

Leandro Vendramin

Associative algebras

Notes

Thursday 26th October, 2023

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 two-hour lectures.

The content presented here draws heavily from [2], [8], and [18]. Additionally, I have followed the outstanding blog on abstract algebra by Yaghoub Sharif.

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

This version was compiled on Thursday 26th October, 2023 at 11:14. Please send comments and corrections to me at `Leandro.Vendramin@vub.be`. Thanks go to Luca Descheemaeker, Lukas Simons.

Leandro Vendramin
Brussels, Belgium

Contents

1	1
2	7
3	15
4	21
5	27
6	35
7	41
8	49
9	57
10	63
11	69
12	77
Some topics for final projects	85
References	89
Index	91

List of topics

§1	Semisimple algebras	1
§2	Group algebras	11
§3	Primitive rings	16
§4	Jacobson's radical	21
§5	Commutative rings with no maximal ideals	27
§6	Amitsur's theorem	32
§7	Jacobson's conjecture	33
§8	Köthe's conjecture	34
§9	Gilmer's theorem	35
§10	Artinian modules	36
§11	Akizuki's theorem	40
§12	Local rings	41
§13	Semiprime and semiprimitive rings	43
§14	Jacobson's density theorem	45
§15	Prime rings	49
§16	Semisimple modules	52
§17	Hopkins–Levitski theorem	54

§18	Andrunakevic–Rjabuhin’s theorem	57
§19	Rickart’s theorem	59
§20	Maschke’s theorem	63
§21	Herstein’s theorem	64
§22	Formanek’s theorem, I	66
§23	Tensor products	69
§24	Formanek’s theorem, II	73
§25	Wedderburn’s little theorem	73
§26	Zsigmondy’s theorem	75
§27	Fermat’s last theorem in finite rings	76
§28	Frobenius’s theorem	77
§29	Jacobson’s commutativity theorem	79

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 $A \times A \rightarrow A$ 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 a ring A is an algebra over K if and only if there is a ring homomorphism $K \rightarrow Z(A)$, where $Z(A) = \{a \in A : ab = ba \text{ for all } b \in A\}$ is the center of A , such that $1_K \rightarrow 1_A$.

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 $[0, 1] \rightarrow \mathbb{R}$ 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 if 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. Let K be a field and A and B be K -algebras. An algebra **homomorphism** is a ring homomorphism $f: A \rightarrow B$ that is also a K -linear map.

The complex conjugation map $\mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$, 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 $f: G \rightarrow \mathcal{U}(A)$ is a group homomorphism, then there exists an algebra homomorphism $\varphi: K[G] \rightarrow A$ 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 $A \rightarrow A/I, a \mapsto a + I$, 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** of A -modules.

Definition 1.16. Let A be a K -algebra. A **homomorphism** of A -modules $f: M \rightarrow N$ is a K -linear map such that $f(a \cdot m) = a \cdot f(m)$ for all $a \in A$ and $m \in M$.

It is a straightforward exercise to prove the isomorphism theorems.

Let A be a finite-dimensional K -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. If M is a module over a finite-dimensional K -algebra A , one defines $\text{End}_A(M)$ as the set of module homomorphisms $M \rightarrow M$. The set $\text{End}_A(M)$ is indeed a K -algebra with

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

for all $f, g \in \text{End}_A(M)$, $\lambda \in K$ and $m \in M$.

Example 1.18. 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 ${}_A A$.

Definition 1.19. 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 1.20. 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.

By definition, the zero module is semisimple. Moreover, any finite direct sum of semisimples is semisimple.

Lemma 1.21 (Schur). *Let A be an algebra. If S and T are simple modules and $f: S \rightarrow T$ 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 1.22. *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, $\varphi: A \rightarrow S, a \mapsto a \cdot s$, 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 1.23. *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 $S_i \cap (N \oplus T) \subseteq S_i$. 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. \square

Proposition 1.24. *If M is a semisimple module and N is a submodule, then N and M/N are semisimple.*

Proof. Assume that $M = S_1 + \dots + S_k$, where each S_i is a simple submodule. If $\pi: M \rightarrow M/N$ is the canonical map, the techniques used in Schur's lemma imply 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.

§1 Semisimple algebras

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. \square

Definition 1.25. An algebra A is **semisimple** if every finitely generated A -module is semisimple.

Proposition 1.26. *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

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

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

Theorem 1.27. *Let A be a finite-dimensional semisimple algebra. Assume that the regular representation can be decomposed as ${}_A A = \bigoplus_{i=1}^k S_i$ 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 $\varphi: A \rightarrow S, a \mapsto a \cdot s$, is a surjective module homomorphism. Since $\varphi \neq 0$, there exists $i \in \{1, \dots, k\}$ such that some restriction $\varphi|_{S_i}: S_i \rightarrow S$ is non-zero. By Schur's lemma, it follows that $\varphi|_{S_i}$ is an isomorphism. \square

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, $S_i \neq S_j$ whenever $i \neq j$.

Lecture 2

Exercise 1.28. 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 1.29. *Let D be a division algebra, and V be a finite-dimensional module over D . Then V is a simple module over $\text{End}_D(V)$ and there exists $n \in \mathbb{Z}_{>0}$ such that $\text{End}_D(V) \simeq nV$ is semisimple.*

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

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

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

$$\dim_D \text{End}_D(V) = n^2 = \dim_D(nV),$$

it follows that the map is an isomorphism. Thus

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

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

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 1.30. Let M , N , and X be modules. Prove that

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

Theorem 1.31. Let A be a finite-dimensional algebra and let S_1, \dots, S_k be the simple modules over A . If

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

then each n_j is uniquely determined.

Proof. Since each S_j is simple and $S_i \neq S_j$ if $i \neq j$, Schur's lemma implies that $\text{Hom}_A(S_i, S_j) = \{0\}$ whenever $i \neq j$. For each $j \in \{1, \dots, k\}$, routine calculations show that

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

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

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

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

Lemma 1.32. If A is an algebra, then $A^{\text{op}} \simeq \text{End}_A(A)$ as algebras.

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

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

Lemma 1.33. If A is an algebra and $n \in \mathbb{Z}_{>0}$, then $M_n(A)^{\text{op}} \simeq M_n(A^{\text{op}})$ as algebras.

Proof. Let $\psi : M_n(A)^{\text{op}} \rightarrow M_n(A^{\text{op}})$, $X \mapsto X^T$, 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

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

Lemma 1.34. *If S is a simple module and $n \in \mathbb{Z}_{>0}$, then*

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

as algebras.

Sketch of the proof. Let (φ_{ij}) be a matrix with entries in $\text{End}_A(S)$. We define a map $nS \rightarrow nS$ as follows:

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

The reader should prove that the map

$$M_n(\text{End}_A(S)) \rightarrow \text{End}_A(nS)$$

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

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

Exercise 1.35. Prove Lemma 1.34.

Exercise 1.36. Let M , N , and X be modules. Prove that

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

Theorem 1.37 (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 $S_i \neq S_j$ whenever $i \neq j$. Schur's lemma implies that

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

where each $D_i = \text{End}_A(S_i)$ is a division algebra by Schur's lemma. Thus

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

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

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

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

Corollary 1.38 (Molien). *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,

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

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

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

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

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

§2. Group algebras

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

Exercise 2.2. Let $G = C_n$ be the (multiplicative) cyclic group of order n . Prove that $K[G] \simeq K[X]/(X^n - 1)$.

Exercise 2.3. Let G be a finitely-generated torsion-free abelian group. Prove that $K[G]$ is a domain.

Exercise 2.4. Let G be a group and $\alpha = \sum_{g \in G} \lambda_g g \in K[G]$. The **support** of α is the set

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

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

Exercise 2.5. 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 2.6. 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

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

is an algebra isomorphism.

2) If the characteristic of K is two, then

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

is an algebra isomorphism.

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

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

is an algebra homomorphism.

Exercise 2.7. Let $G = C_3$ be the (multiplicative) group of three elements. Prove that $\mathbb{R}[G] \simeq \mathbb{R} \times \mathbb{C}$.

Exercise 2.8. Let $G = \langle r, s : r^3 = s^2 = 1, sr s = r^{-1} \rangle$ 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) $\mathbb{Q}[G] \simeq \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q})$.

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 2.9. 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 2.10. 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 2.11. 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 2.1 (Brauer). Which algebras are group algebras?

§2 Group algebras

This question might be impossible to answer, but it is extremely interesting. Examples 2.10 and 2.11 show that \mathbb{C}^4 and $\mathbb{C}^2 \times M_2(\mathbb{C})$ are complex group algebras.

Exercise 2.12. Is $\mathbb{C}^2 \times M_2(\mathbb{C}) \times M_3(\mathbb{C})$ a complex group algebra?

Lecture 3

Definition 2.13. An algebra A is **simple** if $A \neq \{0\}$ and $\{0\}$ and A are the only ideals of A .

Proposition 2.14. *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

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

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

$$\varphi: I \rightarrow M, \quad x \mapsto x \cdot m,$$

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. \square

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 2.15. *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 $f: T \rightarrow Ta, t \mapsto ta$. Since f is a surjective module homomorphism and T is simple, it follows that either $\ker f = \{0\}$ or $\ker f = T$. If $\ker f = T$, 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. \square

Theorem 2.16 (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 . \square

§3. 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 3.1. \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 3.2. 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 3.3. 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 an ideal of R .

Example 3.4. If 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 $RaR + Ra + aR + \mathbb{Z}a$.

§3 Primitive rings

The following exercise asks to prove the **Chinese Remainder Theorem** for arbitrary rings.

Exercise 3.5. Let R be a ring and I_1, \dots, I_n be ideals such that $I_j + I_k = R$ whenever $j \neq k$ and $R = I_j + R^2$ for all j . Prove that

$$R/(I_1 \cap \dots \cap I_n) \simeq R/I_1 \times \dots \times R/I_n.$$

In the previous exercise, the condition $R = I_j + R^2$ trivially holds in the case of rings with one.

Definition 3.6. 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 3.7. 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 $A = (a_{ij}) \in M_n(S)$ and E_{ij} is the matrix such that $(E_{ij})_{kl} = \delta_{ik} \delta_{jl}$, then

$$E_{ij} A E_{kl} = a_{jk} E_{il} \quad (3.1)$$

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

Example 3.8. 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 $R \times M \rightarrow M$, $(r, m) \mapsto r \cdot m$, such that

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

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 3.9. Let R be a simple unitary ring.

- 1) Prove that the center $Z(R)$ of R is a field.
- 2) Prove that R is an algebra over $Z(R)$.

Definition 3.10. 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 3.11. 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 $M = R \cdot x \subseteq L$. \square

Example 3.12. Let D be a division ring and let V be a non-zero vector space (over D). If $R = \text{End}_D(V)$, then V is a simple R -module with $fv = f(v)$, $f \in R$, $v \in V$.

Example 3.13. 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 3.14. 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 3.15. Let D be a division ring and let $R = M_n(D)$. Then $L = RE_{11}$ is a minimal left ideal.

Example 3.16. 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 3.17. 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 3.18. 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 3.19. 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 3.11. The map $\phi: R \rightarrow M, r \mapsto r \cdot m$, 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).

§3 Primitive rings

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 . □

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

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

Example 3.20. $\text{Ann}_{\mathbb{Z}}(\mathbb{Z}/n) = n\mathbb{Z}$.

Exercise 3.21. Let R be a ring and M be a module. If $N \subseteq M$ is a subset, then $\text{Ann}_R(N)$ is a left ideal of R . If $N \subseteq M$ is a submodule of R , then $\text{Ann}_R(N)$ is an ideal of R .

Definition 3.22. A module M is said to be **faithful** if $\text{Ann}_R(M) = \{0\}$.

Example 3.23. If K is a field, then K^n is a faithful unitary $M_n(K)$ -module.

Example 3.24. If V is vector space over a field K , then V is faithful unitary $\text{End}_K(V)$ -module.

Definition 3.25. 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 3.26. If R is a simple unitary ring, then R is primitive.

Exercise 3.27. If R is a commutative ring (maybe without identity), then R is primitive if and only if R is a field.

Example 3.28. The ring \mathbb{Z} is not primitive.

Definition 3.29. An ideal P of a ring R is said to be **primitive** if $P = \text{Ann}_R(M)$ for some simple R -module M .

Lemma 3.30. 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 $P = \text{Ann}_R(M)$ 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 $P = \text{Ann}_R(M)$. Since M is a simple R -module, it follows that M is a simple (R/P) -module. Moreover, $\text{Ann}_{R/P} M = \{0\}$. Indeed, if $(r + P) \cdot M = \{0\}$, then $r \in \text{Ann}_R M = P$ 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 $P = \text{Ann}_R(M)$. \square

Example 3.31. Let R_1, \dots, R_n be primitive rings and $R = R_1 \times \dots \times R_n$. Then each $P_i = R_1 \times \dots \times R_{i-1} \times \{0\} \times R_{i+1} \times \dots \times R_n$ is a primitive ideal of R since $R/P_i \simeq R_i$.

Lemma 3.32. Let R be a ring. If P is a primitive ideal, there exists a regular 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 $P = \text{Ann}_R(M)$ for some simple R -module M . By Proposition 3.19, there exists a regular maximal left ideal I such that $M \simeq R/I$. Then $P = \text{Ann}_R(R/I) = \{x \in R : xR \subseteq I\}$.

Conversely, let I be a regular maximal left ideal. By Proposition 3.19, R/I is a simple R -module. Then

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

is a primitive ideal. \square

Exercise 3.33. Maximal ideals of unitary rings are primitive.

Exercise 3.34. Prove that every primitive ideal of a commutative ring is maximal.

Exercise 3.35. Prove that $M_n(R)$ is primitive if and only if R is primitive.

Lecture 4

§4. Jacobson's radical

Definition 4.1. 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 4.2. 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 $x_1 x_2 \dots x_n = 0$ for all $x_1, \dots, x_n \in I$.

Definition 4.3. 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 4.4. 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 4.5. 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 4.6. 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 $n = x \cdot m \neq 0$ for some $x \in I$ and some $m \in M$. Since M is simple, $R \cdot n = M$ 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 4.7. 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

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

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

$$\begin{array}{c|ccc} \circ & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{array}$$

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 4.8. 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 4.9. 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 4.10. 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

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

The following result uses Zorn's lemma.

Lemma 4.11. *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 $x \notin \text{Ann}_R(R/M)$.*

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 3.19. 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 $x \notin \text{Ann}_R(R/M)$. \square

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

Theorem 4.12. *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 $x \notin J(R)$, by definition, there exists a simple R -module M such that $x \cdot m \neq 0$ for some $m \in M$. The simplicity of M implies that $(Rx) \cdot m = M$. Thus there exists $r \in R$ such that $(rx) \cdot m = -m$. There is an element $s \in R$ such that $s + rx + s(rx) = 0$ and hence

$$-m = (rx) \cdot m = (-s - srx) \cdot m = -s \cdot m + s \cdot m = 0,$$

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 4.10. \square

The theorem immediately implies the following corollary.

Corollary 4.13. *If R is a ring, then $J(R)$ is a quasi-regular ideal that contains every quasi-regular left ideal.*

The following result is somewhat what we all had in mind. We first need a lemma.

Lemma 4.14. *Let R be such that $J(R) \neq R$. If I is a left quasi-regular left ideal of R , then $I \subseteq J(R)$.*

Proof. Assume that $I \not\subseteq J(R)$. There exists a simple R -module N such that $I \cdot N \neq \{0\}$. In particular, $I \cdot n \neq \{0\}$ for some $0 \neq n \in N$. Since I is a left ideal, $I \cdot n$ is a non-zero submodule of N . Then $I \cdot n = N$, as N is simple. There exists $x \in I$ such that $x \cdot n = -n$. Since I is left quasi-regular, there exists $r \in R$ such that $r + x + rx = 0$. Thus

$$0 = 0 \cdot n = (r + x + rx) \cdot n = r \cdot n + x \cdot n + (rx) \cdot n = r \cdot n - n - r \cdot n = -n,$$

a contradiction. \square

The following exercise uses Zorn's lemma and will be used in the proof of Theorem 4.16.

Exercise 4.15. Let R be a ring. Prove that every proper left ideal of R that is regular is contained in a maximal ideal that is regular.

Theorem 4.16. *Let R be a ring such that $J(R) \neq R$. Then*

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

Proof. Let

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

Let us prove that $K \subseteq J(R)$. By Lemma 4.14, it is enough to prove that K is left quasi-regular. Let $a \in K$ and $T = \{r + ra : r \in R\}$. If $T = R$, then $-a = r + ra$ for some $r \in R$ and hence a is left quasi-regular. So we need to prove that $T = R$. Note that T is a regular left ideal with $e = -a$ (see Definition 3.17). If $T \neq R$, then T is contained in a maximal left ideal J by the previous exercise. Then $a \in K \subseteq J$ and hence $ra \in J$ for all $r \in R$. Since $r + ra \in T \subseteq J$ for all $r \in R$, it follows that $J = R$, a contradiction. Therefore $T = R$.

Now we prove that $J(R) \subseteq K$. By Proposition 3.19,

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

Let I be a regular maximal left ideal. If $r \in J(R) \subseteq \text{Ann}_R(R/I)$, 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 $J(R) \subseteq K$. \square

Example 4.17. Each maximal ideals of \mathbb{Z} is of the form $p\mathbb{Z} = \{pm : m \in \mathbb{Z}\}$ for some prime number p . Thus $J(\mathbb{Z}) = \bigcap_p p\mathbb{Z} = \{0\}$.

We now review some basic results useful to compute radicals.

Proposition 4.18. *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 $i \in I$. \square

For the next result, we shall need a lemma.

Lemma 4.19. *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

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

Proposition 4.20. *If I is an ideal of R , then $J(I) = I \cap J(R)$.*

Proof. Note that $I \cap J(R)$ is an ideal of I . Let $x \in I \cap J(R)$ and $r \in R$. Since rx is left quasi-regular in R , there exists $s \in R$ such that $s + rx + srx = 0$. Since $s = -rx - srx \in I$, rx is left quasi-regular in I . Thus $I \cap J(R) \subseteq J(I)$.

Let $x \in J(I) \subseteq I$ 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 4.19. \square

Lecture 5

Definition 4.21. A ring R is said to be **radical** if $J(R) = R$.

Example 4.22. If R is a ring, then $J(R)$ is a radical ring, by Proposition 4.20.

Example 4.23. The Jacobson radical of $\mathbb{Z}/8$ is $\{0, 2, 4, 6\}$.

There are several characterizations of radical rings.

Theorem 4.24. *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 4.25. Prove Theorem 4.24.

Example 4.26. 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

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

§5. Commutative rings with no maximal ideals

There are rings with no maximal ideals.

Exercise 5.1. Prove that the additive group of rational numbers is an abelian group with no maximal subgroups.

One can turn the additive group \mathbb{Q} of rational into a non-unitary ring by considering the zero multiplication $xy = 0$ for all $x, y \in \mathbb{Q}$. This ring has no maximal ideals.

Exercise 5.2. Let R be a commutative ring and I be an ideal of R . Prove that I is maximal if and only if R/I is a field or a ring isomorphic to \mathbb{Z}/p with zero multiplication for some prime number p .

Exercise 5.3. Let R be a commutative ring. Prove that $J(R)$ equals the intersection of maximal ideals such that R/M is a field.

Recall that the **characteristic of a ring** is defined as the least positive integer n such that $nx = 0$ for all x . If no such n exists, then we say that the ring is of characteristic zero.

Exercise 5.4. Let R be a ring such and p be a prime number. If $px = 0$ for all $x \in R$, then R has characteristic p .

We now characterize commutative rings with no maximal ideals. The result appeared in [6].

Theorem 5.5 (Henriksen). *Let R be a commutative ring. Then R has no maximal ideals if and only if $J(R) = R$ and $R^2 + pR = R$ for all prime number p .*

Proof. Assume first that R has no maximal ideals. Then $J(R) = R$ by Exercise 5.3. Let p be a prime number such that $I = R^2 + pR \neq R$. Then I is a proper ideal of R . Let $\pi: R \rightarrow R/I$ be the canonical map. Since $R^2 \subseteq I$, $0 = \pi(xy) = \pi(x)\pi(y)$ for all $x, y \in R$. Thus R/I has zero multiplication. By Exercise ??, R/I has characteristic p . Thus R/I is a vector space over the field \mathbb{Z}/p . Let $\{x_\alpha : \alpha \in \Lambda\}$ be a basis of R/I . Every element $x \in R/I$ can be written uniquely as a finite sum of the form $x = \sum \lambda_\alpha x_\alpha$ for scalars λ_α . Let A be the ring with underlying additive group \mathbb{Z}/p and zero multiplication. For a fixed $\beta \in \Lambda$, the map

$$\gamma: R/I \rightarrow A, \quad x = \sum \lambda_\alpha x_\alpha \mapsto \lambda_\beta$$

is a ring homomorphism. The composition $f = \gamma\pi: R \rightarrow R/I \rightarrow A$ is a ring homomorphism. By Exercise 5.2, $\ker f$ is a maximal ideal, a contradiction.

Conversely, let M be a maximal ideal of R . If R/M is a field, then $J(R) \subseteq M \neq R$, a contradiction. By Exercise 5.2, there exists a prime number p such that $R/M \simeq \mathbb{Z}/p$ as abelian groups and zero multiplication (i.e. $xy \in M$ for all $x, y \in R$). Let us write A to denote this ring and $\pi: R \rightarrow R/M$ be the canonical map. Note that $R^2 \subseteq M$. Moreover, $pR \subseteq M$, as $\pi(px) = p\pi(x) = 0$ for all $x \in R$. Thus $R^2 + pR \subseteq M \neq R$, a contradiction. \square

We now present a non-trivial concrete example of a ring with no maximal ideals. For that purpose, we will use the field of fractions $\mathbb{R}(X)$ of the real polynomial ring $\mathbb{R}[X]$.

Exercise 5.6. Let R be the set of rational real functions of the form $f(X)/g(X)$, where $f(X), g(X) \in \mathbb{R}(X)$ and $g(0) \neq 0$. Prove the following statements:

- 1) R is an integral domain with a unique maximal ideal $M = XR$.
- 2) M has no maximal ideals.

Definition 5.7. 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 5.8. Prove that a nil ring is a radical ring.

Exercise 5.9. 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 5.10. 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 . \square

Theorem 5.11. 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, $x_{ij} \in \text{Ann}_R(M)$ 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 is quasi-regular, there exists $y_1 \in R$ such that $x_1 + y_1 + x_1 y_1 = 0$. 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

$$u = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ x_2 y_1 & 0 & \cdots & 0 \\ x_3 y_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x_n y_1 & 0 & \cdots & 0 \end{pmatrix}.$$

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 5.12. Let R be a unitary ring. Then

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

Exercise 5.13. 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 5.14. A pair (X, r) is a **solution** to the Yang–Baxter equation if X is a set and $r: X \times X \rightarrow X \times X$ is a bijective map such that

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

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

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

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

- 1) Let X be a set and $\sigma: X \rightarrow X$ 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

$$\begin{aligned}\lambda_x(y) &= -x + x \circ y = xy + y, \\ \mu_y(x) &= \lambda_x(y)' \circ x \circ y = (xy + y)'x + x\end{aligned}$$

Prove the following statements:

- 2) $\lambda: (R, \circ) \rightarrow \text{Aut}(R, +)$, $x \mapsto \lambda_x$, is a group homomorphism.
 3) $\mu: (R, \circ) \rightarrow \text{Aut}(R, +)$, $y \mapsto \mu_y$, is a group antihomomorphism.
 4) The map

$$r: R \times R \rightarrow R \times R, \quad r(x, y) = (\lambda_x(y), \mu_y(x)),$$

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

Exercise 5.15. If D is a division ring and $R = D[X_1, \dots, X_n]$, then $J(R) = \{0\}$.

Example 5.16. 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 5.17. 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 5.18. 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 5.19. Let A be an algebra. Prove that the Jacobson radical of the ring A coincides with the Jacobson radical of the algebra A .

§6. Amitsur's theorem

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

Lemma 6.1. *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

$$a_0 + a_1x + \dots + a_nx^n = 0.$$

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

$$x^r(1 + b_1x + \dots + b_mx^m) = 0,$$

for some $b_1, \dots, b_m \in K$. Since $1 + b_1x + \dots + b_mx^m$ is a unit by Exercise 5.13, it follows that $x^r = 0$. \square

An application:

Proposition 6.2. *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 4.6 now implies that $J(A)$ is the largest nil ideal of A . \square

Theorem 6.3 (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 6.2.

Assume that K is infinite and let $a \in J(A)$. Exercise 5.13 implies that every element of the form $1 - \lambda^{-1}a$, $\lambda \in K \setminus \{0\}$, is invertible. Thus

§7 Jacobson's conjecture

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

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

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

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 $\beta_1 \neq 0$, 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 6.1. \square

Amitsur's theorem implies the following result.

Corollary 6.4. *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 .*

§7. 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 7.1 (Jacobson). Let R be a noetherian ring. Is then

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

Open problem 7.1 was originally formulated by Jacobson in 1956 [10] for one-sided noetherian rings. In 1965 Herstein [7] found a counterexample in the case of one-sided noetherian rings and reformulated the conjecture as it appears here.

Exercise 7.2 (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.

§8. Köthe's conjecture

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

Open problem 8.1 (Köthe). Let R be a ring. Is the sum of two arbitrary nil left ideals of R nil?

Open problem 8.1 is the well-known Köthe's conjecture. The conjecture was first formulated in 1930, see [12]. It is known to be true in several cases. In full generality, the problem is still open. In [13] 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 [20] 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 [17]. See [21, 22] for more information on Köthe's conjecture and related topics.

Lecture 6

§9. Gilmer's theorem

Hilbert's theorem states that if R is a noetherian commutative unitary ring, then $R[X]$ is noetherian. Following [5], we now present the converse of Hilbert's theorem.

Theorem 9.1 (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

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

Then $I_0 \subseteq I_1 \subseteq \dots \subseteq I_m \subseteq I_{m+1} \subseteq \dots$ 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

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

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 $a_n = r_2 a_n$. 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 $R[X] \rightarrow R$, $f(X) \mapsto f(0)$, be an evaluation map. Since it is a surjective ring homomorphism, R is noetherian. In particular, R is finitely generated, say

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

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

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

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

§10. Artinian modules

Definition 10.1. Let R be a ring. A module N is **artinian** if every decreasing sequence $N_1 \supseteq N_2 \supseteq \dots$ 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 10.2. 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

$$N_1 \supsetneq N_2 \supsetneq \dots \supsetneq N_k$$

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 $N_1 \supsetneq N_2 \supsetneq \dots$ that cannot stabilize, a contradiction.

If $N_1 \supseteq N_2 \supseteq \dots$ 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 $N_1 \subseteq N_2 \subseteq \dots$ 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 10.3. 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 S of submodules of M contains a maximal element, that is an element $X \in S$ such that there is no $Z \in S$ such that $X \subsetneq Z$.

Exercise 10.4. Prove that a ring R is left noetherian if every sequence of left ideals $I_1 \subseteq I_2 \subseteq \cdots$ stabilizes.

Exercise 10.5. 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 10.6. A ring R is **left artinian** if the module ${}_R R$ is artinian.

Similarly one defines right artinian rings.

Example 10.7. 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 10.8. Prove that a ring R is left artinian if every sequence of left ideals $I_1 \supseteq I_2 \supseteq \cdots$ stabilizes.

Definition 10.9. 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 10.10. 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 10.5.

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 10.2). 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 . \square

Definition 10.11. Let M be a module. We say that the composition series

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

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

Theorem 10.13 (Jordan–Hölder). Any two composition series for a module are equivalent.

Proof. Let M be a module and

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

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 $M \supseteq \{0\}$ 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 10.10. The submodule $U = V_1 \cap W_1$ is also artinian and noetherian and hence, by Theorem 10.10, it admits a composition series

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

Thus $V_1 \supseteq \cdots \supseteq V_k = \{0\}$ and $V_1 \supseteq U \supseteq U_1 \supseteq \cdots \supseteq U_r = \{0\}$ 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. \square

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

Definition 10.14. 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 10.15. 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 10.16. If A and B are finite-length submodules of M , then

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

Theorem 10.17. 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. \square

Corollary 10.18. 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 4.6, L is contained in $J(R)$. Thus L is nilpotent, as $J(R)$ is nilpotent by Theorem 10.17. \square

§11. Akizuki's theorem

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

Exercise 11.1. 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 11.2. Let R be a 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 11.3 (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 $f: I \rightarrow rI$, $x \mapsto rx$. 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 11.1, $\dim_K I = \infty$. 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 11.1). This is a contradiction, because J is an ideal of R such that $J \subsetneq I$. \square

Lecture 7

§12. Local rings

In this section, we will consider arbitrary rings with one.

Definition 12.1. A ring is said to be **local** if it contains only one maximal left ideal.

Division rings are local rings.

Theorem 12.2. Let R be a ring and $I = R \setminus \mathcal{U}(R)$. The following statements are equivalent:

- 1) R is local.
- 2) $R/J(R)$ is a division ring.
- 3) $I = J(R)$.
- 4) I is an ideal of R .

Proof. We first prove 1) \implies 2). Let M be the maximal left ideal of R . Then $J(R) = M$. Let $x \notin M$. Then $R = Rx + M$, so $1 = rx + m$ for some $r \in R$ and $m \in M$. Thus $r + M$ is a left inverse of $x + M$ and hence R/M is a division ring. In particular, $r \notin M$. Since $R = Rr + M$, there exists $y \in R$ such that $1 = yr$. Therefore $y + M$ is a left inverse of $r + M$. Thus

$$\begin{aligned} y + M &= (y + M)(1 + M) = (y + M)(r + M)(x + M) \\ &= (yr + M)(x + M) = (1 + M)(x + M) = x + M \end{aligned}$$

and hence $x + M$ is invertible.

Now we prove 2) \implies 3). Clearly $J(R) \subseteq I$. Conversely, let $x \in I$. If $x \notin J(R)$, then $x + J(R) \neq 0$. Since $R/J(R)$ is a division ring, $x + J(R) \in \mathcal{U}(R/J(R))$. In particular, $1 - rx \in J(R) \subseteq I$ for some $r \in R$. Since $x \in I$, $rx \in I$. Therefore $1 = 1 - rx + rx \in I$, a contradiction.

It is trivial that 3) \implies 4).

Finally, we prove 4) \implies 1). Let M be a maximal left ideal of R . Then $M \subseteq I$. Since M is maximal and I is in particular a left ideal of R , it follows that $M = I$. \square

Definition 12.3. An element x of a ring is said to be **idempotent** if $x^2 = x$.

Examples of idempotents are 0 and 1. An idempotent x is said to be **non-trivial** if $x \notin \{0, 1\}$.

Exercise 12.4. Let p be a prime number and $m > 0$. Prove that the only idempotents of \mathbb{Z}/p^m are 0 and 1.

Exercise 12.5. How many idempotent does \mathbb{Z}/n have?

Exercise 12.6. Let R be a ring with one and I be an ideal of R . We say that an idempotent $x \in R/I$ can be lifted if $x = e + I$ for some idempotent e of R . Prove that if every element of I is nilpotent, then every idempotent of R/I can be lifted.

The previous exercise shows that if R is left artinian, every idempotent of $R/J(R)$ can be lifted to R .

Lemma 12.7. Let R be a left artinian ring. Then $J(R)$ is nil.

Proof. Let $x \in J(R)$. The sequence $Rx \supseteq Rx^2 \supseteq \cdots$ stabilizes, so $Rx^n = Rx^{n+1}$ for some n . In particular, there exists $r \in R$ such that $x^n = rx^{n+1}$. This implies that $(1 - rx)x^n = 0$. Since $x \in J(R)$, the element $1 - rx$ is invertible. Hence $x^n = 0$. \square

Theorem 12.8. Let R be a left artinian ring. Then R is local if and only if R has no non-trivial idempotents.

Proof. Let us first prove \implies . For this implication, we do not need to use that R is left artinian. Let $x \in R$ be an idempotent. Then $x(1 - x) = 0$. If $x \in \mathcal{U}(R)$, then $x = 1$. If $1 - x \in \mathcal{U}(R)$, then $x = 0$. If $x \notin \mathcal{U}(R)$ and $1 - x \notin \mathcal{U}(R)$, then, since $R \setminus \mathcal{U}(R)$ is an ideal of R , it follows that $1 = x + 1 - x \notin \mathcal{U}(R)$, a contradiction.

Now we prove \impliedby . By the previous lemma, $J(R)$ is nil. By the previous exercise, every idempotent of $R/J(R)$ can be lifted. Thus $R/J(R)$ has no non-trivial idempotents. On the other hand, by Artin–Wedderburn,

$$R/J(R) \simeq \prod_{i=1}^k M_{n_i}(D_i)$$

for some $n_1, \dots, n_k \geq 1$ and division rings D_1, \dots, D_k . Then $k = n_1 = 1$, as $R/J(R)$ has no non-trivial idempotents. Since $R/J(R)$ is a division ring, R is local by the previous theorem. \square

Theorem 12.9. The center of a local ring is local.

Proof. Let R be a local ring. By Theorem 12.2, $J(R) = R \setminus \mathcal{U}(R)$. We need to prove that $Z(R) \setminus \mathcal{U}(Z(R)) = J(Z(R))$. We first note that

$$\mathcal{U}(Z(R)) = Z(R) \cap \mathcal{U}(R). \quad (7.1)$$

§13 Semiprime and semiprimitive rings

We claim that $Z(R) \cap J(R) \subseteq J(Z(R))$. Let $x \in Z(R) \cap J(R)$. Let $z \in Z(R)$. Since $x \in J(R)$, $1 - zx \in \mathcal{U}(R)$. Moreover, $1 - zx \in Z(R)$. Thus

$$1 - zx \in Z(R) \cap \mathcal{U}(R) = \mathcal{U}(Z(R)).$$

Hence $x \in J(Z(R))$.

To prove the theorem it is enough to show that $Z(R) \setminus \mathcal{U}(Z(R)) = J(Z(R))$. Let us prove the non-trivial inclusion. Let $x \in Z(R) \setminus \mathcal{U}(Z(R))$. Then (7.1) implies that $x \notin \mathcal{U}(R)$. By Theorem 12.2, $x \in J(R)$. Then $x \in J(R) \cap Z(R) \subseteq J(Z(R))$. \square

Exercise 12.10. Let R be a local ring. Prove that $Z(R) = J(R) \subseteq J(Z(R))$.

Exercise 12.11. Prove that a ring is local if and only if it contains only one maximal right ideal.

Exercise 12.12. Find a non-local ring with a unique maximal ideal.

Exercise 12.13. Let R be a ring with at least three elements. If $|\mathcal{U}(R)| = 1$, then R is not local.

A ring R is said to be **Von Neumann regular** if for every non-zero $r \in R$, $r = rxr$ for some $x \in R$.

Exercise 12.14. Prove that a ring R is local if and only if R is a division ring.

Exercise 12.15. Let R be a ring such that every element of R is either nilpotent or a unit. Prove that R is local.

A ring R is said to be **semilocal** if $R/J(R)$ is left artinian.

Exercise 12.16. Prove the following statements:

- 1) Every local ring is semilocal.
- 2) R is semilocal if and only if $R/J(R)$ is semisimple.
- 3) If R has finitely many maximal ideals, then R is semilocal.
- 4) If R_1, \dots, R_k are rings, then $\oplus_{i=1}^k R_i$ is semilocal if and only if each R_i is semilocal.

Example 12.17. Let R be a ring such that $R/J(R)$ is commutative. Prove that R is semilocal if and only if R has finitely many maximal ideals.

§13. Semiprime and semiprimitive rings

Definition 13.1. 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 13.2. 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 13.3. \mathbb{Z} is semiprimitive, as $J(\mathbb{Z}) = \cap_p p\mathbb{Z} = \{0\}$.

Example 13.4. Let $R = C[a, b]$ be the ring of continuous maps $f: [a, b] \rightarrow \mathbb{R}$. 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 5.10 (Lecture 4) that $R/J(R)$ is semiprimitive.

Definition 13.5. Let $\{R_i : i \in I\}$ be an arbitrary family of rings. For each $j \in I$, let $\pi_j: \prod_{i \in I} R_i \rightarrow R_j$ 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 $R \rightarrow \prod_{i \in I} R_i$.
- 2) For each j , the composition $\pi_j f: R \rightarrow R_j$ is injective.

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

Exercise 13.6. Write (if possible) \mathbb{Z} as a non-trivial subdirect product.

Example 13.7. Let R be a ring, $\{I_j : j\}$ be a collection of ideals of R and

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

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 13.8. 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 $\lambda_j: R \rightarrow R/P_j$ and $\pi_j: \prod_{i \in I} R/P_i \rightarrow R/P_j$ be canonical maps. The ring homomorphism

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

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 $\varphi: R \rightarrow \prod_{i \in I} R_i$ 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 $J(R) \subseteq \cap_{i \in I} P_i = 0$. \square

Example 13.9. The ring $C[a, b]$ of Example 13.4 is isomorphic to a subdirect product of the fields $C[a, b]/U_c \simeq \mathbb{R}$.

Definition 13.10. A ring R **semiprime** if $aRa = \{0\}$ implies $a = 0$.

Proposition 13.11. 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 $\mathbb{Z}a = \{0\}$. \square

Two consequences:

Exercise 13.12. A commutative ring is semiprime if and only if it does not contain non-zero nilpotent elements.

We will prove in Lecture 9 (Corollary 19.5) that the if G is a group, then the ring $\mathbb{C}[G]$ is semiprime.

Exercise 13.13. Let D be a division ring.

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

§14. 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 14.1. Let D be a division ring, and V be a vector space over D . A subring $R \subseteq \text{End}_D(V)$ 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 14.2. Let D be a division ring and V be a finite-dimensional D -vector space. Then $\text{End}_D(V)$ 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, $R \subseteq \text{End}_D(V)$. If $g \in \text{End}_D(V)$ 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 $g = f \in R$. \square

Theorem 14.3 (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 14.4. 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 $j \in \{1, \dots, n\}$. \square

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

Proof of Theorem 14.3. 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 $f \in \text{Ann}_R(V)$, 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 $D = \text{End}_R(V)$ is a division ring. Thus V is a D -vector space with

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

For $r \in R$ let

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

A straightforward calculation shows that $\gamma_r \in \text{End}_D(V)$ and that $R \rightarrow \text{End}_D(V)$, $r \mapsto \gamma_r$, 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

$$\delta : V \rightarrow V, \quad v \mapsto lv,$$

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 $v = l_1u = l_2u$, then $(l_1 - l_2)u = 0$ and thus

$$0 = \delta(0) = \delta((l_1 - l_2)u) = (l_1 - l_2)w = l_1w - l_2w.$$

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 $i \in \{1, \dots, n\}$. \square

Corollary 14.5. *If R is a primitive ring, then either there exists a division ring D such that $R \simeq \text{End}_D(V)$ 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 $R_m \rightarrow \text{End}_D(V_m)$ 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 $\gamma: R \rightarrow \text{End}_D(V)$, $r \mapsto \gamma_r$, 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 14.2. 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

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

is a surjective ring homomorphism. □

Lecture 8

§15. 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 15.1. 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 15.2. A commutative ring is prime if and only if it is a domain, as $ab = 0$ if and only if $aRb = \{0\}$.

Example 15.3. A non-zero ideal of a prime ring is a prime ring.

Exercise 15.4. A ring is a domain if and only if it is both prime and reduced.

A characterization of prime rings:

Proposition 15.5. 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 15.6. 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 15.7 (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 [18, Theorem 2.10 of Chapter 4]. \square

Lemma 15.8. *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 $x \in \text{Ann}_R(L)$. Since $xRy \in xRL \subseteq xL = \{0\}$, it follows that $x = 0$. \square

Lemma 15.9. *Let D be a division ring and R be a dense ring in a module V over D . If R is left artinian, then $\dim_D V < \infty$.*

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

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

Each I_j is a left ideal of R and $I_1 \supseteq I_2 \supseteq \dots \supseteq I_n \supseteq \dots$. 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 $I_1 \supseteq I_2 \supseteq \dots \supseteq I_n \supseteq \dots$, a contradiction. \square

Theorem 15.10 (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 15.8, 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 15.9 implies that $R = \text{End}_D(V) \simeq M_n(D)$, 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 [9]– 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

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

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 15.11. 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 15.12. *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. \square

Theorem 15.13 (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 15.14. *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 3.30. By Wedderburn’s theorem, R/I is simple. Thus I is maximal by Proposition 3.19. \square

Lemma 15.15. *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. \square

Lemma 15.16. *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 $I_1 \supseteq I_1 I_2 \supseteq \dots$ 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. \square

Now we are ready to prove the theorem.

Proof of Theorem 15.13. 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, $I_1 \cap \dots \cap I_k = J(R) = \{0\}$. Let

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

Then φ is a ring homomorphism with kernel $I_1 \cap \dots \cap I_k = \{0\}$, 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, $I_2 \cdots I_k \not\subseteq I_1$. 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

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

§16. 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 16.1. 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 16.2. *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 10.2. \square

Definition 16.3. 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 $R = \bigoplus_{i \in I} L_i$, 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 $R = \bigoplus_{j \in J} L_j$, 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 16.4. *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 10.10. It follows from the definitions that R is left artinian and left noetherian. \square

Exercise 16.5. If R is a semisimple ring, every R -module is semisimple.

Exercise 16.6. 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 16.7. *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 $R \simeq L_1 \oplus \dots \oplus L_k$. 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

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

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

Conversely, if R is left artinian and $J(R) = \{0\}$, then $R \simeq M_{n_1}(D_1) \times \dots \times M_{n_k}(D_k)$ 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. \square

§17. Hopkins–Levitski theorem

Theorem 17.1 (Hopkins–Levitski). *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 10.17. Let n be such that $J^n = \{0\}$. Now consider the sequence

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

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 5.10, 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. \square

Theorem 17.2 (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.*

§17 Hopkins–Levitski theorem

Proof. It follows from Theorem 15.7 and Hopkins–Levitzky theorem; see [18, Theorem 1.1 of Chapter 10]. \square

Lecture 9

§18. Andrunakevic–Rjabuhin’s theorem

Definition 18.1. A ring R is **reduced** if has no non-zero nilpotent elements.

Every commutative domain is reduced.

Example 18.2. The ring $\mathbb{Z} \times \mathbb{Z}$ with the usual operations is reduced but not a domain.

Example 18.3. The ring $\mathbb{Z}/6$ is reduced. However, $\mathbb{Z}/4$ is not reduced.

Exercise 18.4. Prove that a ring R is **reduced** if and only if for all $r \in R$ such that $r^2 = 0$ one has $r = 0$.

Exercise 18.5. 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 18.6. 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 18.7. Let R be a ring and I be an ideal of R . Then I 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 18.8 (Andrunakevic–Rjabuhin). *Let R be a non-zero ring. If R is reduced, there exists an ideal I of R such that then R/I has no non-zero zero-divisors.*

Let R be a ring and I be an ideal of R . If S is a subset of R , the *left annihilator* of S modulo I is the set $\{r \in R : rS \subseteq I\}$.

Lemma 18.9. *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 $aas = a^2s \in I$ 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 $a \in A$. \square

Similarly, if S is a subset of a ring R , then the right annihilator $\{r \in R : Sr \subseteq I\}$ of S modulo I is a reduced ideal.

Proof of Theorem 18.8. 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 $a \in A$, $M \subseteq A$. Similarly, since $b \in B$, $M \subseteq B$. 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. \square

Exercise 18.10. Prove that a reduced ring is a subdirect product of rings without non-zero divisors.

Exercise 18.11. Is the ring $\mathbb{C}[\mathbb{Z}/2]$ reduced?

Open problem 18.1. Let G be a torsion-free group. Is $K[G]$ reduced?

Problem 18.1 is related to other important open problems about group algebras (e.g. zero-divisors, units, idempotents and semisimplicity of group rings).

Exercise 18.12. Prove that idempotents of reduced rings are central.

The previous exercise is used to solve the following problem.

Exercise 18.13. Let R be a ring such that $x^3 = x$ for all $x \in R$. Prove that R is commutative.

Exercise 18.13 is hard. Even harder is the following exercise:

Exercise 18.14. Let R be a ring such that $x^4 = x$ for all $x \in R$. Prove that R is commutative.

Exercise 18.15. Reduced rings are semiprime.

Theorem 18.16. *Let K be a field and G be a group. If $K[G]$ is reduced, then every finite subgroup of G is normal.*

§19 Rickart's theorem

Proof. Let $H = \{h_1, \dots, h_n\}$ be a finite normal subgroup of G . We claim that $n = |H|$ is invertible in K . If $\text{char } K = 0$, this is clear. If $\text{char } K = p > 0$ and n is not invertible in K , then p divides $n = |H|$. By Cauchy's theorem, there exists an element $h \in H$ of order n , that is $|h| = n$. Since $(1 - h)^p = 1 - h^p = 0$ and $K[G]$ is reduced, $h = 1$, a contradiction.

Let $\alpha = \frac{1}{n} \sum_{i=1}^n h_i \in K[G]$. Then

$$\alpha^2 = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n h_i h_j = \frac{1}{n^2} \sum_{i=1}^n n \alpha = \alpha.$$

Thus α is idempotent. As idempotent element of reduced rings are central (Exercise 18.12), $g\alpha g^{-1} = \alpha$ for all $g \in G$. If $g \in G$, then

$$\sum_{i=1}^n g h_i g^{-1} = \sum_{i=1}^n h_i.$$

It follows that H is normal in G , as for each $i \in \{1, \dots, n\}$ there exists $j \in \{1, \dots, n\}$ such that $g h_i g^{-1} = h_j \in H$. \square

Example 18.17. If K is a field, then $K[\mathbb{S}_3]$ is not reduced. In fact, if

$$\alpha = (12) + (123) - (132) - (13),$$

then $\alpha^2 = 0$.

Exercise 18.18. Prove that the converse of Theorem 18.16 does not hold.

§19. Rickart's theorem

We now consider Jacobson's semisimplicity problem.

Open problem 19.1. Let G be a group and K be a field. When $J(K[G]) = \{0\}$?

As an application of Amitsur's theorem 6.3, 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 19.2 (Rickart). *Let G be a group. Then $J(\mathbb{C}[G]) = \{0\}$.*

To prove the theorem, we need a lemma.

Lemma 19.3. *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 6.3. 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 6.3. \square

We now prove the theorem.

Proof of Theorem 19.2. For $\alpha = \sum_{i=1}^n \lambda_i g_i \in \mathbb{C}[G]$ let

$$\alpha^* = \sum_{i=1}^n \bar{\lambda}_i g_i^{-1}.$$

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

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

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

Exercise 19.4. If G is a group, then $J(\mathbb{R}[G]) = 0$.

Corollary 19.5. 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 4.6, 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. \square

Exercise 19.6. 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 1.23. However, in the arbitrary setting we are considering, we need to use Zorn's lemma.

Lemma 19.7. *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 $M_i \not\subseteq N \oplus N_1$. The simplicity of M_i implies that $M_i \cap (N \oplus N_1) = \{0\}$, which contradicts the maximality of K . \square

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

Proposition 19.8. *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 $If = (Re)f = R(ef) = \{0\}$ (note that $I = Re$ because $x = xe$ for all $x \in I$), 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. \square

Theorem 19.9. *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 16.7. \square

Lecture 10

§20. Maschke's theorem

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

Theorem 20.1 (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

$$\rho: K[G] \rightarrow K, \quad \alpha \mapsto \text{trace}(L_\alpha),$$

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 4.6 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 20.2. *Let G be a finite group. Then $K[G]$ does not contain non-zero nil left ideals.*

§21. 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 21.1. 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 21.2. Every finite group is locally finite

Example 21.3. The group \mathbb{Z} is not locally finite because it is torsion-free.

Example 21.4. 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 21.5. Let X be an infinite set and \mathbb{S}_X be the set of bijective maps $X \rightarrow X$ 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 21.6. 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 21.7. *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 $\pi: G \rightarrow G/N$ 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 some $g_{n+1}, \dots, g_m \in G$.

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 $|H| \leq m|U|$. \square

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

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \dots \subsetneq G_n = G \quad (10.1)$$

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

Example 21.8. Abelian groups are solvable.

Subgroups and quotients of solvable groups are solvable.

Example 21.9. Groups of order < 60 are solvable.

Example 21.10. A_5 and 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 21.11. *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 21.7. \square

We now prove Herstein's theorem.

Theorem 21.12 (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 $H = \langle \text{supp } \alpha \rangle$ 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

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

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

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

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

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

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

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

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

Since K is of characteristic zero, it follows that $w \in \text{supp}(\alpha^{n+1})$. Since, moreover, $\alpha^{n+1} = \sum_{j=0}^n a_j \alpha^j$, it follows that $w \in \text{supp}(\alpha^j)$ 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

§22. Formanek's theorem, I

Exercise 22.1. 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 22.2. 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 22.3 (Formanek). Let G be a group. If every element of $\mathbb{Q}[G]$ is invertible or a zero divisor, then G is locally finite.

§22 Formanek's theorem, I

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

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

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

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

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

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

Then

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

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 $\lim_{k \rightarrow \infty} |\gamma_k| = 0$.

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

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

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

Lecture 11

§23. 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 23.1. *Let U and V be vector spaces. Then there exists a bilinear map $U \times V \rightarrow U \otimes V$, $(u, v) \mapsto u \otimes v$, 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 $\beta: U \times V \rightarrow W$ is a bilinear map, there exists a linear map $\bar{\beta}: U \otimes V \rightarrow W$ such that $\bar{\beta}(u \otimes v) = \beta(u, v)$ for all $u \in U$ and $v \in V$.

Proof. By definition, the map

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

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

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

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

$$\begin{array}{ccc} K[U \times V] & \xrightarrow{\gamma} & W \\ \downarrow & \nearrow & \\ U \otimes V & & \end{array}$$

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

Exercise 23.2. Prove that the properties of the previous theorem characterize tensor products up to isomorphism.

Some properties:

Proposition 23.3. Let $\varphi: U \rightarrow U_1$ and $\psi: V \rightarrow V_1$ be linear maps. There exists a unique linear map $\varphi \otimes \psi: U \otimes V \rightarrow U_1 \otimes V_1$ such that

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

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

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

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

is well-defined. □

Exercise 23.4. 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 23.5. If U and V are vector spaces, then $U \otimes V \simeq V \otimes U$.

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

Exercise 23.6. Prove that $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$.

Exercise 23.7. Prove that $U \otimes K \simeq U \simeq K \otimes U$.

Proposition 23.8. 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

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

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

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

Exercise 23.9. Prove that $u \otimes v = 0$ and $v \neq 0$ imply $u = 0$.

Theorem 23.10. 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 $0 = \sum_k u_{i_k} \otimes (\sum_l \lambda_{kl} v_{j_l})$. Since the u_{i_k} are linearly independent, Proposition 23.8 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. \square

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

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

Corollary 23.11. 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

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

Exercise 23.12. 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 23.13. 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 23.14. *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

$$K[G] \otimes K[H] \rightarrow K[G \times H], \quad g \otimes h \mapsto (g, h),$$

that is multiplicative. Thus $K[G] \otimes K[H] \simeq K[G \times H]$ as algebras. \square

Proposition 23.15. *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 $A \otimes K[X] \mapsto A[X]$, $\sum a_i \otimes X^i \mapsto \sum a_i X^i$, is a linear algebra isomorphism. \square

Exercise 23.16. 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 23.15 and Exercise 23.16 are examples of a procedure known as **scalar extensions**.

Theorem 23.17. *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 $E \times A \rightarrow E \otimes_K A$, $(\mu, a) \mapsto (\lambda\mu) \otimes a$, is K -bilinear, there exists a linear map $E \otimes_K A \rightarrow E \otimes_K A$, $\mu \otimes a \mapsto (\lambda\mu) \otimes a$. 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 $\lambda, \mu \in E$. \square

Exercise 23.18. 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 23.19. Prove that if G is a group and K is a subfield of E , then

$$E \otimes_K K[G] \simeq E[G].$$

§24. 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 24.1 (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 $\beta \in K \otimes_{\mathbb{Q}} \mathbb{Q}[G]$ 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

§25. Wedderburn's little theorem

Definition 25.1. The n -th cyclotomic polynomial is defined as the polynomial

$$\Phi_n(X) = \prod (X - \zeta), \quad (11.1)$$

where the product is taken over all n -th primitive roots of one.

Some examples:

$$\begin{aligned} \Phi_2 &= X - 1, \\ \Phi_3 &= X^2 + X + 1, \\ \Phi_4 &= X^2 + 1, \\ \Phi_5 &= X^4 + X^3 + X^2 + X + 1, \\ \Phi_6 &= X^2 - X + 1, \\ \Phi_7 &= X^6 + X^5 + \dots + X + 1. \end{aligned}$$

Lemma 25.2. *If $n \in \mathbb{Z}_{>0}$, then*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Proof. Write

$$X^n - 1 = \prod_{j=1}^n (X - e^{2\pi i j/n}) = \prod_{d|n} \prod_{\substack{1 \leq j \leq n \\ \gcd(j,n)=d}} (X - e^{2\pi i j/n}) = \prod_{d|n} \Phi_d(X). \quad \square$$

Lemma 25.3. *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 $\Phi_n(X) / \prod_{d|n, d < n} \Phi_d(X) \in \mathbb{Z}[X]$. \square

Theorem 25.4 (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 D is a K -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

$$q^n - 1 = q - 1 + \sum_{j=1}^m \frac{q^n - 1}{q^{d_j} - 1}, \quad (11.2)$$

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

$$X^n - 1 = \Phi_n(X)(X^{d_j} - 1)h(X) \quad (11.3)$$

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. \square

There are several proofs of Wedderburn's theorem. For example, [23] contains a proof that uses only elementary linear algebra. In [19, Chapter 14] the theorem is proved using group theory.

Theorem 25.5. *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. The lemma uses a well-known result from elementary number theory: If φ is the Euler function that counts the positive integers up to a given integer n that are relatively prime to n , then

$$\sum_{d|n} \varphi(d) = n.$$

Let us present a quick group-theoretical proof. Let $G = \langle g \rangle$ be the cyclic group of order n . Then

$$n = |G| = \sum_{1 \leq d \leq n} |\{g \in G : |g| = d\}| = \sum_{d|n} |\{g \in G : |g| = d\}|$$

by Lagrange's Theorem. Since G is cyclic, for each $d | n$, $\langle g^{n/d} \rangle$ is the unique subgroup of G of order d . Now the claim follows, as each subgroup of the form $\langle g^{n/d} \rangle$ has $\varphi(d)$ generators.

Lemma 25.6. *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

$$\sum_{d|n} f(d) = n. \quad (11.4)$$

We claim that if $d | n$ 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 $p(X) = X^d - 1 \in K[X]$. 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 $f(d) = \varphi(d)$.

Since $\sum_{d|n} \varphi(d) = n$ and (11.4), it follows that $f(n) = \varphi(n) \neq 0$. Hence there exists $g \in G$ such that $|g| = n = |G|$ and G is cyclic. \square

Proof of Theorem 25.5. 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. \square

§26. Zsigmondy's theorem

One of Wedderburn's original proof of Theorem 25.4 uses a result proved by Zsigmondy [25]. Zsigmondy's theorem is quite popular in mathematical contests.

Theorem 26.1 (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 [24]. \square

We now quickly sketch a proof of Wedderburn's theorem 25.4 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 x . Note that F is a finite-dimensional (\mathbb{Z}/p) -vector space. Let $m = \dim F$. Since $x^{p^m-1} = 1$, 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.

§27. Fermat's last theorem in finite rings

Theorem 27.1. *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 $x^n + y^n = z^n$. \square

Lecture 12

§28. Frobenius's theorem

Theorem 28.1 (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 28.2. *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 at x . 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 28.3. *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. If $x \in D \setminus V$ is such that $x^2 \in \mathbb{R}$, then, 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

$$\alpha^2 x^2 = \beta^2 y^2 + 2\beta\gamma y + \gamma^2 = (-\beta y - \gamma)^2.$$

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 $x \in \mathbb{R}$, a contradiction. Hence

$$x = -\lambda/2 + (x + \lambda/2) \in \mathbb{R} \oplus V. \quad \square$$

Lemma 28.4. *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*

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i. \quad (12.1)$$

Proof. Let $V = \{x \in D : x^2 \in \mathbb{R}, x^2 \leq 0\}$ be the subspace of Lemma 28.3. 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

$$x \circ y = \left(z - \frac{z \circ y}{y \circ y} y \right) \circ y = zy - \frac{z \circ y}{y \circ y} y^2 + yz - \frac{z \circ y}{y \circ y} y^2 = z \circ y - \frac{z \circ y}{y \circ y} y \circ y = 0,$$

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,

§29 Jacobson's commutativity theorem

$$ji = \frac{1}{\sqrt{-y^2}} \frac{1}{\sqrt{-x^2}} yx = \frac{1}{\sqrt{-x^2}} \frac{1}{\sqrt{-y^2}} (-xy) = -k. \quad \square$$

Now we are finally ready to prove the theorem:

Proof of 28.1. 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 28.3 is non-zero and thus there exists $i \in D$ such that $i^2 = -1$. Hence $D \simeq \mathbb{C}$. Lemma 28.4 implies that $n \neq 3$. If $n = 4$, then $D \simeq \mathbb{H}$. Suppose that $n > 4$. By Lemma 28.4 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 28.3, $\dim V = n - 1$. 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. \square

§29. Jacobson's commutativity theorem

Exercise 29.1. 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 29.2. 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. \square

In this lecture, we will prove extend the result of Proposition 29.2 to arbitrary (i.e. non-finite) rings.

Theorem 29.3 (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 29.4. *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 $\text{ad } r: R \rightarrow R, x \mapsto rx - xr$, is a derivation. This means that $\text{ad}(xy) = (\text{ad } x)y + x(\text{ad } y)$ for all $x, y \in R$. By induction one proves that

$$(\text{ad } r)^n(x) = \sum_{k=0}^n (-1)^k \binom{n}{k} r^{n-k} x r^k \quad (12.2)$$

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 29.5. Let p be a prime number and R be a ring of characteristic p . Prove that $(\text{ad } r)^{p^n} = \text{ad } r^{p^n}$.

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

Proof of Theorem 29.3. 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 $R \rightarrow \prod_{i \in I} R/P_i$, $r \mapsto (r + P_i)_{i \in I}$, 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 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 $R \simeq D^{\text{op}}$, 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 $\delta = \text{ad } x: R \rightarrow R, y \mapsto xy - yx$, is a K -linear map. Moreover, by the exercise,

$$\delta^{p^k} = (\text{ad } x)^{p^k} = \text{ad } (x^{p^k}) = \text{ad } x = \delta$$

and

$$\delta(\delta - x_1 \text{id}) \cdots (\delta - x_{p^k-1} \text{id}) = 0 \quad (12.3)$$

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. \square

There are elementary proofs of Jacobson's commutativity theorem. See for example [16].

§30. Skolem–Noether theorem

Definition 30.1. 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 30.2. 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 $a \in Z(A) = K1$. \square

Example 30.3. \mathbb{H} is a real central algebra.

Example 30.4. \mathbb{C} is a complex central algebra but it is not a real central algebra.

Frobenius' theorem 28.1 translates into the following statement: Every finite-dimensional real central division algebra is isomorphic to \mathbb{R} or \mathbb{H} .

Proposition 30.5. 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. \square

For an algebra A , let $L: A \rightarrow \text{End}_K(A)$, $a \mapsto L_a$, and $R: A \rightarrow \text{End}_K(A)$, $a \mapsto R_a$, be given by $L_a(x) = ax$ and $R_a(x) = xa$. Then both L and R are linear maps such that

$$L_{ab} = L_a L_b, \quad R_{ab} = R_b R_a, \quad L_a R_b = R_b L_a$$

for all $a, b \in A$.

Definition 30.6. Let A be an algebra. The **algebra of multipliers** of A is

$$M(A) = \left\{ \sum_{j=1}^n L_{a_j} R_{b_j} : n \in \mathbb{Z}_{\geq 0}, a_1, \dots, a_n, b_1, \dots, b_n \in A \right\}.$$

It is an exercise to show that $M(A)$ is a subalgebra of $\text{End}_K(A)$. Moreover, if A is unitary, then $M(A)$ is generated by the L_a and the R_b for $a, b \in A$.

Lemma 30.7. *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 30.8. *Let A be a central simple algebra. If $\sum_{i=1}^n L_{a_i} R_{b_i} = 0$ and $\{b_1, \dots, b_n\}$ (resp. $\{a_1, \dots, a_n\}$) is linearly independent, then $a_i = 0$ (resp. $b_i = 0$) for all i .*

Proof. The result holds for $n = 1$. We want to prove that if $a_1 x b_1 = 0$ for all $x \in A$ and $b_1 \neq 0$, then $a_1 = 0$. Assume that $a_1 \neq 0$. The ideal of A generated by a_1 is non-zero, and hence it is equal to A . Thus there exist $u_1, \dots, u_m, v_1, \dots, v_m \in A$ such that $1 = \sum_{j=1}^m u_j a_1 v_j$. Write

$$0 = \sum_{j=1}^m L_{u_j} (L_{a_1} R_{b_1}) L_{v_j} = \sum_{j=1}^m L_{u_j a_1 v_j} R_{b_1} = R_{b_1}.$$

Hence $b_1 = 0$.

Assume that the lemma is not true and let $n > 1$ be the smallest positive integer where the lemma is false. Assume that $a_n \neq 0$. Since A is simple, the ideal generated by a_n is A . Then there exist $u_1, \dots, u_m, v_1, \dots, v_m \in A$ such that $1 = \sum_{j=1}^m u_j a_1 v_j$ and

$$0 = \sum_{j=1}^m L_{u_j} \left(\sum_{i=1}^n L_{a_i} R_{b_i} \right) L_{v_j} = \sum_{i=1}^n \sum_{j=1}^m L_{u_j a_i v_j} R_{b_i} = \sum_{i=1}^n L_{c_i} R_{b_i},$$

where $c_i = \sum_{j=1}^m u_j a_i v_j$ and $c_n = 1$. Since

$$0 = L_x \left(\sum_{i=1}^n L_{c_i} R_{b_i} \right) - \left(\sum_{i=1}^n L_{c_i} R_{b_i} \right) L_x = \sum_{i=1}^{n-1} L_{x c_i - c_i x} R_{b_i}$$

for all $x \in A$, it follows that $x c_i - c_i x = 0$ for all $x \in A$. Since A is central, $c_i \in k$ for all $i \in \{1, \dots, n-1\}$. Evaluate $0 = \sum_{i=1}^n L_{c_i} R_{b_i}$ in 1_A we obtain that $0 = c_1 b_1 + \dots + c_n b_n$, a contradiction since $\{b_1, \dots, b_n\}$ is linearly independent. □

Lemma 30.9. *If A is a finite-dimensional central simple algebra, then*

$$M(A) = \text{End}_K(A).$$

Proof. Let $\{a_1, \dots, a_n\}$ be a basis of A . We claim that $\{L_{a_i}R_{a_j} : 1 \leq i, j \leq n\}$ is linearly independent. If

$$\sum_{i,j=1}^n \lambda_{ij} L_{a_i} R_{a_j} = 0,$$

then $\sum_{i=1}^n L_{a_i} R_{c_i} = 0$, where $c_i = \sum_{j=1}^n \lambda_{ij} R_{a_j}$. Since the a_i 's are linearly independent, Lemma 30.8 implies that $c_i = 0$ for all $i \in \{1, \dots, n\}$, a contradiction since the a_j 's are linearly independent. Hence $\dim_k M(A) \geq n^2 = \dim \text{End}_K(A)$. \square

Definition 30.10. Let R be a unitary ring. An automorphism $f \in \text{Aut}(R)$ is **inner** if there exists an invertible $r \in R$ such that $f(x) = r x r^{-1}$ for all $x \in R$.

For example, $\mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$, is not inner.

Example 30.11. Let $\lambda \in k \setminus \{0\}$ and $R = k[X]$. Then

$$k[X] \rightarrow k[X], \quad f(X) \mapsto f(X + \lambda),$$

is not inner.

Example 30.12. Let R be a ring. Then $R \times R \rightarrow R \times R, (x, y) \mapsto (y, x)$, is not inner.

Theorem 30.13 (Skolem–Noether). *If A is a finite-dimensional central simple algebra, every automorphism of A is inner.*

Proof. Let $f \in \text{Aut}(A)$. By Lemma 30.9, $f = \sum_{i=1}^n L_{a_i} R_{b_i}$. Without loss of generality, we may assume that $a_1 \neq 0$ and that $\{b_1, \dots, b_n\}$ is linearly independent. Since f is a homomorphism, $L_{f(x)}f = fL_x$ for all $x \in A$. Then

$$0 = \sum_{i=1}^n L_{f(x)a_i - a_i x} R_{b_i}.$$

By Lemma 30.8, $f(x)a_1 - a_1 x = 0$ for all $x \in A$. We claim that a_1 is invertible. Since $a_1 \neq 0$ and A is simple, the ideal of A generated by a_1 is A . Write $1 = \sum_{j=1}^m u_j a_1 v_j$. Thus a_1 is invertible, as

$$\left(\sum_{j=1}^m u_j f(v_j) \right) a_1 = a_1 \left(\sum_{j=1}^m f^{-1}(u_j) v_j \right) = 1. \quad \square$$

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 [14, (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 15.7); the proof of this result appears for example in [18, 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 [18, 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 [15].

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 does not always hold. The double centralizer theorems give conditions under which one can conclude that equality occurs; see [2, Chapter 4].

Amitsur–Levitzki theorem

The theorem states that if A is a commutative algebra, then the matrix algebra $M_n(K)$ satisfies the identity

$$s_{2n}(a_1, \dots, a_{2n}) = 0,$$

where

$$s_n(X_1, \dots, X_n) = \sum_{\sigma \in \mathbb{S}_n} \text{sign}(\sigma) X_{\sigma(1)} \cdots X_{\sigma(n)}.$$

See [2, Theorem 6.39] for the beautiful proof found by Rosset.

Non-commutative Hilbert's basis theorem

There exists a non-commutative version of the celebrated Hilbert's basis theorem. It is based on the theory of Ore's extensions (also known as *skew polynomial rings*). The theorem appears in [11, I.8.3]; see [11, I.7] for the basic theory of Ore's extensions.

Bi-ordered or left-ordered groups

Basic notions about ordered groups appear in the book of Passman [18], where the motivation is based on algebraic properties of group algebras.

Golod-Shafarevich theorem

This is an important theorem of non-commutative algebra with several interesting applications, for example, in group theory. A quick proof (and some applications) can be found in the book [8] of Herstein.

The Brauer group

The Brauer group is a helpful tool to classify division algebras over fields. It can also be defined in terms of Galois cohomology. See [3] for the definition and some properties.

The Weyl algebra

The Weyl algebra is the quotient of the free algebra on two generators X and Y by the ideal generated by the element $YX - XY - 1$. The Weyl algebra is a simple ring that is not a matrix ring over a division ring. It is also a non-commutative domain and an Ore extension. See [14] for more information. In 1968, Dixmier conjectured that any endomorphism of a Weyl algebra is an automorphism; the conjecture is still open.

Gardam's theorem

Let K be a field and G be a torsion-free group. What do the units of $K[G]$ look like? The conjecture is that units of $K[G]$ are of the form λg for some $0 \neq \lambda \in K$ and $g \in G$. Recently, Gardam [4] found a counterexample in the case that K is the field of two elements. The problem is still open for fields of characteristic zero.

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. B. Farb and R. K. Dennis. *Noncommutative algebra*, volume 144 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.
4. G. Gardam. A counterexample to the unit conjecture for group rings. *Ann. of Math. (2)*, 194(3):967–979, 2021.
5. R. W. Gilmer, Jr. If $R[X]$ is Noetherian, R contains an identity. *Amer. Math. Monthly*, 74:700, 1967.
6. M. Henriksen. A simple characterization of commutative rings without maximal ideals. *Amer. Math. Monthly*, 82:502–505, 1975.
7. I. N. Herstein. A counterexample in Noetherian rings. *Proc. Nat. Acad. Sci. U.S.A.*, 54:1036–1037, 1965.
8. 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.
9. T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.
10. N. Jacobson. *Structure of rings*. American Mathematical Society Colloquium Publications, Vol. 37. American Mathematical Society, Providence, R.I., revised edition, 1964.
11. C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
12. G. Köthe. Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist. *Math. Z.*, 32(1):161–186, 1930.
13. J. Krempa. Logical connections between some open problems concerning nil rings. *Fund. Math.*, 76(2):121–130, 1972.
14. T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.
15. T. Y. Lam. *Exercises in modules and rings*. Problem Books in Mathematics. Springer, New York, 2007.
16. 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.
17. P. P. Nielsen. Simplifying Smoktunowicz’s extraordinary example. *Comm. Algebra*, 41(11):4339–4350, 2013.
18. D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.
19. W. R. Scott. *Group theory*. Dover Publications, Inc., New York, second edition, 1987.

20. A. Smoktunowicz. Polynomial rings over nil rings need not be nil. *J. Algebra*, 233(2):427–436, 2000.
21. A. Smoktunowicz. On some results related to Köthe’s conjecture. *Serdica Math. J.*, 27(2):159–170, 2001.
22. A. Smoktunowicz. Some results in noncommutative ring theory. In *International Congress of Mathematicians. Vol. II*, pages 259–269. Eur. Math. Soc., Zürich, 2006.
23. D. E. Taylor. Some classical theorems on division rings. *Enseign. Math. (2)*, 20:293–298, 1974.
24. M. Teleuca. Zsigmondy’s theorem and its applications in contest problems. *Internat. J. Math. Ed. Sci. Tech.*, 44(3):443–451, 2013.
25. K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.

Index

- Akizuki's theorem, 40
- Algebra, 1
 - algebraic, 2
 - commutative, 1
 - dimension, 1
 - ideal, 2
 - of multipliers, 82
 - semisimple, 5
 - simple, 15
- Algebraic element, 2
- Amitsur's theorem, 32
- Andrunakevic–Rjabuhin's theorem, 57
- Artin–Wedderburn theorem, 9
- Artin–Wedderburn's theorem, 51
- Automorfism
 - inner, 84
- Brauer's problem, 12
- Burnside's theorem, 65
- Characteristic of a ring, 28
- Chinese Remainder Theorem, 17
- Composition series
 - equivalence, 38
- Connel's theorem, 50
- Division algebra, 7
- Domain, 49
- Element
 - left quasi-regular, 22
 - quasi-regular, 22
- Feit–Thompson's theorem, 65
- Fermat's last theorem for finite rings, 76
- Formanek's theorem, 66, 73
- Frobenius
 - theorem, 77
- Gilmer's theorem, 35
- Group
 - locally finite, 64
 - solvable, 65
 - torsion, 64
- Henriksen's theorem, 28
- Herstein's theorem, 65
- Homomorphism
 - of algebras, 2
- Hopkins–Levitski theorem, 54
- Ideal
 - maximal, 18
 - nil, 21
 - nilpotent, 21
 - prime, 51
 - primitive, 19
 - reduced, 57
 - regular, 18
- Idempotent, 42
- Jacobson conjecture, 33
- Jacobson radical, 21
- Jacobson's commutativity theorem, 79
- Jacobson's density theorem, 46
- Jacobson–Herstein conjecture, 33
- Jordan–Hölder theorem, 38
- Köthe conjecture, 34
- Left ideal
 - maximal, 18
 - nil, 21
 - nilpotent, 21

- regular, 18
- Maschke's theorem, 63
- Minimal element, 36
- Minimal left ideal, 18
- Module, 3
 - artinian, 36
 - composition series, 37
 - faithful, 19
 - homomorphism, 3
 - length, 39
 - noetherian, 36
 - of finite length, 39
 - semisimple, 3
 - simple, 3
- Mollien's theorem, 10
- Prüfer's group, 64
- Rickart's theorem, 59
- Ring
 - boolean, 79
 - left artinian, 37
 - local, 31, 41
 - nil, 29
 - prime, 49
 - primitive, 19
 - radical, 27
 - reduced, 57
 - semilocal, 43
 - semiprime, 45
 - semisimple, 53
 - simple, 17
 - Von Neumann regular, 43
- Schur's lemma, 3
- Skolem–Noether theorem, 84
- Subdirect product, 44
- Trivial idempotent, 42
- Wedderburn's little theorem, 74
- Wedderburn's theorem, 16, 50
- Zsigmondy's theorem, 76

