □

Lecture 9

§15. Andrunakevic–Rjabuhin's theorem

Definition 15.1. A ring R is **reduced** if has no non-zero nilpotent elements.

Every commutative domain is reduced.

Example 15.2. The ring $\mathbb{Z}\times\mathbb{Z}$ with the usual operations is reduced but not a domain.

Example 15.3. The ring $\mathbb{Z}/6$ is reduced. However, $\mathbb{Z}/4$ is not reduced.

Exercise 15.4. Prove that a ring R is **reduced** if and only of for all $r \in R$ such that $r^2 = 0$ one has $r = 0$.

Exercise 15.5. Let $n \geq 2$. Then $\mathbb{Z}/n$ is reduced but not a domain if and only if n is square-free but not prime.

Exercise 15.6. Let R be a commutative ring that is reduced but not a domain. Prove that $R[X]$ is reduced but not a domain.

The previous exercise and induction shows that if R is reduced but not a domain, then so is $R[X_1,\dots,X_n]$.

Example 15.7. Let $R = \mathbb{Z}/3\times\mathbb{Z}/3$ with operations $(a,b)+(c,d) = (a+c,b+d)$ and $(a,b)(c,d) = (ac,ad+bc)$. Then R is a commutative ring with identity $(1,0)$. Since $(0,1)$ is a non-zero nilpotent element, R is not reduced.

Definition 15.8. Let R be a ring and I be an ideal of R. Then R is **reduced** if R/I is a reduced ring.

Let R be a ring and I be a reduced ideal of R. If $ab \in I$, then $ba \in I$. In fact, since $ab \in I$, $(ba)^2 = b(ab)a \in I$. Since R/I is reduced, $ba \in I$.

Theorem 15.9 (Andrunakevic–Rjabuhin). *Let R be a non-zero ring. If R is reduced, then R has no non-zero zero-divisors.*

We shall need a lemma.

Lemma 15.10. *Let R be a ring and I be a reduced ideal. If $S \subseteq R$ is a subset, then the left annihilator of S modulo I is a reduced ideal.*

Proof. We need to show that $A = \{r \in R : rS \subseteq I\}$ is a reduced ideal. A straightforward calculation shows that A is a left ideal. We claim that A is a right ideal. Let $r \in R$ and $a \in A$. Then $as \in I$ for all $s \in S$. Since I is reduced, $sa \in I$ for all $s \in S$. Since I is an ideal of R, $sar \in I$ for all $s \in S$. Using again that I is reduced, $ars \in I$ for all $s \in S$. Thus $ar \in A$.

We now claim that A is reduced. If $a^2 \in A$, then $aas = a^2 s \in I$ for all $s \in S$. Since I is reduced, $asa \in I$ for all $s \in S$. Thus $(as)^2 = (asa)s \in I$ for all $s \in S$. Since I is reduced, $as \in I$ for all $s \in S$. Hence $a \in A$. □

Exercise 15.11. Let R be a ring and I be a reduced ideal. If $S \subseteq R$ is a subset, then the right annihilator of S modulo I is a reduced ideal.

Proof of Theorem 15.9. Let $x \in R \setminus \{0\}$. Let X be the set of reduced ideals I such that $x \notin I$. Since R is reduced, $\{0\}$ is a reduced ideal and hence $X \neq \emptyset$. A standard application of Zorn's lemma shows that there exists a maximal element $M \in X$.

We claim that R/M has no non-zero divisors. If not, there exist $a, b \in R$ such that $ab \in M$, $a \notin M$ and $b \notin M$. Let A be the left annihilator of $\{b\}$ modulo M and B be the right annihilator of $\{a\}$ modulo M. By the previous lemma, A and B are reduced ideals of R. Since $a \in A$, $M \subsetneq A$. Similarly, since $b \in B$, $M \subsetneq B$. Moreover, $AB \subseteq M$. Since $x \in A \cap B$, $x^2 \in AB \subseteq M$. Since M is reduced, $x \in M$, a contradiction. □

Exercise 15.12. Is the ring $\mathbb{C}[\mathbb{Z}/2]$ reduced?

Open problem 15.1. Let G be a torsion-free group. Is $K[G]$ is reduced?

Problem 15.1 is related to other important open problems about group algebras (e.g. zero-divisors, units, indempotents and semisimplicity of group rings).

Exercise 15.13. Prove that idempotents of reduced rings are central.

The previous exercise is used to solve the following problem.

Exercise 15.14. Let R be a ring such that $x^3 = x$ for all $x \in R$. Prove that R is commutative.

Exercise 15.14 is hard. Even harder is the following exercise:

Exercise 15.15. Let R be a ring such that $x^4 = x$ for all $x \in R$. Prove that R is commutative.

Exercise 15.16. Reduced rings are semiprime.

§16. Rickart's theorem

Let K be a field, and G be a group. The **group algebra** $K[G]$ is the vector space (over K) with basis $\{g : g \in G\}$ and the algebra structure is given by the multiplication

$$\left(\sum_{g\in G}\lambda_g g\right)\left(\sum_{h\in G}\mu_h h\right) = \sum_{g,h\in G}\lambda_g\mu_h(gh).$$

Every element of $K[G]$ is a finite sum of the form $\sum_{g\in G}\lambda_g g$.

Exercise 16.1. If G is non-trivial, then $K[G]$ is not simple.

Exercise 16.2. Let $G = C_n$ be the (multiplicative) cyclic group of order n. Prove that $K[G] \simeq K[X]/(X^n - 1)$.

Exercise 16.3. Let G be a finitely-generated torsion-free abelian group. Prove that $K[G]$ is a domain.

Exercise 16.4. Let G be a group and H be a subgroup of G. Let $\alpha \in K[H]$. Prove that α is invertible (resp. a left zero divisor) in $K[H]$ if and only if α is invertible (resp. a left zero divisor) in $K[G]$.

Exercise 16.5. Let G be a group and $\alpha = \sum_{g\in G}\lambda_g g \in K[G]$. The **support** of α is the set

$$\operatorname{supp}\alpha = \{g \in G : \lambda_g \neq 0\}.$$

Prove that if $g \in G$, then $\operatorname{supp}(g\alpha) = g(\operatorname{supp}\alpha)$ and $\operatorname{supp}(\alpha g) = (\operatorname{supp}\alpha)g$.

Exercise 16.6. Let $G = C_2 = \langle g\rangle \simeq \mathbb{Z}/2$ the (multiplicative) group with two elements. Note that every element of $K[G]$ is of the form $a + bg$ for some $a, b \in K$. Prove the following statements:

1) If the characteristic of K is different from two, then

$$K[G] \to K \times K, \quad a1 + bg \mapsto (a+b, a-b),$$

is an algebra isomorphism.

2) If the characteristic of K is two, then

$$K[G] \to \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}, \quad a1 + bg \mapsto \begin{pmatrix} a+b & b \\ 0 & a+b \end{pmatrix},$$

is an algebra isomorphism.

If A is an algebra over K and $\rho\colon G \to \mathcal{U}(A)$ is a group homomorphism, where $\mathcal{U}(A)$ is the group of units of A, then the map

$$K[G] \to A, \quad \sum_{g\in G}\lambda_g g \mapsto \sum_{g\in G}\lambda_g \rho(g),$$

is an algebra homomorphism.

Exercise 16.7. Let $G = C_3$ be the (multiplicative) group of three elements. Prove that $\mathbb{R}[G] \simeq \mathbb{R} \times \mathbb{C}$.

Exercise 16.8. Let $G = \langle r, s : r^3 = s^2 = 1, srs = r^{-1} \rangle$ be the dihedral group of six elements. Prove the following statements:

1) $\mathbb{C}[G] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$.
2) $\mathbb{Q}[G] \simeq \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q})$.

We now consider the following problem. It is known as Jacobson's semisimplicity problem.

Open problem 16.9. Let G be a group and K be a field. When $J(K[G]) = \{0\}$?

As an application of Amitsur's theorem, we prove that complex group algebras have null Jacobson radical. This is known as Rickart's theorem. The original proof found by Rickart uses complex analysis. Here, however, we present an algebraic proof.

Theorem 16.10 (Rickart). *Let G be a group. Then $J(\mathbb{C}[G]) = \{0\}$.*

To prove the theorem, we need a lemma.

Lemma 16.11. *Let G be a group. Then $J(\mathbb{C}[G])$ is nil.*

Proof. We need to show that every element of $J(\mathbb{C}[G])$ is nilpotent. If G is countable, then the result follows from Amitsur's theorem. So assume that G is not countable. Let $\alpha \in J(\mathbb{C}[G])$, say

$$\alpha = \sum_{i=1}^{n} \lambda_i g_i,$$

where $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ and $g_1, \dots, g_n \in G$. Let $H = \langle g_1, \dots, g_n \rangle$. Then $\alpha \in \mathbb{C}[H]$ and H is countable. We claim that $\alpha \in J(\mathbb{C}[H])$. Decompose G as a disjoint union

$$G = \bigcup_{\lambda} x_\lambda H$$

of cosets of H in G. Then $\mathbb{C}[G] = \bigoplus_\lambda x_\lambda \mathbb{C}[H]$ and hence $\mathbb{C}[G] = \mathbb{C}[H] \oplus K$ for some right module K over $\mathbb{C}[H]$ (this follows from the fact that one of the cosets is that of H). Since $\alpha \in J(\mathbb{C}[G])$, for each $\beta \in \mathbb{C}[H]$ there exists $\gamma \in \mathbb{C}[G]$ such that $\gamma(1 - \beta\alpha) = 1$. Write $\gamma = \gamma_1 + \kappa$ for $\gamma_1 \in \mathbb{C}[H]$ and $\kappa \in K$. Then

$$1 = \gamma(1 - \beta\alpha) = \gamma_1(1 - \beta\alpha) + \kappa(1 - \beta\alpha)$$

and hence $\kappa(1 - \beta\alpha) \in K \cap \mathbb{C}[H] = \{0\}$, as $\beta \in \mathbb{C}[H]$. Since $1 = \gamma_1(1 - \beta\alpha)$, it follows that $\alpha \in J(\mathbb{C}[H])$ and the lemma follows from Amitsur's theorem. $\square$

We now prove the theorem.

Proof of Theorem 16.10. For $\alpha = \sum_{i=1}^{n} \lambda_i g_i \in \mathbb{C}[G]$ let

$$\alpha^* = \sum_{i=1}^{n} \overline{\lambda_i} g_i^{-1}.$$

Then $\alpha\alpha^* = 0$ if and only if $\alpha = 0$ and, moreover, $(\alpha\beta)^* = \beta^*\alpha^*$ for all $\beta \in \mathbb{C}[G]$. Assume that $J(\mathbb{C}[G]) \neq \{0\}$ and let $\alpha \in J(\mathbb{C}[G]) \setminus \{0\}$. Then $\beta = \alpha\alpha^* \in J(\mathbb{C}[G])$, as $J(\mathbb{C}[G])$ is an ideal of $\mathbb{C}[G]$. Moreover, the previous lemma implies that β is nilpotent. Note that $\beta \neq 0$, as $\alpha \neq 0$. Now

$$(\beta^m)^* = (\beta^*)^m = \beta^m$$

for all $m \geq 1$. If there exists $k \geq 2$ such that $\beta^k = 0$ and $\beta^{k-1} \neq 0$, then

$$\beta^{k-1}\left(\beta^{k-1}\right)^* = \beta^{2k-2} = 0$$

and hence $\beta^{k-1} = 0$, a contradiction. Thus $\beta = 0$ and therefore $\alpha = 0$. □

Exercise 16.12. If G is a group, then $J(\mathbb{R}[G]) = 0$.

Corollary 16.13. *The ring $\mathbb{C}[G]$ is semiprime.*

Proof. Since $J(\mathbb{C}[G]) = \{0\}$ by Rickart's theorem and the Jacobson radical contains every nil ideal by Proposition 3.6, it follows that $\mathbb{C}[G]$ does not contain non-trivial nil ideals. Thus $\mathbb{C}[G]$ does not contain non-trivial nilpotent ideals and hence $\mathbb{C}[G]$ is semiprime. □

Exercise 16.14. Prove that $Z(\mathbb{C}[G])$ is semiprime.

We now characterize when complex group algebras are left artinian. For that purpose, we need a lemma. This is similar to one of the implications proved in Proposition 1.22. However, in the arbitrary setting we are considering, we need to use Zorn's lemma.

Lemma 16.15. *Let M be a semisimple module and N be a submodule. Then N is a direct summand.*

Sketch of the proof. Let $M = \oplus_{i\in I} M_i$ be a direct sum of simple modules and let $i \in I$. Since $N \cap M_i$ is a submodule of M_i and M_i is simple, it follows that $N \cap M_i = \{0\}$ or $N \cap M_i = M_i$. If $N \cap M_i = M_i$ for all $i \in I$, then $N = M$ and the lemma is proved. So we may assume that there exists $i \in I$ such that $N \cap M_i = \{0\}$. Let X be the set of subsets J of I such that $N \cap (\oplus_{j\in J} M_j) = \{0\}$. Our assumptions imply that X is non-empty. Zorn's lemma implies the existence of a maximal element K. Let $N_1 = \oplus_{k\in K} M_k$. We claim that $N \oplus N_1 = M$. If not, there exists $i \in I$ such that $M_i \nsubseteq N \oplus N_1$. The simplicity of M_i implies that $M_i \cap (N \cap N_1) = \{0\}$, which contradicts the maximality of K. □

A direct application of the lemma proves that complex group algebras of infinite groups are never semisimple.

Proposition 16.16. *If G is an infinite group, then $\mathbb{C}[G]$ is not semisimple.*

Proof. Assume that $R = \mathbb{C}[G]$ is semisimple. Let I be the augmentation ideal of R, that is

$$I = \left\{ \alpha = \sum_{g \in G} \lambda_g g \in R : \sum_{g \in G} \lambda_g = 0 \right\}.$$

By the previous lemma, there exists a non-zero ideal J such that $R = I \oplus J$. Since R is unitary, there exist $e \in I$ and $f \in J$ such that $1 = e + f$. If $x \in I$, then $x = xe + xf$ and hence $xf = x - xe \in I \cap J = \{0\}$. Since $x = xe$ for all $x \in I$, it follows that $e = e^2$. Similarly, one proves that $f^2 = f$. Moreover, $ef = 0$, as $ef \in I \cap J = \{0\}$. Since I is the augmentation ideal of R and $If = (Re)f = R(ef) = \{0\}$, we conclude that $(g-1)f = 0$ for all $g \in G$, as $g - 1 \in I$. If $f = \sum_{h \in G} \lambda_h h$ (finite sum), then

$$f = gf = \sum_{h \in G} \lambda_h (gh) = \sum_{h \in G} \lambda_{g^{-1}h} h.$$

Thus $\lambda_h = \lambda_{g^{-1}h}$ for all $g, h \in G$. Since G is infinite, some $\lambda_g = 0$ and hence $f = 0$. Thus $e = 1$ and $I = \mathbb{C}[G]$, a contradiction. □

Theorem 16.17. *Let G be a group. Then $\mathbb{C}[G]$ is left artinian if and only if G is finite.*

Proof. If G is finite, then $\mathbb{C}[G]$ is left artinian because $\dim \mathbb{C}[G] = |G| < \infty$. So assume that G is infinite. By Rickart's theorem, $J(\mathbb{C}[G]) = 0$. Moreover, $\mathbb{C}[G]$ is not semisimple by the previous proposition. Thus $\mathbb{C}[G]$ is not left artinian by Theorem 13.7. □

§17. Maschke's theorem

We now present another instance of the Jacobson semisimplicity problem. In this case, our result is for finite groups.

Theorem 17.1 (Maschke). *Let G be a finite group. Then $J(K[G]) = 0$ if and only if the characteristic of K is zero or does not divide the order of G.*

Proof. Assume that $G = \{g_1, \dots, g_n\}$, where $g_1 = 1$. Let

$$\rho \colon K[G] \to K, \quad \alpha \mapsto \operatorname{trace}(L_\alpha),$$

where $L_\alpha(\beta) = \alpha\beta$. Then

$$\rho(g_i) = \begin{cases} n & \text{if } i = 1, \\ 0 & \text{if } 2 \leq i \leq n, \end{cases}$$

as $L_{g_i}(g_j) = g_i g_j \neq g_j$, the matrix of L_{g_i} in the basis $\{g_1, \dots, g_n\}$ contains zeros in the main diagonal.

Assume that $J = J(K[G])$ is non-zero and let $\alpha = \sum_{i=1}^{n} \lambda_i g_i \in J \setminus \{0\}$. Without loss of generality we may assume that $\lambda_1 \neq 0$ (if $\lambda_1 = 0$ there exists some $\lambda_i \neq 0$ and we need to take $g_i^{-1}\alpha \in J$). Then

$$\rho(\alpha) = \sum_{i=1}^{n} \lambda_i \rho(g_i) = n\lambda_1.$$

Since G is finite, $K[G]$ is a finite-dimensional algebra and hence $K[G]$ is left artinian. Since J is a nilpotent ideal, in particular, α is a nilpotent element. Then L_α is nilpotent and hence $0 = \rho(\alpha) = n\lambda_1$. This implies that the characteristic of the field K divides n.

Conversely, let K be a field of prime characteristic and that this prime divides n. Let $\alpha = \sum_{i=1}^{n} g_i$. Since $\alpha g_j = g_j \alpha = \alpha$ for all $j \in \{1, \dots, n\}$, the set $I = K[G]\alpha$ is an ideal of $K[G]$. Since, moreover,

$$\alpha^2 = \sum_{i=1}^{n} g_i \alpha = n\alpha = 0$$

in the field K, it follows that I is a nilpotent non-zero ideal. Thus $J(K[G]) \neq \{0\}$, as Proposition 3.6 yields $I \subseteq J(K[G])$. $\square$

Since the Jacobson radical of a group algebra of a finite group contains every nil left ideal, the following consequence of the theorem follows immediately:

Corollary 17.2. *Let G be a finite group. Then $K[G]$ does not contain non-zero nil left ideals.*

Lecture 10

§18. Herstein's theorem

Our aim now is to answer the following question: When a group algebra is algebraic? Herstein's theorem provides a solution in the case of fields of characteristic zero. In prime characteristic, the problem is still open.

Definition 18.1. A group G is **locally finite** if every finitely generated subgroup of G is finite.

If G is a locally finite group, then every element $g \in G$ has finite order, as the subgroup $\langle g \rangle$ is finite because it is finitely generated.

Example 18.2. Every finite group is locally finite

Example 18.3. The group $\mathbb{Z}$ is not locally finite because it is torsion-free.

Example 18.4. Let p be a prime number. The **Prüfer's group**

$$\mathbb{Z}(p^\infty) = \{z \in \mathbb{C} : z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}_{>0}\},$$

is locally finite.

Example 18.5. Let X be an infinite set and $\mathbb{S}_X$ be the set of bijective maps $X \to X$ moving only finitely many elements of X. Then $\mathbb{S}_X$ is locally finite.

A group G is a **torsion** group if every element of G has finite order. Locally finite groups are torsion groups.

Example 18.6. Abelian torsion groups are locally finite. Let G be a locally finite abelian group and H be a finitely generated subgroup. Since G is an abelian torsion group, so is H. Thus H is finite by the structure theorem of abelian groups.

Proposition 18.7. *Let G be a group and N be a normal subgroup of G. If N and G/N are locally finite, then G is locally finite.*

Proof. Let $\pi\colon G \to G/N$ be the canonical map and $\{g_1,\dots,g_n\}$ be a finite subset of G. Since G/N is locally finite, the subgroup Q of G/N generated by $\pi(g_1),\dots,\pi(g_n)$ is finite, say

$$Q = \{\pi(g_1),\dots,\pi(g_n),\pi(g_{n+1}),\dots,\pi(g_m)\}.$$

For each $i,j \in \{1,\dots,n\}$ there exist $u_{ij} \in N$ and $k \in \{1,\dots,m\}$ such that $g_i g_j = u_{ij} g_k$. Let U be the subgroup of G generated by $\{u_{ij} : 1 \leq i,j \leq n\}$. Since N is locally finite, U is finite. Moreover, since each $g_i g_j g_l$ can be written as

$$g_i g_j g_l = u_{ij} g_k g_l = u_{ij} u_{kl} g_t = u g_t$$

for some $u \in U$ and $t \in \{1,\dots,m\}$, it follows that the subgroup H of G generated by $\{g_1,\dots,g_n\}$ is finite, as $|H| \leq m|U|$. □

A group G is **solvable** if there exists a sequence of subgroups

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = G \tag{10.1}$$

where each G_i is normal in G_{i+1} and each quotient G_i/G_{i-1} is abelian.

Example 18.8. Abelian groups are solvable.

Subgroups and quotients of solvable groups are solvable.

Example 18.9. Groups of order < 60 are solvable.

Example 18.10. $\mathbb{A}_5$ and $\mathbb{S}_5$ are not solvable.

A famous theorem of Burnside states that groups of order $p^a q^b$ for prime numbers p and q are solvable A much harder theorem proved by Feit and Thompson states that groups of odd order are solvable.

Proposition 18.11. *If G is a solvable torsion group, then G is locally finite.*

Proof. We proceed by induction on n, the length of the sequence (10.1). If $n = 1$, then G is finite because it is abelian and a torsion group. Now assume the result holds for solvable groups of length $n-1$ and let G be a solvable group with a sequence (10.1). Since G_{n-1} is a solvable torsion group, the inductive hypothesis implies that G_{n-1} is locally finite. Since G/G_{n-1} is an abelian torsion group, it is locally finite. The result now follows from Proposition 18.7. □

We now prove Herstein's theorem.

Theorem 18.12 (Herstein). *If G is a locally finite group, then $K[G]$ is algebraic. Conversely, if $K[G]$ is algebraic and K has characteristic zero, then G is locally finite.*

Proof. Assume that G is locally finite. Let $\alpha \in K[G]$. The subgroup $H = \langle \operatorname{supp} \alpha \rangle$ is finite, as it is finitely generated. Since $\alpha \in K[H]$ and $\dim_K K[H] < \infty$, the set $\{1, \alpha, \alpha^2, \dots\}$ is linearly dependent. Thus α is algebraic over K.

Let $\{x_1, \dots, x_m\}$ be a finite subset of G. Adding inverses if needed, we may assume that $\{x_1, \dots, x_m\}$ generates the subgroup $H = \langle x_1, \dots, x_m \rangle$ as a semigroup. Let

$$\alpha = x_1 + \cdots + x_m \in K[G].$$

Since α is algebraic over K, there exist $b_0, b_1, \dots, b_{n+1} \in K$ such that

$$b_0 + b_1 \alpha + \cdots + b_{n+1} \alpha^{n+1} = 0,$$

where $b_{n+1} \neq 0$. Rewrite this as

$$\alpha^{n+1} = a_0 + a_1 \alpha + \cdots + a_n \alpha^n$$

for some $a_0, \dots, x_n \in K$. Let $w = x_{i_1} \cdots x_{i_{n+1}} \in H$ be a word of length $n+1$. Note that

$$\alpha^k = (x_1 + \cdots + x_m)^k = \sum x_{i_1} \cdots x_{i_k}$$

for all k. Two words $x_{i_1} \cdots x_{i_k}$ and $x_{j_1} \cdots x_{j_k}$ could represent the same element of the group H. In this case, the coefficient of $x_{i_1} \cdots x_{i_k} = x_{j_1} \cdots x_{j_k}$ in α^k will be a positive integer ≥ 2.

Since K is of characteristic zero, it follows that $w \in \operatorname{supp}(\alpha^{n+1})$. Since, moreover, $\alpha^{n+1} = \sum_{j=0}^{n} a_j \alpha^j$, it follows that $w \in \operatorname{supp}(\alpha^j)$ for some $j \in \{0, \dots, n\}$. Thus each word in the letters x_j of length $n+1$ can be written as a word in the letters x_j of length $\leq n$. Therefore H is finite and hence G is locally finite. $\square$

§19. Formanek's theorem, I

Exercise 19.1. Let A be an algebraic algebra and $a \in A$.

1) a is a left zero divisor if and only if a is a right zero divisor.
2) a is left invertible if and only if a is right invertible.
3) a is invertible if and only if a is not a zero divisor.

Exercise 19.2. For $\alpha = \sum_{g \in G} \alpha_g g \in \mathbb{C}[G]$ let $|\alpha| = \sum_{g \in G} |\alpha_g| \in \mathbb{R}$. Prove the following statements:

1) $|\alpha + \beta| \leq |\alpha| + |\beta|$, and
2) $|\alpha\beta| \leq |\alpha||\beta|$

for all $\alpha, \beta \in \mathbb{C}[G]$.

Theorem 19.3 (Formanek). *Let G be a group. If every element of $\mathbb{Q}[G]$ is invertible or a zero divisor, then G is locally finite.*

Proof. Let $\{x_1,\dots,x_n\}$ be a finite subset of G. Adding inverses if needed, we may assume that $\{x_1,\dots,x_n\}$ generates the subgroup $H=\langle x_1,\dots,x_n\rangle$ as a semigroup. Let

$$\alpha=\frac{1}{2n}(x_1+\cdots+x_n)\in\mathbb{Q}[G]$$

Note that $|\alpha|\leq 1/2$. We claim that $1-\alpha\in\mathbb{Q}[G]$ is invertible. If not, then it is a zero divisor. If there exists $\delta\in\mathbb{Q}[G]$ such that $\delta(1-\alpha)=0$, then $\delta=\delta\alpha$. Since

$$|\delta|=|\delta\alpha|\leq|\delta||\alpha|=|\delta|/2,$$

it follows that $\delta=0$. Similarly, $(1-\alpha)\delta=0$ implies $\delta=0$.

Let $\beta=(1-\alpha)^{-1}\in\mathbb{Q}[G]$. For each k let

$$\gamma_k=(1+\alpha+\cdots+\alpha^k)-\beta.$$

Then

$$\begin{aligned}\gamma_k(1-\alpha)&=(1+\alpha+\cdots+\alpha^k-\beta)(1-\alpha)\\&=(1+\alpha+\cdots+\alpha^k)(1-\alpha)-\beta(1-\alpha)=-\alpha^{k+1}\end{aligned}$$

and thus $\gamma_k=-\alpha^{k+1}\beta$. Since

$$|\gamma_k|=|-\alpha^{k+1}\beta|\leq|\beta||\alpha^{k+1}|\leq\frac{|\beta|}{2^{k+1}},$$

it follows that $\lim_{k\to\infty}|\gamma_k|=0$.

We now prove that $H\subseteq\operatorname{supp}\beta$. This will finish the proof of the theorem, as $\operatorname{supp}\beta$ is a finite subset of G by definition. If $H\not\subseteq\operatorname{supp}\beta$, let $h\in H\setminus\operatorname{supp}\beta$. Assume that $h=x_{i_1}\cdots x_{i_m}$ is a word in the letters x_j of length m. Let c_j be the coefficient of h in α^j. Then $c_0+\cdots+c_k$ is the coefficient of h in γ_k, but

$$|\gamma_k|\geq c_0+c_1+\cdots+c_k\geq c_m>0$$

for all $k\geq m$, as each c_j is non-negative, a contradiction to $|\gamma_k|\to 0$ si $k\to\infty$. $\square$

§20. Tensor products

The **tensor product** of the vector spaces (over K) U and V is the quotient vector space $K[U\times V]/T$, where $K[U\times V]$ is the vector space with basis

$$\{(u,v):u\in U,v\in V\}$$

and T is the subspace generated by elements of the form

$$(\lambda u+\mu u',v)-\lambda(u,v)-\mu(u',v),\quad(u,\lambda v+\mu v')-\lambda(u,v)-\mu(u,v')$$

for $\lambda,\mu \in K$, $u,u' \in U$ and $v,v' \in V$. The tensor product of U and V will be denoted by $U \otimes_K V$ or $U \otimes V$ when the base field is clear from the context. For $u \in U$ and $v \in V$ we write $u \otimes v$ to denote the coset $(u,v)+T$.

Theorem 20.1. *Let U and V be vector spaces. Then there exists a bilinear map $U \times V \to U \otimes V$, $(u,v) \mapsto u \otimes v$, such that each element of $U \otimes V$ is a finite sum of the form*

$$\sum_{i=1}^{N} u_i \otimes v_i$$

for some $u_1,\dots,u_N \in U$ and $v_1,\dots,v_N \in V$. Moreover, if W is a vector space and $\beta\colon U \times V \to W$ is a bilinear map, there exists a linear map $\overline{\beta}\colon U \otimes V \to W$ such that $\overline{\beta}(u \otimes v) = \beta(u,v)$ for all $u \in U$ and $v \in V$.

Proof. By definition, the map

$$U \times V \to U \otimes V, \quad (u,v) \mapsto u \otimes v,$$

is bilinear. From the definitions, it follows that $U \otimes V$ is a finite linear combination of elements of the form $u \otimes v$, where $u \in U$ and $v \in V$. Since $\lambda(u \otimes v) = (\lambda u) \otimes v$ for all $\lambda \in K$, the first claim follows.

Since the elements of $U \times V$ form a basis of $K[U \times V]$, there exists a linear map

$$\gamma\colon K[U \times V] \to W, \quad \gamma(u,v) = \beta(u,v).$$

Since β is bilinear by assumption, $T \subseteq \ker\gamma$. It follows that there exists a linear map $\overline{\beta}\colon U \otimes V \to W$ such that

$$\begin{tikzcd} K[U \times V] \arrow[r] \arrow[d] & W \\ U \otimes V \arrow[ur, dashed] & \end{tikzcd}$$

commutes. In particular, $\overline{\beta}(u \otimes v) = \beta(u,v)$. □

Exercise 20.2. Prove that the properties of the previous theorem characterize tensor products up to isomorphism.

Some properties:

Proposition 20.3. *Let $\varphi\colon U \to U_1$ and $\psi\colon V \to V_1$ be linear maps. There exists a unique linear map $\varphi \otimes \psi\colon U \otimes V \to U_1 \otimes V_1$ such that*

$$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v)$$

for all $u \in U$ and $v \in V$.

Proof. Since $U \times V \to U_1 \otimes V_1$, $(u,v) \mapsto \varphi(u) \otimes \psi(v)$, is bilinear, there exists a linear map $U \otimes V \to U_1 \otimes V_1$, $u \otimes v \to \varphi(u) \otimes \psi(v)$. Thus

$$\sum u_i \otimes v_i \mapsto \sum \varphi(u_i) \otimes \psi(v_i)$$

is well-defined. □

Exercise 20.4. Prove the following statements:

1) $(\varphi \otimes \psi)(\varphi' \otimes \psi') = (\varphi\varphi') \otimes (\psi\psi')$.
2) If φ and ψ are isomorphisms, then $\varphi \otimes \psi$ is an isomorphism.
3) $(\lambda\varphi + \lambda'\varphi') \otimes \psi = \lambda\varphi \otimes \psi + \lambda'\varphi' \otimes \psi$.
4) $\varphi \otimes (\lambda\psi + \lambda'\psi') = \lambda\varphi \otimes \psi + \lambda'\varphi \otimes \psi'$.
5) If $U \simeq U_1$ and $V \simeq V_1$, then $U \otimes V \simeq U_1 \otimes V_1$.

The following proposition is extremely useful:

Proposition 20.5. *If U and V are vector spaces, then $U \otimes V \simeq V \otimes U$.*

Proof. Since $U \times V \to V \otimes U$, $(u, v) \mapsto v \otimes u$, is bilinear, there exists a linear map $U \otimes V \to V \otimes U$, $u \otimes v \mapsto v \otimes u$. Similarly, there exists a linear map $V \otimes U \to U \otimes V$, $v \otimes u \mapsto u \otimes v$. Thus $U \otimes V \simeq V \otimes U$. □

Exercise 20.6. Prove that $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$.

Exercise 20.7. Prove that $U \otimes K \simeq K \simeq K \otimes U$.

Proposition 20.8. *Let U and V be vector spaces. If $\{u_1, \dots, u_n\}$ is a linearly independent subset of U and $v_1, \dots, v_n \in V$ is such that $\sum_{i=1}^n u_i \otimes v_i = 0$, then $v_i = 0$ for all $i \in \{1, \dots, n\}$.*

Proof. Let $i \in \{1, \dots, n\}$ and

$$f_i \colon U \to K, \quad f_i(u_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Since the map $U \times V \to V$, $(u, v) \mapsto f_i(u)v$, is bilinear, there exists a linear map $\alpha_i \colon U \otimes V \to V$ such that $\alpha_i(u \otimes v) = f_i(u)v$. Thus

$$v_i = \sum_{j=1}^n \alpha_i(u_j \otimes v_j) = \alpha_i\left(\sum_{j=1}^n u_j \otimes v_j\right) = 0.$$ □

Exercise 20.9. Prove that $u \otimes v = 0$ and $v \neq 0$ imply $u = 0$.

Theorem 20.10. *Let U and V be vector spaces. If $\{u_i : i \in I\}$ is a basis of U and $\{v_j : j \in J\}$ is a basis of V, then $\{u_i \otimes v_j : i \in I, j \in J\}$ is a basis of $U \otimes V$.*

Proof. The $u_i \otimes v_j$ are generators of $U \otimes V$, as $u = \sum_i \lambda_i u_i$ and $v = \sum_j \mu_j v_j$ imply $u \otimes v = \sum_{i,j} \lambda_i \mu_j u_i \otimes v_j$. We now prove that the $u_i \otimes v_j$ are linearly independent. We need to show that each finite subset of the $u_i \otimes v_j$ is linearly independent. If $\sum_k \sum_l \lambda_{kl} u_{i_k} \otimes v_{j_l} = 0$, then $0 = \sum_k u_{i_k} \otimes \left(\sum_l \lambda_{kl} v_{j_l}\right)$. Since the u_{i_k} are linearly independent, Proposition 20.8 implies that $\sum_l \lambda_{kl} v_{j_l} = 0$. Thus $\lambda_{kl} = 0$ for all k, l, as the v_{j_l} are linearly independent. □

If U and V are finite-dimensional vector spaces, then

$$\dim(U\otimes V)=(\dim U)(\dim V).$$

Corollary 20.11. *If $\{u_i : i\in I\}$ is a basis of U, then every element of $U\otimes V$ can be written uniquely as a finite sum $\sum_i u_i\otimes v_i$.*

Proof. Every element of $U\otimes V$ is a finite sum $\sum_i x_i\otimes y_i$, where $x_i\in U$ and $y_i\in V$. If $x_i=\sum_j \lambda_{ij}u_j$, then

$$\sum_i x_i\otimes y_i=\sum_i\left(\sum_j \lambda_{ij}u_j\right)\otimes y_i=\sum_j u_j\otimes\left(\sum_i \lambda_{ij}y_i\right). \qquad \square$$

Exercise 20.12. Let A and B be algebras. Prove that $A\otimes B$ is an algebra with

$$(a\otimes b)(x\otimes y)=ax\otimes by.$$

Exercise 20.13. Prove the following statements:

1) $A\otimes B\simeq B\otimes A$.
2) $(A\otimes B)\otimes C\simeq A\otimes(B\otimes C)$.
3) $A\otimes K\simeq A\simeq K\otimes A$.
4) If $A\otimes A_1$ and $B\otimes B_1$, then $A\otimes B\simeq A_1\otimes B_1$.

Some examples:

Proposition 20.14. *If G and H are groups, then $K[G]\otimes K[H]\simeq K[G\times H]$.*

Proof. The set $\{g\otimes h : g\in G, h\in H\}$ is a basis of $K[G]\otimes K[H]$ and the elements of $G\times H$ form a basis of $K[G\times H]$. There exists a linear isomorphism

$$K[G]\otimes K[H]\to K[G\times H],\quad g\otimes h\mapsto (g,h),$$

that is multiplicative. Thus $K[G]\otimes K[H]\simeq K[G\times H]$ as algebras. $\square$

Proposition 20.15. *If A is an algebra, then $A\otimes K[X]\simeq A[X]$.*

Proof. Each element of $A\otimes K[X]$ can be written uniquely as a finite sum of the form $\sum a_i\otimes X^i$. Routine calculations show that $A\otimes K[X]\mapsto A[X]$, $\sum a_i\otimes X^i\mapsto\sum a_iX^i$, is a linear algebra isomorphism. $\square$

Exercise 20.16. Prove that if A is an algebra, then $A\otimes M_n(K)\simeq M_n(A)$. In particular, $M_n(K)\otimes M_m(K)\simeq M_{nm}(K)$.

Proposition 20.15 and Exercise 20.16 are examples of a procedure known as **scalar extensions**.

Theorem 20.17. *Let A be an algebra over K and E be an extension of K (this just simply means that K is a subfield of E). Then $A^E = E \otimes_K A$ is an algebra over E with respect to the scalar multiplication*

$$\lambda(\mu \otimes a) = (\lambda\mu) \otimes a,$$

for all $\lambda, \mu \in E$ and $a \in A$.

Proof. Let $\lambda \in E$. Since $E \times A \to E \otimes_K A$, $(\mu, a) \mapsto (\lambda\mu) \otimes a$, is K-bilinear, there exists a linear map $E \otimes_K A \to E \otimes_K A$, $\mu \otimes a \mapsto (\lambda\mu) \otimes a$. The scalar multiplication is then well-defined and

$$\lambda(u + v) = \lambda u + \lambda v$$

for all $\lambda \in E$ and $u, v \in E \otimes_K A$. Moreover,

$$(\lambda + \mu)u = \lambda u + \mu u, \quad (\lambda\mu)u = \lambda(\mu u), \quad \lambda(uv) = (\lambda u)v = u(\lambda v)$$

for all $u, v \in E \otimes_K A$ and $\lambda, \mu \in E$. □

Exercise 20.18. Prove the following statements:

1) $\{1\} \otimes A$ is a subalgebra of A^E isomorphic to A.
2) If $\{a_i : i \in I\}$ is a basis of A, then $\{1 \otimes a_i : i \in I\}$ is a basis of A^E.

Exercise 20.19. Prove that if G is a group and K is a subfield of E, then

$$E \otimes_K K[G] \simeq E[G].$$

§21. Formanek's theorem, II

The combination of technique known as extensions of scalars we have seen in the previous section and Formanek's theorem for rational group algebras yield the following general result.

Theorem 21.1 (Formanek). *Let K be a field of characteristic zero and let G be a group. If every element of $K[G]$ is invertible or a zero divisor, then G is locally finite.*

Proof. Since K is of characteristic zero, $\mathbb{Q} \subseteq K$. Then $K[G] \simeq K \otimes_{\mathbb{Q}} \mathbb{Q}[G]$. Each $\beta \in K \otimes_{\mathbb{Q}} \mathbb{Q}[Q]$ can be written uniquely as

$$\beta = 1 \otimes \beta_0 + \sum k_i \otimes \beta_i,$$

where $\{1, k_1, k_2, \dots,\}$ is a basis of K as a $\mathbb{Q}$-vector space. Let $\alpha \in \mathbb{Q}[G]$ and let $\beta \in K[G]$ be such that $\alpha\beta = 1$. Since

$$1 \otimes 1 = (1 \otimes \alpha)\beta = 1 \otimes \alpha\beta_0 + \sum k_i \otimes \alpha\beta_i,$$

it follows that $\alpha\beta_0 = 1$. Similarly, if $\alpha\beta = 0$, then $\alpha\beta_j = 0$ for all j. Since each $\alpha \in \mathbb{Q}[G]$ is invertible or a zero divisor, Formanek's theorems for $\mathbb{Q}$ applies. $\square$

Lecture 11

§22. Wedderburn's little theorem

Definition 22.1. The n-th cyclotomic polynomial is defined as the polynomial

$$\Phi_n(X) = \prod (X - \zeta), \tag{11.1}$$

where the product is taken over all n-th primitive roots of one.

Some examples:

$$\begin{aligned}
\Phi_2 &= X - 1,\\
\Phi_3 &= X^2 + X + 1,\\
\Phi_4 &= X^2 + 1,\\
\Phi_5 &= X^4 + X^3 + X^2 + X + 1,\\
\Phi_6 &= X^2 - X + 1,\\
\Phi_7 &= X^6 + X^5 + \cdots + X + 1.
\end{aligned}$$

Lemma 22.2. *If $n \in \mathbb{Z}_{>0}$, then*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Proof. Write

$$X^n - 1 = \prod_{j=1}^{n} (X - e^{2\pi i j/n}) = \prod_{d|n} \prod_{\substack{1 \le j \le n \\ \gcd(j,n)=d}} (X - e^{2\pi i j/n}) = \prod_{d|n} \Phi_d(X). \qquad \square$$

Lemma 22.3. *If $n \in \mathbb{Z}_{>0}$, then $\Phi_n(X) \in \mathbb{Z}[X]$.*

Proof. We proceed by induction on n. The case $n = 1$ is trivial, as $\Phi_1(X) = X - 1$. Assume that $\Phi_d(X) \in \mathbb{Z}[X]$ for all $d < n$. Then

$$\prod_{d|n, d\neq n} \Phi_d(X) \in \mathbb{Z}[X]$$

is a monic polynomial. Thus $\Phi_n(X)/\prod_{d|n,d<n} \Phi_d(X) \in \mathbb{Z}[X]$. □

Theorem 22.4 (Wedderburn). *Every finite division ring is a field.*

Proof. Let D be a finite division ring and $K = Z(D)$. Then K is a finite field, say $|K| = q$. We claim that $|q - \zeta| > q - 1$ for all n-th root of one $\zeta \neq 1$. In fact, write $\zeta = \cos\theta + i\sin\theta$. Then $\cos\theta < 1$ and

$$|q-\zeta|^2 = q^2 - (2\cos\theta)q + 1 > (q-1)^2.$$

Note that K is a D-vector space. Let $n = \dim_K D$. We claim that $n = 1$. If $n > 1$, the class equation for the group $D^\times = D \setminus \{0\}$ implies that

$$q^n - 1 = q - 1 + \sum_{j=1}^{m} \frac{q^n - 1}{q^{d_j} - 1}, \tag{11.2}$$

where $1 < \frac{q^n-1}{q^{d_j}-1} \in \mathbb{Z}$ for all $j \in \{1, \dots, m\}$. Since $d^{d_j} - 1$ divides $q^n - 1$, each d_j divides n. In particular, (11.1) implies that

$$X^n - 1 = \Phi_n(X)(X^{d_j} - 1)h(X) \tag{11.3}$$

for some $h(X) \in \mathbb{Z}[X]$. By evaluating (11.3) in $X = q$ we obtain that $\Phi_n(q)$ divides $q^n - 1$ and that $\Phi_n(q)$ divides $\frac{q^n-1}{q^{d_j}-1}$. By (11.2), $\Phi_n(q)$ divides $q - 1$. Thus

$$q - 1 \geq |\Phi_n(q)| = \prod |q - \zeta| > q - 1,$$

as each $|q - \zeta| > q - 1$, a contradiction. □

There are several proofs of Wedderburn's theorem. For example, [19] contains a proof that uses only elementary linear algebra. In [15, Chapter 14] the theorem is proved using group theory.

Theorem 22.5. *Let D be a division ring of characteristic $p > 0$. If G is a subgroup of $D \setminus \{0\}$, then G is cyclic.*

We shall need a lemma.

Lemma 22.6. *Let K be a field. Any finite subgroup of $K \setminus \{0\}$ is cyclic.*

Proof. Let G be a finite subgroup of $K \setminus \{0\}$ and $n = |G|$. For a divisor d of n, let $f(d)$ be the number of elements of G of order d. Then

$$\sum_{d|n} f(d) = n.$$

We claim that if $d \mid n$ is such that $f(d) \neq 0$, then $f(d) = \varphi(d)$, where φ is the Euler function. In fact, if $f(d) \neq 0$, then there exists $g \in G$ such that $|g| = d$. Let $H = \langle g \rangle$ be the subgroup of G generated by g. Every element of H is a root of the polynomial $p(X) = X^d - 1 \in D[X]$. Since $p(X)$ has at most d roots, H is the set of roots of $p(X)$. In particular, $g^m \in H$ and $|g^m| = d$ if and only if $\gcd(m,d) = 1$. Hence $f(d) = \varphi(d)$.

The previous claim shows that, in particular, $f(n) = \varphi(n) \neq 0$. Hence there exists $g \in G$ such that $|g| = n = |G|$ and G is cyclic. □

Proof of Theorem 22.5. Let $F = \sum_{g \in G}(\mathbb{Z}/p)g$. Then F is a finite subring of D. Since D is a domain, F is a domain. Let $\alpha \in F \setminus \{0\}$. Then $\{\lambda\alpha : \lambda \in F\} = F$. Since $\lambda\alpha = 1$ for some $\lambda \in F$, F is a division ring. By Wedderburn's theorem, F is a field. Note that $G \subseteq F$. Therefore G is cyclic by the previous lemma. □

§23. Zsigmondy's theorem

One of Wedderburn's original proof of Theorem 22.4 uses a result proved by Zsigmondy [21]. Zsigmondy's theorem is quite popular in mathematical contests.

Theorem 23.1 (Zsigmondy). *Let $a > b \geq 1$ be such that $\gcd(a,b) = 1$ and $n \geq 2$. Then there exists a prime divisor of $a^n - b^n$ that does not divide $a^k - b^k$ for all $k \in \{1, \dots, n-1\}$ except when $n = 2$ and $a+b$ is a power of two or $(a,b,n) = (2,1,6)$.*

Proof. See for example [20]. □

We now quickly sketch a proof of Wedderburn 's theorem 22.4 based on Zsigmondy's theorem.

Let D be a division ring of dimension n over $\mathbb{Z}/p$ for a prime number p. Assume first that there exists a prime number q such that $q \nmid p$ and the order of p modulo q is n. Let $x \in D \setminus \{0\}$ be an element of order q and F be the subring of D generated by g. Note that F is a finite-dimensional $(\mathbb{Z}/p)$-vector space. Let $m = \dim F$. Since $g^{p^m-1} = 1$, q divides $p^m - 1$. Thus $m = n$ and hence $D = F$ is commutative.

Assume now that there is no prime number q such that $q \nmid p$ and the order of p modulo q is n. By Zsigmondy's theorem, $n = 2$ or $n = 6$ and $p = 2$. If $n = 2$, then D is commutative, as it is the subring generated by any element of $D \setminus \mathbb{Z}/p$. If $n = 6$ and $p = 2$, then the order of 2 modulo 9 is 6. Since $D \setminus \{0\}$ contains a subgroup of order 9 and all groups of order 9 are abelian, we can use the previous argument to complete the proof.

§24. Fermat's last theorem in finite rings

Theorem 24.1. *Let K be a finite field and A be a finite-dimensional K-algebra. For $n \geq 1$, there exist $x, y, z \in A \setminus \{0\}$ such that $x^n + y^n = z^n$ if and only if A is not a division algebra.*

Proof. Assume first that A is a division algebra. By Wedderburn's theorem, A is a finite field, say $|A| = q$. Then $x^{q-1} = 1$ for all $x \in A \setminus \{0\}$. Hence $x^n + y^n = z^n$ does not have a solution.

Conversely, assume that A is not a division algebra. In particular, A is not a field and $|A| > 2$. The equation $x + y = z$ has a solution in $A \setminus \{0\}$ (for example, $x = 1$, $y = z - 1$ and $z \notin \{0, 1\}$ is a solution). Since $\dim A < \infty$, the Jacobson radical $J(A)$ is nilpotent. There are two cases to consider.

If $J(A) \neq \{0\}$, then there exists $a \in A \setminus \{0\}$ such that $a^2 = 0$. Thus $a^n = 0$ for all $n \geq 2$. Hence $x^n + y^n = z^n$ has a non-trivial solution in $A \setminus \{0\}$ for all $n \geq 2$ (for example, take $x = a$ and $y = z = 1$).

If $J(A) = \{0\}$, then A is semisimple and $A \simeq \prod_{i=1}^{k} M_{n_i}(D_i)$ for (finite) division rings $D_1, \dots, D_k$ and integers $n_1, \dots, n_k$. By Wedderburn's theorem, each D_i is a finite field. We consider two possible cases.

If there exists $i \in \{1, \dots, k\}$ such that $n_i > 1$, then $M_{n_i}(D_i)$ has non-zero elements such that their squares are zero. Thus there exists $x \in A \setminus \{0\}$ such that $x^2 = 0$. In particular, $x^n + y^n = z^n$ has a solution.

If $k \geq 2$, then $x = (1, 0, 0, \dots, 0)$, $y = (0, 1, 0, \dots, 0)$ and $z = (1, 1, 0, \dots, 0)$ is a solution of $x^n + y^n = z^n$. □

Lecture 12

§25. Frobenius's theorem

Theorem 25.1 (Frobenius). *Every finite-dimensional real division algebra is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.*

We present an elementary proof. We shall need some lemmas.

Lemma 25.2. *Let D be a real division algebra such that $\dim D = n$. If $x \in D$, then there exists $\lambda \in \mathbb{R}$ such that $x^2 + \lambda x \in \mathbb{R}$.*

Proof. Since $\dim D = n$, the set $\{1, x, x^2, \dots, x^n\}$ is linearly dependent. So there exists a non-zero polynomial $f(X) \in \mathbb{R}[X]$ of degree $\leq n$ such that $f(x) = 0$. Without loss of generality, we may assume that the leading coefficient of $f(X)$ is one. Then we can write $f(X)$ as a product of polynomials of degree ≤ 2, say

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_r)(X^2 + \lambda_1 X + \mu_1) \cdots (X^2 + \lambda_s X + \mu_s).$$

Since D is a division algebra and $f(x) = 0$, some factor of $f(X)$ is zero. If $x - \lambda_j \neq 0$ for all j, then x is a root of some $X^2 + \lambda_k X + \mu_k$. In any case, there exists $\lambda \in \mathbb{R}$ such that $x^2 + \lambda x \in \mathbb{R}$. $\square$

Lemma 25.3. *Let D be a real division algebra of dimension n. Then*

$$V = \{x \in D : x^2 \in \mathbb{R}_{\leq 0}\}$$

is a subspace of D such that $D = \mathbb{R} \oplus V$.

Proof. Let $x \in D \setminus V$ be such that $x^2 \in \mathbb{R}$. Since $x^2 > 0$, it follows that $x^2 = \alpha^2$ for some $\alpha \in \mathbb{R}$. Thus $x = \pm\alpha \in \mathbb{R}$, as D is a division algebra and $(x - \alpha)(x + \alpha) = x^2 - \alpha^2 = 0$.

We claim that V is a subspace of D. Note that $0 \in V$ and that if $x \in V$, then $\lambda x \in V$ for all $\lambda \in \mathbb{R}$. Let $x, y \in V$. If $\{x, y\}$ is linearly dependent, then $x + y \in V$. If not, we claim that $\{1, x, y\}$ is linearly independent. If there exist $\alpha, \beta, \gamma \in \mathbb{R}$ such that $\alpha x + \beta y + \gamma = 0$, then

$$\alpha^2x^2 = \beta^2y^2 + 2\beta\gamma y + \gamma^2 = (-\beta y - \gamma)^2.$$

This implies that $2\beta\gamma y \in \mathbb{R}$ and thus $\beta\gamma = 0$. Hence $\alpha = \beta = \gamma = 0$. The previous lemma implies that there exist $\lambda, \mu \in \mathbb{R}$ such that

$$(x+y)^2 + \lambda(x+y) \in \mathbb{R}, \quad (x-y)^2 + \mu(x-y) \in \mathbb{R}.$$

Since

$$(x+y)^2 + (x-y)^2 = 2x^2 + 2y^2 \in \mathbb{R},$$

it follows that $(\lambda+\mu)x + (\lambda-\mu)y \in \mathbb{R}$. Since $\{1, x, y\}$ is linearly independent, $\lambda = \mu = 0$. Thus $(x+y)^2 \in \mathbb{R}$. If $x + y \notin V$, then, the first paragraph of the proof implies that $x + y \in \mathbb{R}$, a contradiction.

Clearly, $\mathbb{R} \cap V = 0$. If $x \in D \setminus \mathbb{R}$, then the previous lemma implies that $x^2 + \lambda x \in \mathbb{R}$ for some $\lambda \in \mathbb{R}$. We claim that $x + \lambda/2 \in V$. If not, since

$$(x + \lambda/2)^2 = x^2 + \lambda x + (\lambda/2)^2 \in \mathbb{R},$$

it follows that $x + \lambda/2 \in \mathbb{R}$ and thus $x \in \mathbb{R}$. Hence $x = -\lambda/2 + (x + \lambda/2) \in \mathbb{R} \oplus V$. □

Lemma 25.4. *Let D be a real algebra of (real) dimension n. If $n > 2$, then there exist $i, j, k \in D$ such that $\{1, i, j, k\}$ is linearly independent and*

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i. \tag{12.1}$$

Proof. Let $V = \{x \in D : x^2 \in \mathbb{R}, x^2 \leq 0\}$ be the subspace of Lemma 25.3. For $x, y \in V$ let $x \circ y = xy + yx = (x+y)^2 - x^2 - y^2 \in \mathbb{R}$. If $x \neq 0$, then $x \circ x = 2x^2 \neq 0$. Since $\dim V = n - 1$, there exist $y, z \in V$ such that $\{y, z\}$ is linearly independent. Let

$$x = z - \frac{z \circ y}{y \circ y} y.$$

Since $\{y, z\}$ is linearly independent, $x \neq 0$. Moreover, since

$$x \circ y = \left(z - \frac{z \circ y}{y \circ y}\right) \circ y = zy - \frac{z \circ y}{y \circ y} y^2 + yz - \frac{z \circ y}{y \circ y} y^2 = z \circ y - \frac{z \circ y}{y \circ y} y \circ y = 0,$$

it follows that $xy = -yx$. Let

$$i = \frac{1}{\sqrt{-x^2}} x, \quad j = \frac{1}{\sqrt{-y^2}} y, \quad k = ij.$$

A direct calculation shows that the formulas of (12.1) hold. For example,

$$ji = \frac{1}{\sqrt{-y^2}} \frac{1}{\sqrt{-x^2}} yx = \frac{1}{\sqrt{-x^2}} \frac{1}{\sqrt{-y^2}} (-xy) = -k.$$ □

Now we are finally ready to prove the theorem:

Proof of 25.1. Let D be a real division algebra and let $n = \dim D$. If $n = 1$, then $D \simeq \mathbb{R}$. If $n = 2$, the subspace V of Lemma 25.3 is non-zero and thus there exists $i \in D$ such that $i^2 = -1$. Hence $D \simeq \mathbb{C}$. Lemma 25.4 implies that $n \neq 3$. If $n = 4$, then $D \simeq \mathbb{H}$. Suppose that $n > 4$. By Lemma 25.4 there exist $i, j, k \in D$ such that $\{1, i, j, k\}$ is linearly independent and that the formulas of (12.1) hold. Let

$$V = \{x \in D : x^2 \in \mathbb{R}_{\leq 0}\}.$$

By Lemma 25.3, $\dim V = n-1$. Thus there exists $x \in V \setminus \langle i, j, k\rangle$. Let

$$e = x + \frac{i \circ x}{2} i + \frac{j \circ x}{2} j + \frac{k \circ x}{2} k \in V \setminus \{0\}.$$

A direct calculation shows that $i \circ e = j \circ e = k \circ e = 0$. Then

$$ek = e(ij) = (ei)j = -(ie)j = -i(ej) = i(je) = (ij)e = ke,$$

a contradiction. □

§26. Jacobson's commutativity theorem

Exercise 26.1. A ring R is **boolean** if $x^2 = x$ for all $x \in R$. Prove that boolean rings are commutative.

To prove this fact, note that $1 = (-1)^2 = -1$. This means that R has characteristic two. Let $x, y \in R$. Since $x + y = (x+y)^2 = x^2 + xy + yx + y^2$. it follows that $0 = xy + yx$ and hence $xy = yx$.

Proposition 26.2. *Let R be a finite ring such that for each $x \in R$ there exists $n(x) \geq 2$ such that $x^{n(x)} = x$. Then R is commutative.*

Proof. Since R is finite, R is artinian and hence $J(R)$ is nil. Since R is reduced, $J(R) = \{0\}$. By the Artin–Wedderburn theorem, $R \simeq \prod_{i=1}^{k} M_{n_i}(D_i)$ for some division rings $D_1, \dots, D_k$. Since R is finite, each D_i is finite. By Wedderburn's theorem, every D_i is a field. Again, since R is reduced, $n_i = 1$ for all i. Therefore R is commutative, as it is direct product of finitely many fields. □

In this lecture, we will prove extend the result of Proposition 26.2 to arbitrary (i.e. non-finite) rings.

Theorem 26.3 (Jacobson). *Let R be a ring such that for each $x \in R$ there exists $n(x) \geq 2$ such that $x^{n(x)} = x$. Then R is commutative.*

We shall need the following lemma.

Lemma 26.4. *Let K be a finite field of characteristic $p > 0$. There exists $n \in \mathbb{Z}_{>0}$ such that $|K| = p^n$ and $x^{p^n} = x$ for all $x \in K$. Moreover, if $K \setminus \{0\} = \{x_1, \dots, x_{p^n-1}\}$, then $X^{p^n} - X = (X - x_1) \cdots (X - x_{p^n-1})X$.*

Proof. The field K is a $(\mathbb{Z}/p)$-vector space. If $\dim_{\mathbb{Z}/p} K = n$, then $|K| = p^n$. In particular, $K \setminus \{0\}$ is an abelian group of order $p^n - 1$ and hence, by Lagrange's theorem, $x^{p^n-1} = 1$ for all $x \in K \setminus \{0\}$. Thus $x^{p^n} = x$ for all $x \in K$ and hence every $x \in K$ is a root of the polynomial $X^{p^n} - X$ of degree p^n. $\square$

Let R be a ring. For each $r \in R$ the map $\operatorname{ad} r \colon R \to R$, $x \mapsto rx - xr$, is a derivation. This means that $\operatorname{ad}(xy) = (\operatorname{ad} x)y + x(\operatorname{ad} y)$ for all $x, y \in R$. By induction one proves that

$$(\operatorname{ad} r)^n(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} r^{n-k} x r^k \tag{12.2}$$

for all $x \in R$ and $n \in \mathbb{Z}_{>0}$. If p is a prime number, p divides $\binom{p}{k}$ for all $k \in \{1, \dots, p-1\}$. This fact is needed to solve the following exercise:

Exercise 26.5. Let p be a prime number and R be a ring of characteristic p. Prove that $(\operatorname{ad} r)^{p^n} = \operatorname{ad} r^{p^n}$.

Now we are ready to prove Jacobson's commutativity theorem.

Proof of Theorem 26.3. We divide the proof in several steps and claims. We may assume that R is non-zero.

Claim. $J(R) = \{0\}$.

Let $x \in J(R)$ and $n = n(x)$. Since $-x^{n-1} \in J(R)$, there exists $y \in R$ such that $-x^{n-1} \circ y = -x^{n-1} + y - x^{n-1}y = 0$. Thus

$$-x^{n-1} + y = x^{n-1}y \implies -x + xy = x(-x^{n-1} + y) = x^n y = xy.$$

This implies that $x = 0$.

Claim. Without loss of generality we may assume that R is primitive.

Let $\{P_i : i \in I\}$ be the collection of primitive ideals of R. The map $R \to \prod_{i \in I} R/P_i$, $r \mapsto (r + P_i)_{i \in I}$, is an injective homomorphism, since its kernel is

$$\bigcap_{i \in I} P_i = J(R) = \{0\}.$$

Note that R is commutative if and only if each R/P_i is commutative. Moreover, each R/P_i satisfies the assumption, that is $(x + P_i)^{n(x)} = x^{n(x)} + P_i = x + P_i$, and and is a primitive ring.

Claim. R is a division ring.

By Jacobson's density theorem, there exists a division ring D and a D-vector space V such that R is dense in V. We claim that $\dim_D V = 1$. If $\dim_D V \geq 2$, let $\{v_1, v_2\} \subseteq V$ be a linearly independent set. Then there exists $f \in R$ such that $f(v_1) = v_2$ and $f(v_2) = 0$. This implies that $f^k(v_1) = 0$ for all $k \geq 2$ and $f(v_1) \neq 0$. This contradicts the fact that $f^n = f$ for $n = n(f)$. Thus $R \simeq D^{\mathrm{op}}$, a division ring.

Claim. R has positive characteristic.

Since R is a division ring, $2 = 1+1 \in R$. There exists $n \geq 2$ such that $2^n = 2$. In particular, $2(2^{n-1}-1) = 0$. This implies the claim.

Claim. Every non-zero subring of R is a division ring.

Let $S \subseteq R$ is a non-zero subring of R. If $x \in S \setminus \{0\}$, then $x^{n(x)} = x$. In particular, $x^{-1} = x^{n(x)-2} \in S$.

Claim. R is commutative.

Let us assume that R is not commutative. Let $x \in R \setminus Z(R)$. Since R has positive characteristic, there exists $m > 0$ such that $mx = 0$. Moreover, since R is a division ring and $x^{n(x)} = x$, it follows that $x^{n(x)-1} = 1$. These facts imply that the subring K of R generated by x is finite. By Wedderburn's theorem, K is a finite field. Thus $|K| = p^k$ for some prime number p and some $k > 0$ and

$$x^{p^k} = x.$$

Note that R is a K-vector space and $\delta = \operatorname{ad} x \colon R \to R$, $y \mapsto xy - yx$, is a K-linear map. Moreover, by the lemma,

$$\delta^{p^k} = (\operatorname{ad} x)^{p^k} = \operatorname{ad}\left(x^{p^k}\right) = \operatorname{ad} x = \delta$$

and

$$\delta(\delta - x_1 \operatorname{id}) \cdots (\delta - x_{p^{k-1}} \operatorname{id}) = 0 \tag{12.3}$$

if $K = \{0, x_1, \dots, x_{p^k-1}\}$. Since x is not central, δ is non-zero. So there exists $y \in R$ such that $\delta(y) \neq 0$. Evaluating (12.3) in y and using that R is a division ring we obtain that

$$x_i y = \delta(y) = xy - yx$$

for some i. Let R_0 be the subring of R generated by x and y. Since $xy - yx = \delta(y) \neq 0$, the ring R_0 is a non-commutative division ring. Note that $yx = (x - x_i)y \in Ky$, as $x \in K$ and $x_i \in K$. By induction one proves that $yx^j \subseteq Ky$ for all $j \geq 1$ and hence $y^i K \subseteq Ky^i$ for all $i \geq 1$. This implies that

$$K + Ky + \cdots + Ky^{n(y)-2} \subseteq R$$

is a subring. It follows that $K + Ky + \cdots + Ky^{n(y)-2} = R_0$, as it is a subring of R included in R_0 that contains x and y. Since R_0 is a finite division ring, it is a field by Wedderburn's theorem, a contradiction since it is non-commutative. □

There are elementary proofs of Jacobson's commutativity theorem. See for example [12].

§27. Skolem–Noether theorem

Definition 27.1. Let K be a field. An algebra A (over K) is **central** if $Z(A) = K$.

If K is a field, then $M_n(K)$ is a central algebra.

Proposition 27.2. *Let A be a unitary algebra and $n \geq 1$. Then A is central if and only if $M_n(A)$ is central.*

Proof. If $M_n(A)$ is central and $z \in Z(A)$, then $zI \in Z(M_n(A)) = KI$. Thus $z \in K$. Conversely, if $X \in Z(M_n(A))$, then, since $XE_{kl} = E_{kl}X$ for all $k \neq l$, $X = aI$ for some $a \in A$. Moreover, $XaE_{11} = aE_{11}X$. Hence $a \in Z(A) = K1$. □

Example 27.3. $\mathbb{H}$ is a real central algebra.

Example 27.4. $\mathbb{C}$ is a complex central algebra but it is not a real central algebra.

Frobenius' theorem 25.1 translates into the following statement: Every finite-dimensional real central division algebra is isomorphic to $\mathbb{R}$ or $\mathbb{H}$.

Proposition 27.5. *Every simple unitary ring is an algebra over its center.*

Proof. Let R be a simple unitary ring. It is enough to show that $Z(R)$ is a field. If $z \in Z(R) \setminus \{0\}$ then zR is a non-zero ideal of R. Since R is simple, $zR = R$. Thus z is invertible. □

For an algebra A, let $L\colon A \to \operatorname{End}_k(A)$, $a \mapsto L_a$, and $R\colon A \to \operatorname{End}_k(A)$, $a \mapsto R_a$, be given by $L_a(x) = ax$ and $R_a(x) = xa$. Then both L and R are linear maps such that

$$L_{ab} = L_a L_b, \qquad R_{ab} = R_b R_a, \qquad L_a R_b = R_b L_a$$

for all $a, b \in A$.

Definition 27.6. Let A be an algebra. The **algebra of multipliers** of A is

$$M(A) = \left\{ \sum_{j=1}^{n} L_{a_i} R_{b_i} : n \in \mathbb{Z}_{\geq 0},\, a_1, \dots, a_n, b_1, \dots, b_n \in A \right\}.$$

It is an exercise to show that $M(A)$ is a subalgebra of $\operatorname{End}_K(A)$. Moreover, if A is unitary, then $M(A)$ is generated by the L_a and the R_b for $a, b \in A$.

Lemma 27.7. *Let A be an algebra and $f \in M(A)$. Then there exists $n \geq 0$ and $a_1, \dots, a_n \in A$ and $b_1, \dots, b_n \in A$ such that*

$$f = \sum_{i=1}^{n} L_{a_i} R_{b_i}$$

and $\{b_1, \dots, b_n\}$ is linearly independent.

Proof. Write $f=\sum_{i=1}^{n} L_{a_i}R_{b_i}$ with n be minimal. If $b_n=\sum_{j=1}^{n-1}\lambda_j b_j$, then

$$f=\sum_{i=1}^{n-1} L_{a_i+\lambda_i a_n}R_{b_i},$$

a contradiction. □

Lemma 27.8. *Sea A un álgebra central simple. Si $\sum_{i=1}^{n} L_{a_i}R_{b_i}=0$ y el conjunto $\{b_1,\dots,b_n\}$ (resp. $\{a_1,\dots,a_n\}$) es linealmente independiente, entonces $a_i=0$ (resp. $b_i=0$) para todo $i\in\{1,\dots,n\}$.*

Proof. Primero observemos que el resultado es válido para $n=1$. Queremos demostrar que si $a_1xb_1=0$ para todo $x\in A$ y $b_1\neq 0$ entonces $a_1=0$. Supongamos que $a_1\neq 0$. Entonces el ideal de A generado por a_1 es no nulo y luego es igual a A. Esto implica que existen $u_1,\dots,u_m,v_1,\dots,v_m\in A$ tales que $1=\sum_{j=1}^{m} u_ja_1v_j$. Podemos escribir entonces

$$0=\sum_{j=1}^{m} L_{u_j}(L_{a_1}R_{b_1})L_{v_j}=\sum_{j=1}^{m} L_{u_ja_1v_j}R_{b_1}=R_{b_1}$$

y luego $b_1=0$.

Supongamos que el lema no es cierto y sea $n>1$ el menor entero positivo donde el lema es falso. Supongamos que $a_n\neq 0$. Como A es simple, el ideal generado por a_n es A y luego existen $u_1,\dots,u_m,v_1,\dots,v_m\in A$ tales que $1=\sum_{j=1}^{m} u_ja_1v_j$. Entonces

$$0=\sum_{j=1}^{m} L_{u_j}\left(\sum_{i=1}^{n} L_{a_i}R_{b_i}\right)L_{v_j}=\sum_{i=1}^{n}\sum_{j=1}^{m} L_{u_ja_iv_j}R_{b_i}=\sum_{i=1}^{n} L_{c_i}R_{b_i},$$

donde $c_i=\sum_{j=1}^{m} u_ja_iv_j$ y obviamente $c_n=1$. Como

$$0=L_x\left(\sum_{i=1}^{n} L_{c_i}R_{b_i}\right)-\left(\sum_{i=1}^{n} L_{c_i}R_{b_i}\right)L_x=\sum_{i=1}^{n-1} L_{xc_i-c_ix}R_{b_i}$$

para todo $x\in A$, la minimalidad de n implica que $xc_i-c_ix=0$ para todo $x\in A$. Luego, como A es central, $c_i\in k$ para todo $i\in\{1,\dots,n-1\}$. Al evaluar $0=\sum_{i=1}^{n} L_{c_i}R_{b_i}$ en 1_A se obtiene que $0=c_1b_1+\cdots+c_nb_n$, una contradicción a la independencia lineal de $\{b_1,\dots,b_n\}$. □

Lemma 27.9. *Si A es un álgebra central simple de dimensión finita, entonces $M(A)=\mathrm{End}_k(A)$.*

Proof. Sea $\{a_1,\dots,a_n\}$ una base de A. El conjunto $\{L_{a_i}R_{a_j}:1\leq i,j\leq n\}$ es linealmente independiente: si $\sum_{i,j=1}^{n}\lambda_{ij}L_{a_i}R_{a_j}=0$ entonces $\sum_{i=1}^{n} L_{a_i}R_{c_i}=0$, donde $c_i=\sum_{j=1}^{n}\lambda_{ij}R_{a_j}$. Como los a_i son linealmente independientes, el lema 27.8 implica que $c_i=0$ para todo $i\in\{1,\dots,n\}$, una contradicción a la independencia lineal de los a_j. Luego $\dim_k M(A)\geq n^2=\dim\mathrm{End}_k(A)$. □

Definition 27.10. Sea R un anillo unitario. Un automorfismo $f \in \operatorname{Aut}(R)$ se dice **interior** si existe un elemento inversible $r \in R$ tal que $f(x) = rxr^{-1}$ para todo $x \in R$.

Example 27.11. El automorfismo $\mathbb{C} \to \mathbb{C}$ dado por $z \mapsto \overline{z}$ no es interior.

Example 27.12. Sea $\lambda \in k \setminus \{0\}$ y sea $R = k[X]$. El automorfismo $k[X] \to k[X]$, $f(X) \mapsto f(X+\lambda)$, no es interior.

Example 27.13. Sea R un anillo. El automorfismo $R \times R \to R \times R$, $(x, y) \mapsto (y, x)$, no es interior.

Theorem 27.14 (Skolem–Noether). *Si A es un álgebra central simple de dimensión finita, todo automorfismo de A es interior.*

Proof. Sea $f \in \operatorname{Aut}(A)$. Gracias al lema 27.9, $f = \sum_{i=1}^{n} L_{a_i} R_{b_i}$. Sin perder generalidad podemos suponer que $a_1 \neq 0$ y que $\{b_1, \dots, b_n\}$ es linealmente independiente (observación **??**). Como f es morfismo, $L_{f(x)} f = f L_x$ para todo $x \in A$. Entonces

$$0 = \sum_{i=1}^{n} L_{f(x)a_i - a_i x} R_{b_i}$$

y luego, por el lema 27.8, $f(x)a_1 - a_1 x = 0$ para todo $x \in A$. Para terminar la demostración basta ver que a_1 es inversible: Como $a_1 \neq 0$ y A es simple, el ideal de A generado por a_1 es A; esto nos permite escribir $1 = \sum_{i=1}^{m} u_j a_1 v_j$ y luego a_1 es inversible pues

$$\left(\sum_{j=1}^{m} u_j f(v_j) \right) a_1 = a_1 \left(\sum_{j=1}^{m} f^{-1}(u_j) v_j \right) = 1.$$

$\square$

Lecture 13

§28. Brauer's group (optional)

Fix a field K. Recall that a K-algebra A is **simple** if $\{0\}$ and A are the only ideals of A. For example, if D is a division algebra, then D and $M_n(D)$ are simple algebras.

Example 28.1. If $a, b \in K \setminus \{0\}$, let $H_K(a,b)$ be the K-algebra with basis $\{1, i, j, k\}$ and multiplication given by

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

The quaternion algebra $H_K(a,b)$ is simple, as either $H_K(a,b)$ is a division algebra or $H_K(a,b) \simeq M_2(K)$.

A well-known particular case: $\mathbb{H} = H_{\mathbb{R}}(-1,-1)$.

Definition 28.2. A **central simple algebra** is a finite-dimensional algebra K-algebra such that A is simple and $Z(A) = K$.

For example, $\mathbb{C}$ is a complex central simple algebra and it is not a real central simple algebra, as $\mathbb{Z}(\mathbb{C}) = \mathbb{C}$. Moreover, $\mathbb{H}$ and $\mathbb{R}$ are central simple algebras over $\mathbb{R}$.

Exercise 28.3. Prove that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq M_4(\mathbb{R})$.

The previous exercise shows that the tensor product of central simple algebras is not necessarily a central simple algebra.

Wedderburn's theorem states that every finite-dimensional simple algebra is isomorphic to $M_n(D)$ for some n and some division algebra D.

Exercise 28.4. Prove that the n in Wedderburn's theorem is unique and the division algebra D is unique up to isomorphism.

Let A and B be central simple K-algebras. By Wedderburn's theorem, $A \simeq M_n(D)$ and $B \simeq M_m(E)$ for some $m, n > 0$ and division algebras D and E. We define

$$A \sim B \Longleftrightarrow D \simeq E.$$

Exercise 28.5. Prove that $\sim$ is an equivalence relation.

If D is a central division K-algebra, then $D = M_1(D) \sim M_n(D)$ for all n.

Exercise 28.6. Let D be a K-algebra. Prove that $D \otimes_K M_n(K) \simeq M_n(D)$ as K-algebras

Exercise 28.7. Prove that $M_n(K) \otimes_K M_m(K) \simeq M_{nm}(K)$.

If A is a central simple algebra, $[A]$ will denote the equivalence class of A under the relation $\sim$, that is $[A] = \{B : B \sim A\}$.

Exercise 28.8. Prove that the collection of equivalence classes of central simple algebras is a set.

One way to solve the previous exercise is to recall that, by definition, central simple algebras are finite-dimensional. Then that the underlying vector space of a central simple algebra over K is K^n for some n. Algebra structures over K^n form a set, as they are indeed a subset of $\mathrm{Hom}(K^n \otimes K^n, K^n)$.

Theorem 28.9. *Let* $\mathrm{Br}(K)$ *be the set of equivalence classes of central simple* K*-algebras. Then* $\mathrm{Br}(K)$ *with the operation*

$$[A][B] = [A \otimes_K B] \tag{13.1}$$

is an abelian group.

Sketch of the proof. We need to show that the product of $\mathrm{Br}(K)$ is well-defined. There are several things to prove:

1) $A \otimes_K B$ is a finite-dimensional central simple K-algebra.
2) The multiplication $[A][B] = [A \otimes_K B]$ is well-defined, that is $A \sim A_1$ and $B \sim B_1$ imply that $A \otimes_K B \sim A_1 \otimes_K B_1$.

To prove 1) we note that $A \otimes_K B$ is a finite-dimensional K-algebra, as

$$\dim_K(A \otimes_K B) = (\dim_K A)(\dim_K B).$$

It is central, as $Z(A \otimes_K B) \simeq Z(A) \otimes_K Z(B)$. Finally, it is simple, as there exists a bijective correspondence between ideals of A and ideals of $A \otimes_K B$.

Let us prove 2). Write $A \simeq M_n(D)$, $A_1 \simeq M_{n_1}(D)$, $B \simeq M_m(E)$ and $B_1 \simeq M_{m_1}(E)$ for some division K-algebras D and E. Since the tensor product is associative and commutative,

$$\begin{aligned} A \otimes_K B &\simeq M_n(D) \otimes_K M_m(E) \\ &\simeq D \otimes_K M_n(K) \otimes_K E \otimes_K M_m(K) \\ &\simeq D \otimes_K E \otimes_K M_{nm}(K) \\ &\simeq M_{nm}(D \otimes_K E). \end{aligned}$$

Note that $D \otimes_K E$ is maybe not a division algebra, but it is indeed a finite-dimensional central simple algebra. By Wedderburn's theorem, $D \otimes_K E \simeq M_p(F)$ for some division K-algebra F and some p. This implies that

$$A \otimes_K B \simeq M_{nmp}(F).$$

Similarly, $A_1 \otimes_K B_1 \simeq M_{n_1 m_1 p}(F)$ and thus $A \otimes_K B \sim A_1 \otimes_K B_1$.

Now we need to prove that $\mathrm{Br}(K)$ is a group. The multiplication (13.1) is associative and commutative since the tensor product $\otimes_K$ is associative and multiplicative. The identity of $\mathrm{Br}(K)$ is $[K]$, as $[A][K] = [A \otimes_K K] = [A]$. Finally, the inverse of $[A]$ is $[A^{\mathrm{op}}]$, as

$$[A][A^{\mathrm{op}}] = [A \otimes_K A^{\mathrm{op}}] = [M_n(K)]. \qquad \square$$

Exercise 28.10. Let D be a division algebra. Compute the center of $M_n(D)$.

Let us compute some examples:

Proposition 28.11. $\mathrm{Br}(\mathbb{C}) = \{0\}$.

Proof. Let A be a complex central simple algebra. Then $A \simeq M_n(D)$ for some complex division algebra D. We claim that $D \simeq \mathbb{C}$. Let $m = \dim D$ and $\alpha \in D$. Since $\{1, \alpha, \dots, \alpha^m\}$ has $m+1$ elements, it is a linearly dependent set. This means that there exists $\lambda_0, \dots, \lambda_m \in \mathbb{C}$ not all zero such that $0 = \sum_{i=0}^m \lambda_i \alpha^i$. Thus the non-zero polynomial $f = \sum_{i=0}^m \lambda_i X^i \in \mathbb{C}[X]$ is such that $f(\alpha) = 0$. Since $\mathbb{C}$ is algebraically closed, there exist $\alpha_0, \dots, \alpha_N \in \mathbb{C}$ and $a \in \mathbb{C} \setminus \{0\}$ such that

$$f = a \prod_{i=0}^{N} (X - \alpha_i).$$

Since D is a division algebra, there exists $i \in \{0, \dots, m\}$ such that $\alpha = \alpha_i$. In particular, $\alpha \in \mathbb{C}$. Therefore $[A] = [\mathbb{C}]$ and hence $\mathrm{Br}(A) = \{0\}$. $\square$

An application of Wedderburn's little theorem:

Proposition 28.12. *Let F be a finite field. Then* $\mathrm{Br}(F) = \{0\}$.

Proof. Let A be a central simple algebra over F. Then $A \simeq M_n(D)$ for some division F-algebra D. Since $\dim_F D < \infty$ and F is finite, $F = Z(A) \simeq Z(M_m(D)) \simeq Z(D) = D$ by Wedderburn's little theorem and hence $[A] = [F]$. $\square$

An application of Frobenius' theorem:

Proposition 28.13. $\mathrm{Br}(\mathbb{R})$ *is the cyclic group of order two.*

Proof. Let A be a central simple real algebra. Then $A \simeq M_n(D)$ where either $D \simeq \mathbb{R}$ or $D \simeq \mathbb{H}$ by Frobenius' theorem, as

$$\mathbb{R} \simeq Z(A) \simeq Z(M_n(D)) \simeq Z(D)$$

and $\mathbb{Z}(\mathbb{C}) = \mathbb{C}$. Thus $\mathrm{Br}(\mathbb{R})$ has only two elements, that is $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$. $\square$

§29. Brauer's group and cohomology (optional)

Let L/K be a Galois extension of degree n. Extending scalars we obtain a group homomorphism

$$\mathrm{res}\colon \mathrm{Br}(K) \to \mathrm{Br}(L), \quad [A] \mapsto [A \otimes_K L],$$

known as the **restriction homomorphism**.

Exercise 29.1. Prove that res is well-defined.

Definition 29.2. Let L/K be a Galois extension of degree n. The **restricted Brauer group** is $\mathrm{Br}(L/K)$ is defined as the kernel of the restriction homomorphism.

Recall that the Galois group G of L/K is a finite group. Let $Z^2(G, L^\times)$ be the set of maps $\alpha\colon G \times G \to L^\times$ such that

$$\alpha(g,h)\alpha(gh,k) = g(\alpha(h,k))\alpha(g,hk)$$

for all $g,h,k \in G$.

We say that $\alpha \in Z^2(G,L^\times)$ and $\beta \in Z^2(G,L^\times)$ are equivalent if and only if there exists $\{\delta_g : g \in G\} \subseteq L$ such that

$$\beta(g,h) = \delta_g g(\delta_h)\alpha(g,h)\delta_{gh}^{-1}$$

for all $g,h \in G$.

The second cohomology group $H^2(G,L^\times)$ is defined as the set of equivalence classes of $Z^2(G,L^\times)$. One proves that $H^2(G,L^\times)$ is indeed an abelian group.

Exercise 29.3. Let G be a finite group. For $\alpha \in Z^2(G,L^\times)$ let us consider the crossed product $L_t^\alpha G$ of G by K given by

$$L_t^\alpha G = \left\{ \sum_{g \in G} \lambda_g e_g : \lambda_g \in L \right\}.$$

1) Prove that the product

$$(\lambda_g e_g)(\lambda_h e_h) = \lambda_g g(\lambda_y)\alpha(g,h)e_{gh}.$$

is associative.

2) Prove that $e = \alpha(1,1)^{-1}e_1$ is such that $ee_g = e_g e = e_g$ for all $g \in G$.

3) Prove that each e_g is invertible with inverse

$$e_g^{-1} = \alpha(g^{-1},g)^{-1}\alpha(1,1)^{-1}e_{g^{-1}}.$$

Theorem 29.4. *Let L/K be a Galois extension of degree n and group G. Then*

$$\mathrm{Br}(L/K) \simeq H^2(G,L^\times).$$

The isomorphism of the theorem is given by

$$H^2(G, L^\times) \to \operatorname{Br}(L/K) \subseteq \operatorname{Br}(K), \quad [\alpha] \mapsto [L_t^\alpha G],$$

We do not have time to prove the theorem in detail, as it requires some tools that are outside the scope of our course.

Corollary 29.5. $\operatorname{Br}(K)$ *is a torsion group.*

Sketch of the proof. The theorem implies that for every finite Galois extension L/K one has $\operatorname{Br}(L/K) \simeq H^2(G, L^\times)$ is a torsion group, as $|G|H^2(G, L^\times) = \{0\}$. To finish the proof note that $\operatorname{Br}(K) = \bigcup \operatorname{Br}(L/K)$, where the union is taken over all finite Galois extensions L/K. ◻

The theorem can be used to compute Brauer groups. Let us give an example. We know that $\mathbb{C}/\mathbb{R}$ is a Galois extension with Galois group isomorphic to $\mathbb{Z}/2$. Thus

$$\operatorname{Br}(\mathbb{R}) = \operatorname{Br}(\mathbb{C}/\mathbb{R}) \simeq H^2(\mathbb{Z}/2, \mathbb{C}^\times) \simeq \mathbb{Z}/2.$$

Some topics for final projects

We collect here some topics for final presentations. Some topics can also be used as bachelor or master theses.

Rickart's theorem

In Lecture 9 we presented an algebraic proof of Rickart's theorem. The original proof uses analysis; see [10, (6.4) of Chapter II].

Connel's theorem

In Lecture 11 we presented the statement of Connel's theorem, which characterizes prime group rings over fields of characteristic zero (see Theorem 12.7); the proof of this result appears for example in [14, Theorem 2.10 of Chapter 4]. As a corollary, one obtains that, if K is a field of characteristic zero, then the group ring $K[G]$ is left artinian if and only if the group G is finite (see Corollary **??**); see [14, Theorem 1.1 of Chapter 10] for a proof.

Kolchin's theorem

Let $U_n(\mathbb{C})$ be the subgroup of $\mathbf{GL}_n(\mathbb{C})$ of matrices (u_{ij}) such that

$$u_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i > j. \end{cases}$$

A matrix $a \in \mathbf{GL}_n(\mathbb{C})$ is said to be **unipotent** if its characteristic polynomial is of the form $(X-1)^n$. A subgroup G of $\mathbf{GL}_n(\mathbb{C})$ is said to be **unipotent** if each $g \in G$ is unipotent.

An important theorem of Kolchin states that every unipotent subgroup of $\mathbf{GL}_n(\mathbb{C})$ is conjugate of some subgroup of $U_n(\mathbb{C})$. The theorem and its proof appear, for example, in the VUB course Representation theory of algebras.

Dedekind-finite rings

The idea is to develop basic aspects of Dedekind-finite rings. A standard reference is Lam's book [11].

Skolem–Noether theorem

Any automorphism of the full $n \times n$ matrix algebra is conjugation by some invertible $n \times n$ matrix. This is an elementary instance of the celebrated Skolem–Noether theorem. We refer to [2, Chapter 4] for the theorem and its proof (in a more general context).

Double centralizer theorem

Let R be a ring. The centralizer of a subring S of R is

$$C_R(S) = \{r \in R : rs = sr \text{ for all } s \in S\}.$$

Clearly $C_R(C_R(S)) \supseteq S$, but equality not always holds. The double centralizer theorems give conditions under which one can conclude that equality occurs; see for example [2, Chapter 4].

References

1. S. A. Amitsur. Nil radicals. Historical notes and some new results. In *Rings, modules and radicals (Proc. Internat. Colloq., Keszthely, 1971)*, pages 47–65. Colloq. Math. Soc. János Bolyai, Vol. 6, 1973.
2. M. Brešar. *Introduction to noncommutative algebra*. Universitext. Springer, Cham, 2014.
3. R. W. Gilmer, Jr. If $R[X]$ is Noetherian, R contains an identity. *Amer. Math. Monthly*, 74:700, 1967.
4. I. N. Herstein. A counterexample in Noetherian rings. *Proc. Nat. Acad. Sci. U.S.A.*, 54:1036–1037, 1965.
5. I. N. Herstein. *Noncommutative rings*, volume 15 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, DC, 1994. Reprint of the 1968 original, With an afterword by Lance W. Small.
6. T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.
7. N. Jacobson. *Structure of rings*. American Mathematical Society Colloquium Publications, Vol. 37. American Mathematical Society, Providence, R.I., revised edition, 1964.
8. G. Köthe. Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist. *Math. Z.*, 32(1):161–186, 1930.
9. J. Krempa. Logical connections between some open problems concerning nil rings. *Fund. Math.*, 76(2):121–130, 1972.
10. T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.
11. T. Y. Lam. *Exercises in modules and rings*. Problem Books in Mathematics. Springer, New York, 2007.
12. T. Nagahara and H. Tominaga. Elementary proofs of a theorem of Wedderburn and a theorem of Jacobson. *Abh. Math. Sem. Univ. Hamburg*, 41:72–74, 1974.
13. P. P. Nielsen. Simplifying Smoktunowicz's extraordinary example. *Comm. Algebra*, 41(11):4339–4350, 2013.
14. D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.
15. W. R. Scott. *Group theory*. Dover Publications, Inc., New York, second edition, 1987.
16. A. Smoktunowicz. Polynomial rings over nil rings need not be nil. *J. Algebra*, 233(2):427–436, 2000.
17. A. Smoktunowicz. On some results related to Köthe's conjecture. *Serdica Math. J.*, 27(2):159–170, 2001.
18. A. Smoktunowicz. Some results in noncommutative ring theory. In *International Congress of Mathematicians. Vol. II*, pages 259–269. Eur. Math. Soc., Zürich, 2006.
19. D. E. Taylor. Some classical theorems on division rings. *Enseign. Math. (2)*, 20:293–298, 1974.

20. M. Teleuca. Zsigmondy's theorem and its applications in contest problems. *Internat. J. Math. Ed. Sci. Tech.*, 44(3):443–451, 2013.
21. K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.

Index