

Associative algebra

Leandro Vendramin

ABSTRACT. The notes correspond to the master course **Associative Algebra** of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences.

CONTENTS

Part 1.

Introduction	3
§ 1. Semisimple algebras	4
§ 2. The Artin–Wedderburn theorem	10
§ 3. Simple algebras	11
§ 4. Wedderburn’s theorem	12
§ 5. Group algebras	12
§ 6. Which algebras are group algebras?	14
§ 7. The isomorphism problem for group algebras	14
§ 8. Primitive rings	15
§ 9. Jacobson’s radical	19
§ 10. Radical rings	23
§ 11. Henriksen’s theorem	23
§ 12. Amitsur’s theorem	28
§ 13. Jacobson’s conjecture	29
§ 14. Köthe’s conjecture	29
§ 15. Gilmer’s theorem	30
§ 16. Artinian modules	31
§ 17. The Jordan–Hölder theorem	32
§ 18. Akizuki’s theorem	34
§ 19. Semiprimitive rings	35
§ 20. Jacobson’s density theorem	36
§ 21. Prime rings	38
§ 22. Wedderburn’s theorem	39
§ 23. The Artin–Wedderburn theorem	40
§ 24. Semisimple modules	42
§ 25. The Hopkins–Levitzki theorem	43
§ 26. Local rings	44
§ 27. Gustafson’s theorem	46
§ 28. Schur’s theorem	49

DEPARTMENT OF MATHEMATICS AND DATA SCIENCE, VRIJE UNIVERSITEIT BRUSSEL, PLEINLAAN 2,
1050 BRUSSEL

E-mail address: `Leandro.Vendramin@vub.be`.

§ 29.	Rickart's theorem	50
§ 30.	Maschke's theorem	52
§ 31.	Herstein's theorem	53
§ 32.	Formanek's theorem, I	55
§ 33.	Tensor products	56
§ 34.	Formanek's theorem, II	60
§ 35.	Wedderburn's little theorem	60
§ 36.	Zsigmondy's theorem	62
§ 37.	Fermat's last theorem in finite rings	63
§ 38.	Frobenius's theorem	63
§ 39.	Jacobson's commutativity theorem	65
Part 2.		
§ 40.	Project: An analytic proof of Rickart's theorem	68
§ 41.	Project: Hurewicz' theorem	71
§ 42.	Project: Dedekind-finite rings	73
§ 43.	Project: The Skolem–Noether theorem	75
§ 44.	Project: The Brauer group	78
§ 45.	Project: The Andrunakevic–Rjabuhin theorem	82
§ 46.	Project: Kolchin's theorem	84
§ 47.	Project: Passman's theorem	90
§ 48.	Project: Gardam's theorem	96
§ 49.	Project: When a group algebra is prime?	99
§ 50.	Project: When a group algebra is local?	101
§ 51.	Project: When a group algebra is reduced?	104
§ 52.	Project: Bi-ordered groups	105
§ 53.	Project: Locally indicable groups	109
§ 54.	Project: Left-ordered groups	112
§ 55.	Project: Unique product groups	114
§ 56.	Project: The braid group	118
Part 3.		
	Some other topics for final projects	120
	References	121
	Index	123

Introduction

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 reader should have a solid understanding of an undergraduate-level abstract algebra course. For reference, you can review my notes for the VUB courses: **Group Theory** and **Ring and Module Theory**.

The content presented here draws heavily from [7], [16], and [33]. Additionally, I have followed the outstanding **blog** on abstract algebra by Yaghoub Sharif.

The notes include many exercises, some with full detailed solutions. Mandatory exercises have a **green background**, while optional ones (bonus exercises) have a **yellow background**.

The notes also include some additional comments. While these are entirely optional, I hope they offer further insight. They are highlighted with a **pink background**.

The notes include Magma code, which we use to verify examples and offer alternative solutions to certain exercises. Magma [6] is a powerful software tool designed for working with algebraic structures. There is a free **online** version of Magma available.

Thanks go to Ilaria Colazzo, Rune De Bode, Luca Descheemaeker, Mathijs Dingemans, Silvia Properzi, Lukas Simons.

This version was compiled on November 27, 2025 at 11:22.

§ 1. Semisimple algebras

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

1.1. DEFINITION. An **algebra** (over the field K) is a vector space (over K) with an associative multiplication $A \times A \rightarrow A$ such that

$$a(\lambda b + \mu c) = \lambda(ab) + \mu(ac) \quad \text{and} \quad (\lambda a + \mu b)c = \lambda(ac) + \mu(bc)$$

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 $1_K \rightarrow 1_A$.

1.2. DEFINITION. 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.

1.3. EXAMPLE. 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 .

1.4. EXAMPLE. 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 algebras over K .

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

1.6. EXAMPLE. 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 $(fg)(x) = f(x)g(x)$.

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

1.8. EXAMPLE. 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.

1.9. DEFINITION. 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} .

1.10. EXERCISE. 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 .

1.11. EXERCISE. 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 $\varphi|_G = f$.

1.12. DEFINITION. 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 .

1.13. DEFINITION. 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.

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

PROOF. Let A be an algebra with $\dim A = n$ and let $a \in A$. Since $\{1, a, a^2, \dots, a^n\}$ is linearly dependent (because if it does not have repetitions, has $n + 1$ elements), there exists a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$. \square

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

Similarly, one defines **submodules** of A -modules.

1.16. DEFINITION. 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.

1.17. EXAMPLE. If M is a module over a finite-dimensional K -algebra A , one defines $\text{End}_A(M)$ as the set of A -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 $m \in M$.

1.18. EXAMPLE. An algebra A is a module over A with left multiplication, that is

$$a \cdot b = ab, \quad a, b \in A.$$

This module is the (left) **regular representation** of A and it will be denoted by ${}_A A$.

1.19. DEFINITION. 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 .

1.20. DEFINITION. 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.

1.21. LEMMA (Schur). *Let A be an algebra. If S and T are simple modules and $f: S \rightarrow T$ is a non-zero A -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

1.22. PROPOSITION. *If A is a finite-dimensional algebra and S is a simple A -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

$$\dim S = \dim(A/\ker \varphi) \leq \dim A. \quad \square$$

1.23. PROPOSITION. *Let A be a finite-dimensional algebra and M a finite-dimensional A -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

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

PROOF. Assume that $M = S_1 + \cdots + S_k$, where each S_i is a simple submodule. If $\pi: M \rightarrow M/N$ 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.

We now prove that N is semisimple. By assumption, there exists a submodule T of M 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

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

1.26. PROPOSITION. *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

1.27. THEOREM. *Let A be a finite-dimensional semisimple algebra. Assume that the regular representation can be decomposed as $A = \bigoplus_{i=1}^k S_i$ 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, $S_i \not\simeq S_j$ whenever $i \neq j$.

1.28. EXERCISE. 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 .

1.29. PROPOSITION. 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.

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

$$(1.1) \quad \text{Hom}_A(M \oplus N, X) \simeq \text{Hom}_A(M, X) \times \text{Hom}_A(N, X).$$

1.31. THEOREM. 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 a simple module and $S_i \not\cong S_j$ 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

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

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

An algebra A is commutative if and only if $A = A^{\text{op}}$.

1.33. LEMMA. 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

$$A^{\text{op}} \rightarrow \text{End}_A(A), \quad a \mapsto \rho_a,$$

is bijective and it is an algebra homomorphism, as

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

1.34. LEMMA. 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

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

1.35. LEMMA. 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

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

1.36. EXERCISE. Prove Lemma 1.35.

§ 2. The Artin–Wedderburn theorem

2.1. EXERCISE. Let M , N , and X be A -modules. Prove that

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

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

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

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

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

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

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

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

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. □

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

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

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

PROOF. By Wedderburn's theorem,

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

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 invertible, hence 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,

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

□

We conclude this section with a nice application of semisimplicity.

2.4. EXERCISE. Prove that there exists a homomorphism $M_n(\mathbb{R}) \rightarrow M_m(\mathbb{R})$ of \mathbb{R} -algebras if and only if n divides m .

§ 3. Simple algebras

3.1. DEFINITION. An algebra A is said to be **simple** if $A \neq \{0\}$ and $\{0\}$ and A are the only ideals of A .

3.2. PROPOSITION. *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. □

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 .

3.3. PROPOSITION. *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

§ 4. Wedderburn's theorem

4.1. THEOREM (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 a division algebra D .*

PROOF. Since A is simple, it follows that A is semisimple. The Artin–Wedderburn theorem implies that $A \simeq \prod_{i=1}^k M_{n_i}(D_i)$ for some n_1, \dots, n_k and 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 (Proposition 3.2). Thus $k = 1$ and hence $A \simeq M_n(D)$ for some $n \in \mathbb{Z}_{>0}$ and some division algebra D . \square

§ 5. 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 $\sum_{g \in G} \lambda_g g$.

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

5.2. EXERCISE. Let $n \geq 2$ and $G = C_n$ the (multiplicative) cyclic group of order n . Prove that $K[G] \simeq K[X]/(X^n - 1)$.

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

5.4. EXERCISE. 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 $\text{supp}(\alpha g) = (\text{supp } \alpha)g$.

5.5. EXERCISE. 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 $K[G]$.

5.6. EXERCISE. 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.

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

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

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

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

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,

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

5.9. THEOREM. *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

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

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

§ 6. Which algebras are group algebras?

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

6.2. EXAMPLE. Let $G = S_3$. Then G has three simple modules and

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

6.3. OPEN PROBLEM (Brauer). Which algebras are group algebras?

This question might be impossible to answer, but it is extremely interesting. Examples 6.1 and 6.2 show that \mathbb{C}^4 and $\mathbb{C}^2 \times M_2(\mathbb{C})$ are complex group algebras.

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

§ 7. The isomorphism problem for group algebras

Recall that if R is a unitary commutative ring and G is a group, then one defines the group ring $R[G]$ (see Appendix 41). Note that $R[G]$ is a left R -module with

$$\lambda \left(\sum_{g \in G} \lambda_g g \right) = \sum_{g \in G} (\lambda \lambda_g) g.$$

In this section, we will briefly discuss the following natural problem:

7.1. QUESTION (The isomorphism problem). Let R be a ring and G and H be groups. Assume that $R[G] \simeq R[H]$ (as R -algebras). Does $G \simeq H$?

For general information on Question 7.1 we refer to the survey paper [29].

7.2. EXERCISE. Prove that if G and H are isomorphic groups, then $K[G] \simeq K[H]$.

7.3. EXERCISE. Let G and H be groups. Prove that if $\mathbb{Z}[G] \simeq \mathbb{Z}[H]$, then $R[G] \simeq R[H]$ for any commutative ring R .

The previous exercise suggest the importance of the following instance of Question 7.1:

7.4. QUESTION. Let G and H be groups. Does $\mathbb{Z}[G] \simeq \mathbb{Z}[H]$ imply $G \simeq H$?

Although there are several cases where the isomorphism problem has an affirmative answer (e.g. abelian groups, metabelian groups, nilpotent groups, nilpotent-by-abelian groups, simple groups, abelian-by-nilpotent groups), it is false in general. In 2001 Hertweck found a counterexample of order $2^{21}97^{28}$, see [17].

7.5. QUESTION (The modular isomorphism problem). Let p be a prime number. Let G and H be finite p -groups and let K be a field of characteristic p . Does $K[G] \simeq K[H]$ imply $G \simeq H$?

Question 7.5 has an affirmative answer in several cases. However, this is not true in general. This question was recently answered by García, Margolis and del Río [10]. They found two non-isomorphic groups G and H both of order 512 such that $K[G] \simeq K[H]$ for all field K of characteristic two.

§ 8. 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.

8.1. EXAMPLE. \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 .

8.2. EXAMPLE. If I and J are both ideals of a ring 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 .

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

8.4. EXAMPLE. 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 $RaR + Ra + aR + \mathbb{Z}a$.

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

8.5. BONUS EXERCISE. 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.

8.6. DEFINITION. 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

$$1 \in R^2 = \{r_1 r_2 : r_1, r_2 \in R\}.$$

8.7. EXAMPLE. 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

$$(8.1) \quad E_{ij} A E_{kl} = a_{jk} E_{il}$$

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

8.8. EXAMPLE. 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 $M = R \cdot M$.

8.9. EXERCISE. 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 $Z(R)$.

8.10. DEFINITION. 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.

8.11. LEMMA. 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

8.12. EXAMPLE. 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 $fv = f(v)$, $f \in R$. $v \in V$.

8.13. EXAMPLE. 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.

8.14. DEFINITION. A left ideal L of a ring R is said to be **minimal** if $L \neq \{0\}$ and L does not properly contain non-zero left ideals of R .

Similarly one defines right minimal ideals and minimal ideals.

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

8.16. EXAMPLE. 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.

8.17. DEFINITION. 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.

8.18. DEFINITION. A left (resp. right) ideal I of R is said to be **maximal** if $I \neq R$ and I is not properly contained in a proper 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.

8.19. PROPOSITION. *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 8.11. 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).

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 $R \cdot (R/I) \neq \{0_{R/I}\}$. Assume that $R \cdot (R/I) = \{0_{R/I}\}$ and let $r \in R$. The regularity of I implies that there exists $e \in R$ such that $r - re \in I$. Hence $r \in I$, as

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

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

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

8.20. EXAMPLE. $\text{Ann}_{\mathbb{Z}}(\mathbb{Z}/n) = n\mathbb{Z}$.

8.21. EXERCISE. 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 .

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

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

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

8.25. DEFINITION. 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.

8.26. EXERCISE. If R is a simple unitary ring, then R is primitive.

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

8.28. EXAMPLE. The ring \mathbb{Z} is not primitive.

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

As we work with left modules, our definition of primitive rings refers to **left primitive rings**. Of course, one can also define right primitive rings. As Bergman showed, there exist rings that are right primitive but not left primitive; see [2, 3].

8.30. EXERCISE. 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.

8.31. EXAMPLE. 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 $R/P_i \simeq R_i$.

8.32. LEMMA. 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 8.19, 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 8.19, R/I is a simple R -module. Then

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

is a primitive ideal. □

8.33. EXERCISE. Maximal ideals of unitary rings are primitive.

8.34. EXERCISE. Prove that every primitive ideal of a commutative ring is maximal.

8.35. BONUS EXERCISE. Prove that $M_n(R)$ is primitive if and only if R is primitive.

§ 9. Jacobson's radical

9.1. DEFINITION. 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 $\{y_1 \dots y_n : y_j \in I\}$.

9.2. DEFINITION. 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 $x_1, \dots, x_n \in I$.

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

9.4. DEFINITION. 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 $x \in I$.

9.5. EXAMPLE. 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 elements. 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 $x_{k+1}^k \neq 0$.

9.6. PROPOSITION. Let R be a ring. Then every nil left ideal is contained in $J(R)$.

PROOF. Assume that there is a nil left 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 $m \in M$. Since M is simple, $R \cdot n = M$ and hence there exists $r \in R$ such that $r \cdot n = m$. Since

$$(rx) \cdot m = r \cdot (x \cdot m) = r \cdot n = m,$$

it follows that $(rx)^k \cdot m = m$ for all $k \geq 1$, a contradiction since $rx \in I$ is a nilpotent element. \square

Similarly, one proves that every nil right ideal is contained in the Jacobson radical.

9.7. DEFINITION. 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 the **Jacobson circle operation**

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

is an associative operation with neutral element 0.

9.8. EXAMPLE. Let $R = \mathbb{Z}/3 = \{0, 1, 2\}$ be the ring of integers modulo 3. The Jacobson circle operation of R is shown in Table 1.

TABLE 1. The table of a radical ring over $\mathbb{Z}/3$.

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

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

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

9.9. EXAMPLE. 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 it also right quasi-regular?

9.10. DEFINITION. 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.

9.11. LEMMA. *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

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

For unitary rings, it is known that every element which is not a unit is contained in a maximal ideal. The proof of this fact relies on Zorn's lemma. More generally, for arbitrary rings, the following result holds.

9.12. LEMMA. *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. Since $T \in \mathcal{S}$, $\mathcal{S} \neq \emptyset$. 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 $x \notin K$). Then 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 8.19. Since $x \cdot (x + M) \neq M$ (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

9.13. EXERCISE. Let R be a ring and $x \in R$ be an element that is not left quasi-regular. Prove that $x \notin J(R)$.

9.14. THEOREM. *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, we prove (3) \implies (1). Let $x \in J(R)$ and I be the left ideal of R generated by x . Since $I \subseteq J(R)$ and every element of $J(R)$ is left quasi-regular (see Exercise 9.13), I is left quasi-regular. By Lemma 9.11, I is quasi-regular. \square

The theorem implies the following corollary.

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

PROOF. By Exercise 9.13, $J(R)$ is left quasi-regular. By Lemma 9.11, $J(R)$ is quasi-regular. Let I be a left ideal of R that is quasi-regular. Let $x \in I$ and J be the left ideal of R generated by x . Since $J \subseteq I$, J is quasi-regular. By Theorem 9.14, $x \in J(R)$. \square

The following exercise uses Zorn's lemma and will be used in the proof of Theorem 9.17.

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

9.17. THEOREM. 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 9.11, 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 8.17). 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 8.19,

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

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 $r \in \text{Ann}_R(R/I)$,

$$re + I = r(e + I) \subseteq I,$$

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

9.18. EXAMPLE. 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.

9.19. PROPOSITION. 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.

9.20. LEMMA. 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

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

9.21. PROPOSITION. *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 9.20. \square

§ 10. Radical rings

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

10.2. EXAMPLE. If R is a ring, then $J(R)$ is a radical ring, by Proposition 9.21.

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

There are several characterizations of radical rings.

10.4. THEOREM. *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.

10.5. EXERCISE. Prove Theorem 10.4.

10.6. EXAMPLE. Let

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

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

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

§ 11. Henriksen's theorem

There are (non-unitary) rings with no maximal ideals. An easy example is given in the following exercise:

11.1. EXERCISE.

- 1) Prove that the additive group of rational numbers is an abelian group with no maximal subgroups.
- 2) Prove that the additive group \mathbb{Q} of rationals with zero multiplication (that is, $xy = 0$ for all $x, y \in \mathbb{Q}$) is a ring with no maximal ideals.

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**.

11.2. EXERCISE. Let R be a non-zero ring 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. We begin with some exercises.

11.3. EXERCISE. 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 .

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

The following result appeared in [14].

11.5. THEOREM (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 11.4. 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. Moreover, by Exercise 11.2, R/I has characteristic p , as $pR \subseteq I$. 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 surjective ring homomorphism. The composition $f = \gamma\pi: R \rightarrow R/I \rightarrow A$ is a ring homomorphism. By Exercise 11.3, $\ker f$ 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 11.3, 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 $\pi: R \rightarrow R/M$ 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 $\mathbb{R}[X]$.

11.6. EXERCISE. 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.

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

11.8. EXERCISE. Prove that every nil ring is radical.

11.9. EXERCISE. 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.

11.10. THEOREM. 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

$$(11.1) \quad (x + J(R)) \cdot m = x \cdot m, \quad x \in R, m \in M.$$

Let us prove first that (11.1) is well-defined: If $r, s \in R$ are such that $r + J(R) = s + J(R)$, then $r - s \in J(R)$. Since $J(R)$ is the intersection of the annihilators of simple R -modules (see Definition 9.1) and M is a simple R -module, $(r - s) \cdot M = \{0\}$. Thus $(r - s) \cdot m = 0$ for all $m \in M$. Hence $r \cdot m = s \cdot m$ for all $m \in M$.

We now prove that M is a simple $R/J(R)$ -module. In fact, if N is a submodule of the $R/J(R)$ -module M , then

$$(r + J(R)) \cdot N \subseteq N$$

for all $r \in R$. Thus $r \cdot N \subseteq N$ for all $r \in R$. Thus N is a submodule of the R -module M . Since M is simple, either $N = \{0\}$ or $N = M$.

Finally, if $r + J(R) \in J(R/J(R))$, then $r \cdot M = (r + J(R)) \cdot M = \{0\}$. Then $r \in J(R)$, as r annihilates any simple module over R . \square

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

PROOF. For clarity, we will prove the result for $n = 3$. The extension to general n is straightforward and left as an exercise for the reader.

We first prove that $J(M_3(R)) \subseteq M_3(J(R))$. 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^3 is a simple $M_3(R)$ -module with the usual multiplication. Let $x = (x_{ij}) \in J(M_3(R))$ and $m_1, m_2, m_3 \in M$. Then

$$x \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix} = 0.$$

In particular, $x_{ij} \in \text{Ann}_R(M)$ for all $i, j \in \{1, 2, 3\}$. Hence $x \in M_3(J)$.

We now prove that $M_3(J) \subseteq J(M_3(R))$. Let

$$J_2 = \begin{pmatrix} 0 & J & 0 \\ 0 & J & 0 \\ 0 & J & 0 \end{pmatrix} \quad \text{and} \quad x = \begin{pmatrix} 0 & x_1 & 0 \\ 0 & x_2 & 0 \\ 0 & x_3 & 0 \end{pmatrix} \in J_2.$$

Since x_2 is quasi-regular, there exists $y_2 \in R$ such that $x_2 + y_2 + x_2 y_2 = 0$. For

$$y = \begin{pmatrix} 0 & 0 & 0 \\ 0 & y_2 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

let

$$u = x + y + xy = \begin{pmatrix} 0 & x_1 + x_1y_2 & 0 \\ 0 & x_2 + y_2 + x_2y_2 & 0 \\ 0 & x_3 + x_3y_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & x_1 + x_1y_2 & 0 \\ 0 & 0 & 0 \\ 0 & x_3 + x_3y_2 & 0 \end{pmatrix}.$$

Since $u^2 = 0$, x is right quasi-regular, as

$$x + (y - u - yu) + x(y - u - uy) = 0,$$

and therefore J_2 is right quasi-regular. Similarly one proves that both J_1 and J_3 are right quasi-regular. Thus $J_i \subseteq J(M_3(R))$ for all $i \in \{1, 2, 3\}$. In conclusion,

$$J_1 + J_2 + J_3 \subseteq J(M_3(R))$$

and therefore $M_3(J) \subseteq J(M_3(R))$. □

11.12. EXERCISE. Let R be a ring and $n \in \mathbb{Z}_{>0}$. Prove that $J(M_n(R)) = M_n(J(R))$.

11.13. EXERCISE. Let R be a unitary ring. Then

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

11.14. EXERCISE. 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.

11.15. BONUS EXERCISE. 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.

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

11.17. EXAMPLE. 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.

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

11.19. PROPOSITION. 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

For algebras, the Jacobson radical of an algebra can be defined as the intersection of the left ideals (of the algebra) that are maximal and regular. The previous proposition then implies that the Jacobson radical of an algebra coincides with the Jacobson radical of the underlying ring.

§ 12. Amitsur's theorem

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

12.1. LEMMA. *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 11.14, it follows that $x^r = 0$. \square

An application:

12.2. PROPOSITION. *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 9.6 now implies that $J(A)$ is the largest nil ideal of A . \square

12.3. THEOREM (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 12.2.

Assume that K is infinite and let $a \in J(A)$. Exercise 11.14 implies that every element of the form $1 - \lambda^{-1}a$, $\lambda \in K \setminus \{0\}$, is invertible. Thus

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

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

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

it follows that $|S| = |K \setminus \{0\}| = |K| > \dim_K A$. Then S is a linearly dependent set, 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

$$(12.1) \quad \sum_{i=1}^n \beta_i (a - \lambda_i)^{-1} = 0.$$

Multiplying (12.1) 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 12.1. \square

Amitsur's theorem implies the following result.

12.4. COROLLARY. *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 .*

§ 13. 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**.

13.1. OPEN PROBLEM (Jacobson). Let R be a noetherian ring. Is then

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

Open problem 13.1 was originally formulated by Jacobson in 1956 [19] for one-sided noetherian rings. In 1965 Herstein [15] found a counterexample in the case of one-sided noetherian rings and reformulated the conjecture as it appears here.

13.2. EXERCISE (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.

§ 14. Köthe's conjecture

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

14.1. OPEN PROBLEM (Köthe). Let R be a ring. Is the sum of two arbitrary nil left ideals of R nil?

Open problem 14.1 is the well-known **Köthe's conjecture**. The conjecture was first formulated in 1930, see [23]. It is known to be true in several cases. In full generality, the problem is still open. In [25] 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 [37] Smoktunowicz found a counterexample to Amitsur's conjecture. This counterexample suggests that Köthe's conjecture might be false. A simplification of Smoktunowicz' example appears in [32]. See [38, 39] for more information on Köthe's conjecture and related topics.

§ 15. Gilmer's theorem

Hilbert's theorem states that if R is a noetherian commutative unitary ring, then $R[X]$ is noetherian. Following [13], we now present the converse of Hilbert's theorem.

15.1. THEOREM (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

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

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

$$(15.1) \quad \text{for every } a \in R \text{ there exists } r \in R \text{ such that } a = ra.$$

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 (15.1). 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 $i \in \{1, \dots, n - 1\}$,

$$ra_i = r_1 a_i + r_2 a_i - r_1 r_2 a_i = a_i + r_2 a_i - r_2 r_1 a_i = a_i + r_2 a_i - r_2 a_i = a_i.$$

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

$$b = t_1 a_1 + \dots + t_n a_n + m_1 a_1 + \dots + m_n a_n$$

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

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

§ 16. Artinian modules

16.1. DEFINITION. 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 $Y \subsetneq A$.

16.2. PROPOSITION. *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 we have the submodules

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

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 $k \in \mathbb{Z}_{\geq 0}$.

16.3. EXERCISE. Let M be a module. The following statements are equivalent:

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

16.4. EXERCISE. Prove that a ring R is left noetherian if every sequence of left ideals $I_1 \subseteq I_2 \subseteq \dots$ stabilizes.

16.5. EXERCISE. 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).

16.6. DEFINITION. A ring R is **left artinian** if the module ${}_R R$ is artinian.

Similarly one defines right artinian rings.

16.7. EXAMPLE. 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.

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

16.9. THEOREM. *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. □

16.10. COROLLARY. *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 9.6, L is contained in $J(R)$. Thus L is nilpotent, as $J(R)$ is nilpotent by Theorem 16.9. □

§ 17. The Jordan–Hölder theorem

17.1. DEFINITION. 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.

17.2. THEOREM. *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 16.5.

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 16.2). 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

17.3. DEFINITION. Let M be a module. We say that the composition series

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

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

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

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

PROOF. Let M be a module and

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

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

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

Since V_1 has a composition series, V_1 is artinian and noetherian by Theorem 17.2. The submodule $U = V_1 \cap W_1$ is also artinian and noetherian and hence, by Theorem 17.2, admits a composition series

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

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

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

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

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

17.6. DEFINITION. 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.

17.7. EXERCISE. 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 $\ell(M) = \ell(N) + \ell(Q)$.

17.8. EXERCISE. If A and B are finite-length submodules of M , then

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

§ 18. Akizuki's theorem

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

18.1. EXERCISE. 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 $y \in I$.

18.2. EXERCISE. Let R be an unitary commutative artinian ring.

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

18.3. THEOREM (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 18.1, $\dim_K I = \infty$. 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 18.1). This is a contradiction, because J is an ideal of R such that $J \subsetneq I$. \square

§ 19. Semiprimitive rings

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

In Lecture 4 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 $J(R) = \{0\}$.

19.2. EXAMPLE. If $R = \prod_{i \in I} R_i$ is a direct product of semiprimitive rings, then R is semiprimitive. In fact,

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

19.3. EXAMPLE. \mathbb{Z} is semiprimitive, as $J(\mathbb{Z}) = \bigcap_p p\mathbb{Z} = \{0\}$.

19.4. EXAMPLE. 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 $J(R) = \bigcap_{a \leq c \leq b} U_c = \{0\}$.

We proved in Theorem 11.10 (Lecture 8) that $R/J(R)$ is semiprimitive.

19.5. DEFINITION. 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 $f: R \rightarrow \prod_{i \in I} R_i$.
- 2) For each j , the composition $\pi_j f: R \rightarrow R_j$ is surjective.

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

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

19.7. EXAMPLE. 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.

19.8. THEOREM. *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 . This collection is non-empty, as R is non-zero and semiprimitive. Each R/P_j is primitive and

$$\{0\} = J(R) = \bigcap_{i \in I} P_i.$$

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 $x \in \bigcap_{i \in I} P_i$, then $\varphi(x) = 0$ and thus $x = 0$. Hence $J(R) \subseteq \bigcap_{i \in I} P_i = \{0\}$. \square

19.9. EXAMPLE. The ring $C[a, b]$ of Example 19.4 is isomorphic to a subdirect product of the fields $C[a, b]/U_c \simeq \mathbb{R}$.

§ 20. 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. For that reason, they are often called **vector spaces over division rings**.

20.1. DEFINITION. 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 $\{x_1, \dots, x_n\} \subseteq V$ and every (not necessarily linearly independent) subset $\{y_1, \dots, y_n\} \subseteq V$ there exists $f \in R$ such that $f(x_j) = y_j$ for all $j \in \{1, \dots, n\}$.

20.2. PROPOSITION. *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 $\{x_1, \dots, x_n\}$ 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 $f(x_j) = g(x_j)$ for all $j \in \{1, \dots, n\}$. Hence $g = f \in R$. \square

20.3. THEOREM (Jacobson). *A unitary ring is primitive if and only if it is isomorphic to a dense ring on a vector space over a division ring.*

PROOF. Let R be a unitary ring. 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 $v = f(w) \in W$.

Assume now that R is a primitive ring. 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 $\gamma: R \rightarrow \text{End}_D(V)$, $r \mapsto \gamma_r$, 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 $v \in V$.

To prove that R is dense we proceed by induction on n . Assume first that $n = 1$. Since V is simple, $Rx_1 = V$ since $x_1 \neq 0$. Then there exists $r \in R$ such that $rx_1 = y_1$.

Let $n \geq 1$ and assume that the theorem holds for all sets of size $\leq n - 1$. Let $\{x_1, \dots, x_n\}$ be a linearly independent subset of V and $\{y_1, \dots, y_n\}$ be a subset of V .

CLAIM. There exist $\lambda_1, \dots, \lambda_n \in R$ such that $\lambda_i x_i \neq 0$ for all $i \in \{1, \dots, n\}$ and $\lambda_i x_j = 0$ for all $i, j \in \{1, \dots, n\}$ with $i \neq j$.

We first note that the claim implies the theorem. As the theorem holds for $n = 1$, for each $i \in \{1, \dots, n\}$ there exists $r_i \in R$ such that $r_i \lambda_i x_i = y_i$. Let $r = r_1 \lambda_1 + \dots + r_n \lambda_n \in R$. Then

$$rx_i = (r_1 \lambda_1 + \dots + r_n \lambda_n)x_i = r_i \lambda_i x_i = y_i$$

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

It remains to prove the claim. To prove it, suppose that it is not true. Then $\lambda x_i = 0$ for all $i \in \{1, \dots, n - 1\}$ implies that $\lambda x_n = 0$. By the inductive hypothesis, given $z_1, \dots, z_{n-1} \in R$, there exists $r \in R$ such that $rx_i = z_i$ for all $i \in \{1, \dots, n - 1\}$. This allows us to define a map

$$\phi: V^{n-1} \rightarrow V, \quad \phi(z_1, \dots, z_{n-1}) = rx_n.$$

The map ϕ is well-defined: if $sx_i = z_i$ for all $i \in \{1, \dots, n - 1\}$, then, since $(r - s)x_i = 0$ for all $i \in \{1, \dots, n - 1\}$, it follows that $(r - s)x_n = 0$. Hence $rx_n = sx_n$. Moreover, a direct calculation shows that ϕ is an R -module homomorphism.

For $i \in \{1, \dots, n - 1\}$, let

$$\xi_i: V \xrightarrow{\iota_i} V^{n-1} \xrightarrow{\phi} V,$$

where the map $\iota_i: V \rightarrow V^{n-1}$ denotes the inclusion in the i -th component. By the inductive hypothesis, for $j \in \{1, \dots, n - 1\}$, there exists $r_j \in R$ such that

$$r_j x_i = \begin{cases} x_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, for example,

$$\xi_1(x_1) = \phi(x_1, 0, \dots, 0) = \phi(r_1x_1, \dots, r_1x_{n-1}) = r_1x_n.$$

More generally, $\xi_j(x_j) = r_jx_n$ for all $j \in \{1, \dots, n-1\}$. Note that, on the one hand,

$$\phi(x_1, \dots, x_{n-1}) = \phi(r_1x_1, r_2x_2, \dots, r_{n-1}x_{n-1}) = \xi_1x_1 + \dots + \xi_{n-1}x_{n-1}.$$

On the other hand,

$$x_n = 1x_n = \phi(x_1, \dots, x_{n-1}) = \xi_1x_1 + \dots + \xi_{n-1}x_{n-1},$$

a contradiction to the linear independence of the set $\{x_1, \dots, x_n\}$. \square

20.4. BONUS EXERCISE. Prove Jacobson's density theorem for non-unitary rings.

20.5. EXERCISE. Let D be a division ring and V be a D -vector space. Prove that if R is dense in V and I is a non-zero ideal of R , then I is dense on V .

20.6. COROLLARY. *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 vector space 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 vector space 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 vector space 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 20.2. 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. \square

§ 21. 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.

21.1. DEFINITION. 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.

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

21.3. EXAMPLE. A non-zero ideal of a prime ring is a prime ring.

21.4. EXERCISE. A ring is a domain if and only if it is both prime and has no non-zero nilpotent elements.

Rings with no non-zero nilpotent elements are called **reduced**.

A characterization of prime rings:

21.5. PROPOSITION. *Let R be a non-zero 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

$$IJ = (RxR)(RyR) \subseteq R(xRy)R = \{0\},$$

we may assume that $I = \{0\}$. In particular, Rx and xR are ideals, as $R(xR) = (Rx)R = \{0\}$. Since $(Rx)(Rx) = \{0\}$, it follows that $Rx = \{0\}$. Similarly, $xR = \{0\}$. Now $\mathbb{Z}x$ is an ideal of R , as

$$R(\mathbb{Z}x) = \mathbb{Z}(Rx) = \{0\} \subseteq \mathbb{Z}x, \quad (\mathbb{Z}x)R = \mathbb{Z}(xR) = \{0\}.$$

Now $(\mathbb{Z}x)R = \{0\}$ implies $\mathbb{Z}x = \{0\}$. Thus $x = 0$. □

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.

21.6. EXAMPLE. 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 $IJ = \{0\}$.

A theorem of Connel states (see Theorem 49.5) that if K is a field of characteristic zero and G is a group, then $K[G]$ is prime if and only if G does not contain non-trivial finite normal subgroups.

§ 22. Wedderburn's theorem

We studied minimal left ideals of rings before (see Definition 8.14).

22.1. LEMMA. *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 $x = 0$. □

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

22.3. THEOREM (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 22.1, R is primitive.

Now we prove that 3) \implies 4). If R is primitive, by Jacobson's density theorem we may assume that there is a division ring D and a D -vector space V such that $R \subseteq \text{End}_D(V)$ is dense in V . Now Lemma 22.2 and Proposition 20.2 imply 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

§ 23. The Artin–Wedderburn theorem

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 [18]– 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 in fact surjective.

23.1. DEFINITION. 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.

23.2. LEMMA. *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 (Exercise 8.30). By Wedderburn theorem, R/I is prime and hence I is prime. \square

23.3. THEOREM (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.

23.4. LEMMA. *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 Exercise 8.30. By Wedderburn's theorem, R/I is simple. Thus I is maximal by Proposition 8.19. \square

23.5. LEMMA. *Let R be a left artinian unitary ring. 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 (this is left as an exercise), it follows that either $x \in I_1$ or $y \in I_1$, a contradiction. \square

23.6. EXERCISE. Complete the proof of Lemma 23.5.

23.7. LEMMA. *Let R be a left artinian unitary ring. Then R has only finitely many primitive ideals.*

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

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

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

Now we are ready to prove the theorem.

PROOF OF THEOREM 23.3. Let I_1, \dots, I_k be the (distinct) primitive ideals of R . We know that each I_i is a maximal ideal. Thus $I_i + I_j = R$ for $i \neq j$. Since R is semiprimitive, $I_1 \cap \cdots \cap I_k = J(R) = \{0\}$. Let

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

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

We first claim that $I_1 + (I_2 \cdots I_k) = R$. In fact, since I_1, \dots, I_k are maximal ideals, $I_2 \cdots I_k \not\subseteq I_1$. 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

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

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

$$\varphi(x_2) = (I_1, x_2 + I_2, \dots, I_k),$$

$$\vdots$$

$$\varphi(x_k) = (I_1, I_2, \dots, x_k + I_k).$$

From this, it follows that φ is surjective: if $(x_1 + I_1, \dots, x_k + I_k) \in \prod_{j=1}^k R/I_j$, then

$$\begin{aligned}\varphi(x_1 + \dots + x_k) &= \varphi(x_1) + \dots + \varphi(x_k) \\ &= (x_1 + I_1, I_2, \dots, I_k) + \dots + (I_1, I_2, \dots, x_k + I_k) \\ &= (x_1 + I_1, \dots, x_k + I_k).\end{aligned}$$

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 (by Wedderburn's theorem). Therefore

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

§ 24. 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.

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

PROOF. Let I be a non-zero left ideal and 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 16.2. \square

24.2. DEFINITION. 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.

24.3. PROPOSITION. *Let R be a semisimple ring. Then ${}_R R$ is noetherian and artinian.*

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

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

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 17.2. \square

The previous proposition shows that every semisimple ring is both left artinian and left noetherian.

24.4. EXERCISE. If R is a semisimple ring, every R -module is semisimple.

24.5. EXERCISE. 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 $M_2(\mathbb{R})$.

24.6. THEOREM. *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 left 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 proper 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 $x_1 \in I \cap L_1$. Thus $I \cap L_1$ is a non-zero left ideal contained in the minimal left ideal L_1 , a contradiction. Now the claim follows, as $J(R) \subseteq M_1 \cap \dots \cap M_k = \{0\}$.

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 the Artin–Wedderburn theorem. Since each $M_{n_j}(D_j)$ is semisimple, it follows that R is semisimple. \square

§ 25. The Hopkins–Levitzki theorem

25.1. THEOREM (Hopkins–Levitzki). *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 16.9. Let n be such that $J^n = \{0\}$. Now consider the sequence

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

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 11.10, 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

§ 26. Local rings

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

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

Division rings are local rings.

26.2. THEOREM. 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 $x + M$. 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 $x + J(R) \neq J(R)$. Since $R/J(R)$ is a division ring, $x + J(R) \in \mathcal{U}(R/J(R))$. In particular, $1 - xy \in J(R)$ and hence $xy = 1 - (1 - xy) \in \mathcal{U}(R)$. Thus $1 = (xy)z = x(yz)$ for some $z \in R$ and therefore $x \notin I$, 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

26.3. DEFINITION. 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 $x \notin \{0, 1\}$.

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

26.5. EXERCISE. How many idempotents does \mathbb{Z}/n have?

26.6. EXERCISE. 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 .

26.7. LEMMA. 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

26.8. THEOREM. *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 theorem,

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

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

26.9. THEOREM. *The center of a local ring is local.*

PROOF. Let R be a local ring. By Theorem 26.2, $J(R) = R \setminus \mathcal{U}(R)$. We need to prove that $Z(R) \setminus \mathcal{U}(Z(R)) = J(Z(R))$. We first note that

$$(26.1) \quad \mathcal{U}(Z(R)) = Z(R) \cap \mathcal{U}(R).$$

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 (26.1) implies that $x \notin \mathcal{U}(R)$. By Theorem 26.2, $x \in J(R)$. Then $x \in J(R) \cap Z(R) \subseteq J(Z(R))$. \square

26.10. EXERCISE. Let R be a local ring. Prove that $Z(R) \cap J(R) = J(Z(R))$.

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

26.12. EXERCISE. Find a non-local ring with a unique maximal ideal.

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

26.14. EXERCISE. A ring R is said to be **Von Neumann regular** if for every non-zero $r \in R$, $r = rxx$ for some $x \in R$. Prove that a local Von Neumann ring is a division ring.

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

26.16. BONUS EXERCISE. A ring R is said to be **semilocal** if $R/J(R)$ is left artinian. 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 left ideals, then R is semilocal.
- 4) If R_1, \dots, R_k are rings, then $\bigoplus_{i=1}^k R_i$ is semilocal if and only if each R_i is semilocal.

26.17. BONUS EXERCISE. 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.

§ 27. Gustafson's theorem

In 1905, Schur proved that the maximum number of linearly independent $n \times n$ complex matrices is $\lfloor n^2/4 \rfloor + 1$, where $x \mapsto \lfloor x \rfloor$ is the greatest integer function. We will prove Schur's theorem by representation-theoretic methods.

27.1. THEOREM (Gustafson). *Let R be a complex commutative finite-dimensional algebra and M be a faithful n -dimensional R -module. Then*

$$\dim_{\mathbb{C}} R \leq \left\lfloor \frac{n^2}{4} \right\rfloor + 1.$$

Recall that the **floor function** is the function that takes an element $x \in \mathbb{R}$ and returns

$$\lfloor x \rfloor = \max\{m \in \mathbb{Z} : m \leq x\}.$$

Thus $x - 1 < \lfloor x \rfloor \leq x$.

27.2. EXERCISE. For $n \geq 1$, let $a_n = \lfloor n^2/4 \rfloor + 1$. Then

$$a_{n_1+\dots+n_k} \geq a_{n_1} + \dots + a_{n_k}.$$

We now need some exercises on commutative artinian unitary rings.

27.3. EXERCISE. Let R be a commutative artinian unitary ring. Prove that R has finitely many maximal ideals.

27.4. LEMMA. *Let R be a commutative artinian unitary ring. Then $R \simeq R_1 \times \dots \times R_k$ for local rings R_1, \dots, R_k .*

PROOF. By Lemma 23.7, R has finitely many primitive ideals, say I_1, \dots, I_k . Each I_j is a maximal ideal by Lemma 23.4. Moreover, $J(R) = I_1 \cap \dots \cap I_k$. Since R is artinian, $J(R)$ is nilpotent by Theorem 16.9. Thus

$$\{0\} = J(R)^m = (I_1 \cap \dots \cap I_k)^m = I_1^m \cap \dots \cap I_k^m$$

for some $m \geq 1$. By the Chinese remainder theorem,

$$R \simeq R/(I_1^m \cdots I_k^m) \simeq \prod_{j=1}^k R/I_j^m.$$

For $j \in \{1, \dots, k\}$, let $R_j = R/I_j^m$ and $\pi_j: R \rightarrow R_j$ be the canonical map. We claim that each R_j is a local ring with maximal ideal $\pi(I_j)$. By the correspondence theorem, the maximal ideals of R_j are in bijective correspondence with the maximal ideals of R containing I_j^m . Let M be a maximal ideal of R_j . We want to prove that $M = \pi(I_j)$. If $x \in I_j$, then $x^m \in I_j^m \subseteq \pi^{-1}(M)$. Since $\pi^{-1}(M)$ is a maximal ideal, it is a prime ideal of R . Thus $x \in \pi^{-1}(M)$, that is $\pi(x) \in M$. Since $\pi(I_j) \subseteq M$ and $\pi(I_j)$ is a maximal ideal of R , it follows that $\pi(I_j) = M$. \square

We also need the following very useful lemma:

27.5. LEMMA (Nakayama). *Let R be a unitary ring and M be a finitely generated R -module. If $J(R) \cdot M = M$, then $M = \{0\}$.*

PROOF. Assume that M is generated by x_1, \dots, x_n . Since $x_n \in M = J(R) \cdot M$, there exist $r_1, \dots, r_n \in J(R)$ such that $x_n = r_1 \cdot x_1 + \cdots + r_n \cdot x_n$, that is $(1 - r_n) \cdot x_n = \sum_{j=1}^{n-1} r_j \cdot x_j$. Since $1 - r_n$ is invertible, there exists $s \in R$ such that $s(1 - r_n) = 1$. Then $x_n = \sum_{j=1}^{n-1} (sr_j) \cdot x_j$ and hence M is generated by x_1, \dots, x_{n-1} . After repeating this procedure sufficiently many times (finitely many times), one gets $M = \{0\}$. \square

27.6. EXERCISE. Let R be a unitary ring and M be a finitely generated module.

- 1) If N be a submodule of M such that $J(R) \cdot M/N = M/N$, then $M = N$.
- 2) If $\pi: M \rightarrow M/(J(R) \cdot M)$ be the canonical map and $M/(J(R) \cdot M)$ is generated by $\{\pi(m_1), \dots, \pi(m_k)\}$ for some $m_1, \dots, m_k \in M$, then M is generated by $\{m_1, \dots, m_k\}$.

Recall that an idempotent of a ring R is an element $e \in R$ such that $e^2 = e$. Two idempotents e and f are said to be **orthogonal** if $ef = fe = 0$.

27.7. EXERCISE. Let R be a unitary ring. Prove that the following statements are equivalent:

- 1) $R = I_1 \oplus \cdots \oplus I_n$ as a direct sum of left ideals I_1, \dots, I_n of R .
- 2) $1 = e_1 + \cdots + e_n$ for some orthogonal idempotents e_1, \dots, e_n .

We are ready to prove Gustafson's theorem.

PROOF OF THEOREM 27.1. Assume first that R is a local ring and let I be its maximal ideal. Then $F = R/I$ is a field. Note that F is a finite extension of \mathbb{C} , so it is an algebraic extension. Since \mathbb{C} is algebraically closed, $F \simeq \mathbb{C}$. Moreover, $M/(I \cdot M)$ is a vector space over \mathbb{C} . Let $k \in \mathbb{Z}$ be such that $k = \dim(I \cdot M)$. Then $\dim M/(I \cdot M) = n - k$. Let

$$\{m_1 + I \cdot M, \dots, m_{n-k} + I \cdot M\}$$

be a basis of $M/(I \cdot M)$. Since $I = J(R)$, it follows from Exercise 27.6 that M is generated by $\{m_1, \dots, m_{n-k}\}$. Let V be the complex vector space generated by m_1, \dots, m_{n-k} and W

be the set of complex linear maps $V \rightarrow I \cdot M$. Then

$$\dim_{\mathbb{C}} W = \dim_{\mathbb{C}}(I \cdot M) \dim_{\mathbb{C}} V \leq k(n - k).$$

Let $f: I \rightarrow W$, $r \mapsto (v \mapsto r \cdot v)$. Then f is a well-defined complex linear map.

We claim that f is injective: if $r \in \ker f$, then $f(r) = 0$. Thus $r \cdot v = 0$ for all $v \in V$. In particular, since $r \cdot m_i = 0$ for all $i \in \{1, \dots, n - k\}$, it follows that $r \cdot m = 0$ for all $m \in M$. Since M is faithful, $r = 0$.

Since f is injective,

$$\dim_{\mathbb{C}} I \leq \dim_{\mathbb{C}} W \leq k(n - k) = \frac{n^2}{4} - \left(\frac{n}{2} - k\right)^2 \leq \frac{n^2}{4}.$$

Hence $\dim_{\mathbb{C}} I \leq \lfloor n^2/4 \rfloor$. Now

$$\dim_{\mathbb{C}} R = \dim_{\mathbb{C}} I + \dim_{\mathbb{C}}(R/I) \leq \lfloor n^2/4 \rfloor + 1.$$

Assume now that R is a commutative artinian ring. By Lemma 27.4, we may assume that $R = \bigoplus_{i=1}^k R_i$, where R_1, \dots, R_k are local artinian rings and ideals of R . Since R is unitary, $1 = e_1 + \dots + e_k$ for orthogonal idempotents $e_1 \in R_1, \dots, e_k \in R_k$ (see Exercise 27.7). In particular, $M = \sum_{j=1}^k e_j \cdot M$.

We claim that $M = \bigoplus_{j=1}^k e_j \cdot M$. For example, let $x \in e_1 \cdot M \cap (e_2 \cdot M + \dots + e_k \cdot M)$. Then $x = e_1 \cdot m_1 = e_2 \cdot m_2 + \dots + e_k \cdot m_k$ for some $m_1, \dots, m_k \in M$. Since $e_1^2 = e_1$ and $e_1 e_j = 0$ for all $j \in \{2, \dots, k\}$, we obtain that

$$\begin{aligned} e_1 \cdot x &= e_1^2 \cdot m_1 = e_1 \cdot m_1 = x, \\ e_1 \cdot x &= (e_1 e_2) \cdot m_2 + \dots + (e_1 e_k) \cdot m_k = 0. \end{aligned}$$

Then $x = 0$. In this way we prove that $M = \bigoplus_{j=1}^k e_j \cdot M$.

Each $e_j \cdot M$ is a faithful R_j -module. It is trivial to see that each $e_j \cdot M$ is an R_j -module. Let us show that, for example, $e_1 \cdot M$ is faithful. Let $r \in \text{Ann}_{R_1}(e_1 \cdot M)$. Then

$$(re_1) \cdot m = r \cdot (e_1 \cdot m) = 0$$

for all $m \in M$. Thus $re_1 = 0$, as $re_1 \in \text{Ann}_R(M) = \{0\}$ since M is faithful. Moreover,

$$r = r1 = r(e_1 + \dots + e_k) = re_1 + re_2 + \dots + re_k = re_2 + \dots + re_k.$$

Thus $r \in R_1 \cap (R_2 + \dots + R_k) = \{0\}$. Similarly one proves that each $e_j \cdot M$ is a faithful R_j -module. For $j \in \{1, \dots, k\}$, let $n_j = \dim_{\mathbb{C}} e_j \cdot M$. Then

$$n = \dim_{\mathbb{C}} M = \sum_{j=1}^k \dim_{\mathbb{C}}(e_j \cdot M) = \sum_{j=1}^k n_j.$$

Using Exercise 27.2 and the previous case,

$$\begin{aligned} \dim_{\mathbb{C}} R &= \sum_{j=1}^k \dim_{\mathbb{C}} R_j \leq \sum_{j=1}^k \left(\left\lfloor \frac{n_j^2}{4} \right\rfloor + 1 \right) \\ &\leq \left\lfloor \frac{(n_1 + \dots + n_k)^2}{4} \right\rfloor + 1 = \left\lfloor \frac{n^2}{4} \right\rfloor + 1. \end{aligned} \quad \square$$

The proof of Gustafson's theorem we presented can be easily adapted for arbitrary algebraically closed fields. Using the technique of **extensions of scalars** (see Theorem 33.17), we can get the result for other fields. Let K be a field and \bar{K} be its algebraic closure. If R is a finite-dimensional commutative K -algebra and M is a faithful R -module with $\dim_K M = n < \infty$, then $\bar{R} = R \otimes_K \bar{K}$ is a commutative \bar{K} -algebra and $\dim_{\bar{K}} \bar{R} = \dim_K R$. Moreover, $\bar{M} = M \otimes_K \bar{K}$ is a faithful \bar{R} -module with $\dim_{\bar{K}} \bar{M} = \dim_K M$. By Gustafson's theorem,

$$\dim_K R = \dim_{\bar{K}} \bar{R} \leq \left\lfloor \frac{n^2}{4} \right\rfloor + 1.$$

§ 28. Schur's theorem

We now present an application. For that purpose, we need a lemma.

28.1. LEMMA. *Let $\{A_1, \dots, A_m\} \subseteq M_n(\mathbb{C})$ be a maximal linearly independent set of commuting matrices. If R is the complex vector space generated by $\{A_1, \dots, A_m\}$, then R is a commutative finite-dimensional complex algebra and \mathbb{C}^n is a faithful R -module.*

PROOF. Let $B \in M_n(\mathbb{C})$ be such that $BA_i = A_iB$ for all $i \in \{1, \dots, m\}$. The set $\{A_1, \dots, A_m, B\}$ is linearly dependent, by the maximality of $\{A_1, \dots, A_m\}$. There exist $\mu, \lambda_1, \dots, \lambda_m \in \mathbb{C}$ not all zero such that

$$\lambda_1 A_1 + \dots + \lambda_m A_m + \mu B = 0.$$

Taking $B = A_i A_j$ for $i, j \in \{1, \dots, m\}$ we see that all products of the form $A_i A_j$ belong to R . Moreover, taking $B = I$ (the $n \times n$ identity matrix), we see that $I \in R$. A direct calculation now shows that R is a commutative finite-dimensional complex algebra.

To see that \mathbb{C}^n is a faithful R -module, let

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \in \text{Ann}_R(\mathbb{C}^n).$$

Then $Av = 0$ for all $v \in \mathbb{C}^n$. In particular,

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} = A \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Thus the first column of Av is zero. Similarly one proves that all the other columns of A need to be zero. \square

28.2. THEOREM (Schur). *Let S be a linearly independent set of commuting matrices of $M_n(\mathbb{C})$. Then*

$$|S| \leq \left\lfloor \frac{n^2}{4} \right\rfloor + 1.$$

PROOF. Let $T = \{A_1, \dots, A_m\}$ be a maximal set of linearly independent commuting $n \times n$ complex matrices. Let R be the complex vector space generated by A_1, \dots, A_m . By

Lemma 28.1, R is a finite-dimensional commutative complex algebra and $M = \mathbb{C}^n$ is a faithful R -module. Then

$$|S| \leq |T| = m = \dim_{\mathbb{C}} R \leq \left\lfloor \frac{n^2}{4} \right\rfloor + 1,$$

by Gustafson's theorem. □

There are other proofs of Schur's inequality. For example, Mirzakhani found a short and elementary proof, see [30].

§ 29. Rickart's theorem

We now consider Jacobson's semisimplicity problem.

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

As an application of Amitsur's theorem 12.3, 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.

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

To prove the theorem, we need a lemma.

29.3. LEMMA. *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 12.3. 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 12.3. □

We now prove the theorem.

PROOF OF THEOREM 29.2. For $\alpha = \sum_{i=1}^n \lambda_i g_i \in \mathbb{C}[G]$ let

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

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

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

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

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

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

29.6. PROPOSITION. *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:

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

29.8. EXERCISE. Let D be a division ring.

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

29.9. COROLLARY. *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 9.6, 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

29.10. EXERCISE. 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.

29.11. LEMMA. *Let M be a semisimple module and N be a submodule. Then N is a direct summand.*

SKETCH OF THE PROOF. Let $M = \bigoplus_{i \in I} M_i$ be a direct sum of simple submodules. Since each $N \cap M_i$ 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 $N \cap (\bigoplus_{j \in J} M_j) = \{0\}$. Our assumptions imply that X is non-empty. Zorn's lemma implies the existence of a maximal element K . Let $N_1 = \bigoplus_{k \in K} M_k$. 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.

29.12. PROPOSITION. *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 left 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 $g - 1 \in I$ for all $g \in G$. If $f = \sum_{h \in G} \lambda_h h$ (finite sum) and $g \in G$, 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

29.13. THEOREM. *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 24.6. \square

§ 30. Maschke's theorem

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

30.1. THEOREM (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 $L_{g_i}(g_j) = g_i g_j \neq g_j$ if $i \neq j$ and hence 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 9.6 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:

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

§ 31. 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.

31.1. DEFINITION. 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.

31.2. EXAMPLE. Every finite group is locally finite

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

31.4. EXAMPLE. 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.

31.5. EXAMPLE. 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.

31.6. EXAMPLE. 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.

31.7. PROPOSITION. *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 N 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

$$(31.1) \quad \{1\} = G_0 \subsetneq G_1 \subsetneq \dots \subsetneq G_n = G$$

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

31.8. EXAMPLE. Abelian groups are solvable.

Subgroups and quotients of solvable groups are solvable.

31.9. EXAMPLE. Groups of order < 60 are solvable.

31.10. EXAMPLE. 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.

31.11. PROPOSITION. *If G is a solvable torsion group, then G is locally finite.*

PROOF. We proceed by induction on n , the length of the sequence (31.1). 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 (31.1). 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 31.7. \square

We now prove Herstein's theorem.

31.12. THEOREM (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 $b_{n+1} \neq 0$. We can rewrite this as

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

for some $a_0, \dots, a_n \in K$. 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 $x_{j_1} \dots x_{j_l}$ could represent the same element of the group H . In this case, the coefficient of $x_{i_1} \dots x_{i_k} = x_{j_1} \dots x_{j_l}$ in α^k will be a positive integer ≥ 2 .

Let $w = x_{i_1} \dots x_{i_{n+1}} \in H$ be a word of length $n+1$. 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

§ 32. Formanek's theorem, I

We start with some exercises.

32.1. EXERCISE. Let K be a field. Let A be a K -algebra algebraic over K 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.

32.2. EXERCISE. 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 $\alpha, \beta \in \mathbb{C}[G]$.

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

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

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

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 $|\gamma_k| \rightarrow 0$ if $k \rightarrow \infty$. \square

§ 33. 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 $(u, v) + T$.

33.1. THEOREM. *Let U and V be vector spaces. Then there exists a bilinear map*

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

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

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

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

33.2. EXERCISE. Prove that the properties of the previous theorem characterize tensor products up to isomorphism.

Some properties:

33.3. PROPOSITION. 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. □

33.4. EXERCISE. 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:

33.5. PROPOSITION. 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

$$U \otimes V \rightarrow V \otimes U, \quad u \otimes v \mapsto v \otimes u.$$

Similarly, there exists a linear map

$$V \otimes U \rightarrow U \otimes V, \quad v \otimes u \mapsto u \otimes v.$$

Thus $U \otimes V \simeq V \otimes U$. □

33.6. EXERCISE. Prove that $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$.

33.7. EXERCISE. Prove that $U \otimes K \simeq U \simeq K \otimes U$.

33.8. PROPOSITION. *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

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

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

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

33.9. EXERCISE. Prove that $u \otimes v = 0$ and $v \neq 0$ imply $u = 0$.

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

PROOF. The $u_i \otimes v_j$ are generators of $U \otimes V$, as $u = \sum_i \lambda_i u_i$ and $v = \sum_j \mu_j v_j$ imply

$$u \otimes v = \sum_{i,j} \lambda_i \mu_j u_i \otimes v_j.$$

We now prove that the $u_i \otimes v_j$ are linearly independent. We need to show that each finite subset of the $u_i \otimes v_j$ is linearly independent. If $\sum_k \sum_l \lambda_{kl} u_{i_k} \otimes v_{j_l} = 0$, then

$$0 = \sum_k u_{i_k} \otimes \left(\sum_l \lambda_{kl} v_{j_l} \right).$$

Since the u_{i_k} are linearly independent, Proposition 33.8 implies that $\sum_l \lambda_{kl} v_{j_l} = 0$. Thus $\lambda_{kl} = 0$ for all k, l , as the v_{j_l} are linearly independent. □

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

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

33.11. COROLLARY. *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 the tensor product $U \otimes V$ is a finite sum of the form $\sum_i x_i \otimes y_i$, where $x_i \in U$ and $y_i \in V$. If $x_i = \sum_j \lambda_{ij} u_j$, then

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

33.12. EXERCISE. Let A and B be algebras. Prove that $A \otimes B$ is an algebra with
 $(a \otimes b)(x \otimes y) = ax \otimes by$.

33.13. EXERCISE. Let K be a field and A, B, C be K -algebras. 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 $A \simeq A_1$ and $B \simeq B_1$, then $A \otimes B \simeq A_1 \otimes B_1$.

Some examples:

33.14. PROPOSITION. 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

33.15. PROPOSITION. If A is an algebra, then $A \otimes K[X] \simeq A[X]$.

PROOF. Each element of the tensor product $A \otimes K[X]$ 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

33.16. EXERCISE. 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 33.15 and Exercise 33.16 are examples of a procedure known as **scalar extensions**.

33.17. THEOREM. 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 $\lambda, \mu \in E$. □

33.18. EXERCISE. 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 .

33.19. EXERCISE. Prove that if G is a group and K is a subfield of E , then

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

§ 34. 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.

34.1. THEOREM (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 $K[G] \simeq K \otimes_{\mathbb{Q}} \mathbb{Q}[G]$. Note that 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 $\alpha \in \mathbb{Q}[G] \subseteq K[G]$. By assumption, every element of $K[G]$ is invertible or a zero divisor. Assume first that α is invertible. Let $\beta \in K[G] \simeq K \otimes_{\mathbb{Q}} \mathbb{Q}[G]$ 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 $\alpha\beta_0 = 1$. Thus α is invertible in $\mathbb{Q}[G]$. Similarly, if α is a zero divisor, then $\alpha\beta = 0$ and $\alpha\beta_j = 0$ for all j . Thus α is a zero divisor in $\mathbb{Q}[G]$. Hence each $\alpha \in \mathbb{Q}[G]$ is invertible or a zero divisor, so Formanek's theorem for \mathbb{Q} applies. □

§ 35. Wedderburn's little theorem

35.1. DEFINITION. The n -th cyclotomic polynomial is defined as the polynomial

$$(35.1) \quad \Phi_n(X) = \prod (X - \zeta),$$

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

Some examples:

$$\Phi_2 = X - 1,$$

$$\Phi_3 = X^2 + X + 1,$$

$$\Phi_4 = X^2 + 1,$$

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1,$$

$$\Phi_6 = X^2 - X + 1,$$

$$\Phi_7 = X^6 + X^5 + \dots + X + 1.$$

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

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

PROOF. Write

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

35.3. LEMMA. *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

35.4. THEOREM (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

$$(35.2) \quad q^n - 1 = q - 1 + \sum_{j=1}^m \frac{q^n - 1}{q^{d_j} - 1},$$

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, (35.1) implies that

$$(35.3) \quad X^n - 1 = \Phi_n(X)(X^{d_j} - 1)h(X)$$

for some $h(X) \in \mathbb{Z}[X]$. By evaluating (35.3) 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 (35.2), $\Phi_n(q)$ 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, [40] contains a proof that uses only elementary linear algebra. In [36, Chapter 14] the theorem is proved using group theory.

35.5. THEOREM. *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.

35.6. LEMMA. *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

$$(35.4) \quad \sum_{d|n} f(d) = n.$$

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 $\sum_{d|n} \varphi(d)$ and (35.4), 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 35.5. 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

§ 36. Zsigmondy's theorem

One of Wedderburn's original proof of Theorem 35.4 uses a result proved by Zsigmondy [42]. Zsigmondy's theorem is quite popular in mathematical contests.

36.1. THEOREM (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 [41]. \square

We now quickly sketch a proof of Wedderburn's theorem 35.4 based on Zsigmondy's theorem.

Let D be a division ring of dimension n over \mathbb{Z}/p for a prime number p . Assume first that there exists a prime number q such that $q \nmid p$ and the order of p modulo q is n . Let $x \in D \setminus \{0\}$ be an element of order q and F be the subring of D generated by g . Note that F is a finite-dimensional (\mathbb{Z}/p) -vector space. Let $m = \dim F$. Since $g^{p^m-1} = 1$, q divides $p^m - 1$. Thus $m = n$ and hence $D = F$ is commutative.

Assume now that there is no prime number q such that $q \nmid p$ and the order of p modulo q is n . By Zsigmondy's theorem, $n = 2$ or $n = 6$ and $p = 2$. If $n = 2$, then D is commutative, as it is the subring generated by any element of $D \setminus \mathbb{Z}/p$. If $n = 6$ and $p = 2$, then the order of 2 modulo 9 is 6. Since $D \setminus \{0\}$ contains a subgroup of order 9 and all groups of order 9 are abelian, we can use the previous argument to complete the proof.

§ 37. Fermat's last theorem in finite rings

37.1. THEOREM. *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

§ 38. Frobenius's theorem

38.1. THEOREM (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.

38.2. LEMMA. *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

38.3. LEMMA. *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 $\beta\gamma = 0$, as $0 \leq 4\beta^2\gamma^2 y^2 \leq 0$. Hence $\alpha = \beta = \gamma = 0$. (If $\beta = 0$, then $0 \leq \gamma^2 = \alpha^2 x^2 \leq 0$. If $\gamma = 0$, then $\alpha = \beta = 0$ because $\{x, y\}$ is linearly independent.) 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

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

38.4. LEMMA. *Let D be a real division 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*

$$(38.1) \quad i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i.$$

PROOF. Let $V = \{x \in D : x^2 \in \mathbb{R}, x^2 \leq 0\}$ be the subspace of Lemma 38.3. For $x, y \in V$ let $x * y = xy + yx = (x + y)^2 - x^2 - y^2 \in \mathbb{R}$. If $x \neq 0$, then $x * x = 2x^2 \neq 0$. Since $\dim V = n - 1$, there exist $y, z \in V$ such that $\{y, z\}$ is linearly independent. Let

$$x = z - \frac{z * y}{y * y}y.$$

Since $\{y, z\}$ is linearly independent, $x \neq 0$. Moreover, since

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

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 (38.1) hold. For example,

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

Now we are finally ready to prove the theorem:

PROOF OF 38.1. 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 38.3 is non-zero and thus there exists $i \in D$ such that $i^2 = -1$. Hence $D \simeq \mathbb{C}$. Lemma 38.4 implies that $n \neq 3$. If $n = 4$, then $D \simeq \mathbb{H}$. Suppose that $n > 4$. By Lemma 38.4 there exist $i, j, k \in D$ such that $\{1, i, j, k\}$ is linearly independent and that the formulas of (38.1) hold. Let

$$V = \{x \in D : x^2 \in \mathbb{R}_{\leq 0}\}.$$

By Lemma 38.3, $\dim V = n - 1$. Thus there exists $x \in V \setminus \langle i, j, k \rangle$. Let

$$e = x + \frac{i * x}{2}i + \frac{j * x}{2}j + \frac{k * x}{2}k \in V \setminus \{0\}.$$

A direct calculation shows that $i * e = j * e = k * e = 0$. Then

$$ek = e(ij) = (ei)j = -(ie)j = -i(ej) = i(je) = (ij)e = ke,$$

a contradiction. \square

§ 39. Jacobson's commutativity theorem

We start with an easy exercise.

39.1. EXERCISE. 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 $xy = yx$.

39.2. EXERCISE. Let $n \geq 1$ and R be a ring such that $x^{3 \cdot 2^n} = x$ for all $x \in R$. Prove that R is commutative. R is commutative.

Hint: note that R has characteristic two and that $x^{2^{n+1}} = x^{2^n}$ for all $x \in R$. Thus R is a boolean ring.

39.3. PROPOSITION. *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 a direct product of finitely many fields. \square

In this lecture, we will extend the result of Proposition 39.3 to arbitrary (i.e. non-finite) rings.

39.4. THEOREM (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.

39.5. LEMMA. *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

$$(39.1) \quad (\text{ad } r)^n(x) = \sum_{k=0}^n (-1)^k \binom{n}{k} r^{n-k} x r^k$$

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:

39.6. EXERCISE. 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 39.4. We divide the proof into 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 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

$$(39.2) \quad \delta(\delta - x_1 \text{id}) \cdots (\delta - x_{p^k-1} \text{id}) = 0$$

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 (39.2) 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 [31].

§ 40. Project: An analytic proof of Rickart's theorem

We will present a different proof of Rickart's theorem 29.2.

40.1. DEFINITION. Let R be a ring. An **involution** in R is an additive map $R \rightarrow R$, $x \mapsto x^*$, such that $x^{**} = x$ and $(xy)^* = y^*x^*$ for all $x, y \in R$.

It follows that if R is a unitary ring, then $1^* = 1$.

40.2. EXAMPLE. The conjugation $z \mapsto \bar{z}$ is an involution of \mathbb{C} .

40.3. EXAMPLE. The transpose map $X \mapsto X^T$ is an involution of $M_n(K)$.

40.4. EXAMPLE. Let G be a group. Then

$$\left(\sum_{g \in G} \alpha_g g \right)^* = \sum_{g \in G} \overline{\alpha_g} g^{-1}$$

is an involution of the group ring $\mathbb{C}[G]$.

For a group G , one defines the **trace** of an element

$$\alpha = \sum_{g \in G} \alpha_g g \in K[G]$$

as $\text{trace}(\alpha) = \alpha_1$. One proves that the map

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

is K -linear such that $\text{trace}(\alpha\beta) = \text{trace}(\beta\alpha)$ for all $\alpha, \beta \in K[G]$.

40.5. EXERCISE. Let G be a finite group and K be a field of characteristic not dividing the order of G . Prove the following statements:

- 1) If $\alpha \in K[G]$ is nilpotent, then $\text{trace}(\alpha) = 0$.
- 2) If $\alpha \in K[G]$ is idempotent, then $\text{trace}(\alpha) = \dim(K[G]\alpha)/|G|$.

40.6. EXERCISE. Prove that $\langle \alpha, \beta \rangle = \text{trace}(\alpha\beta^*)$, $\alpha, \beta \in \mathbb{C}[G]$, defines an inner product in $\mathbb{C}[G]$.

40.7. LEMMA. Let G be a group. Prove that if $J(\mathbb{C}[G]) \neq 0$, then there exists $\alpha \in J(\mathbb{C}[G])$ such that $\text{trace}(\alpha^{2^m}) \in \mathbb{R}_{\geq 1}$ for all $m \geq 1$.

PROOF. Let $\alpha = \sum_{g \in G} \alpha_g g \in \mathbb{C}[G]$. Then

$$\text{trace}(\alpha^* \alpha) = \sum_{g \in G} \overline{\alpha_g} \alpha_g = \sum_{g \in G} |\alpha_g|^2 \geq |\alpha_1|^2 = |\text{trace}(\alpha)|^2.$$

By induction, one proves that, if α is such that $\alpha^* = \alpha$, then

$$\text{trace}(\alpha^{2^m}) \geq |\text{trace}(\alpha)|^{2^m}$$

for all $m \geq 1$.

Let $\beta = \sum_{g \in G} \beta_g g \in J(\mathbb{C}[G])$ be such that $\beta \neq 0$. Since $\text{trace}(\beta^* \beta) = \sum_{g \in G} |\beta_g|^2 \neq 0$ and $J(\mathbb{C}[G])$ is an ideal,

$$\alpha = \frac{\beta^* \beta}{\text{trace}(\beta^* \beta)} \in J(\mathbb{C}[G]).$$

Then α is such that $\alpha^* = \alpha$ and $\text{trace}(\alpha) = 1$. Hence $\text{trace}(\alpha^{2^m}) \geq 1$ for all $m \geq 1$. \square

Exercise 32.2 implies that $\mathbb{C}[G]$ with $\text{dist}(\alpha, \beta) = |\alpha - \beta|$ is a metric space. In this metric space, the map $\mathbb{C}[G] \rightarrow \mathbb{C}$, $\alpha \mapsto \text{trace}(\alpha)$, is a continuous map.

40.8. LEMMA. *Let $\alpha \in J(\mathbb{C}[G])$. The map*

$$\varphi: \mathbb{C} \rightarrow \mathbb{C}[G], \quad \varphi(z) = (1 - z\alpha)^{-1},$$

is continuous, differentiable and $\varphi(z) = \sum_{n \geq 0} \alpha^n z^n \in \mathbb{C}[G]$ if $|z|$ is sufficiently small.

PROOF. Let $y, z \in \mathbb{C}$. Since $\varphi(y)$ and $\varphi(z)$ commute,

$$(40.1) \quad \begin{aligned} \varphi(y) - \varphi(z) &= ((1 - z\alpha) - (1 - y\alpha)) (1 - y\alpha)^{-1} (1 - z\alpha)^{-1} \\ &= (y - z)\alpha\varphi(y)\varphi(z). \end{aligned}$$

Hence $|\varphi(y)| \leq |\varphi(z)| + |y - z|\|\alpha\varphi(y)\|\varphi(z)|$ and therefore

$$|\varphi(y)| (1 - |y - z|\|\alpha\varphi(z)\|) \leq |\varphi(z)|.$$

Fix z and choose y sufficiently close to z in such a way that $1 - |y - z|\|\alpha\varphi(z)\| \geq 1/2$. Then $|\varphi(y)| \leq 2|\varphi(z)|$. Using (40.1) one obtains that $|\varphi(y) - \varphi(z)| \leq 2|y - z|\|\alpha\|\varphi(z)|^2$. Hence φ is continuous. By (40.1),

$$\varphi'(z) = \lim_{y \rightarrow z} \frac{\varphi(y) - \varphi(z)}{y - z} = \lim_{y \rightarrow z} \alpha\varphi(y)\varphi(z) = \alpha\varphi(z)^2$$

for all $z \in \mathbb{C}$.

If z is such that $|z|\|\alpha\| = |z\alpha| < 1$, then

$$\varphi(z) - \sum_{n=0}^N z^n \alpha^n = \varphi(z) \left(1 - (1 - z\alpha) \sum_{n=0}^N z^n \alpha^n \right) = \varphi(z)(z\alpha)^{N+1}.$$

Then

$$\left| \varphi(z) - \sum_{n=0}^N z^n \alpha^n \right| \leq |\varphi(z)| |z\alpha|^{N+1}.$$

Since $\varphi(z)$ is bounded close to $z = 0$, we conclude that

$$\left| \varphi(z) - \sum_{n=0}^N z^n \alpha^n \right| \rightarrow 0$$

if $N \rightarrow \infty$. □

We now provide an alternative proof of Rickart's theorem:

40.9. THEOREM (Rickart). *If G is a group, then $J(\mathbb{C}[G]) = \{0\}$.*

PROOF. Let $\alpha \in J(\mathbb{C}[G])$ and $\varphi(z) = (1 - \alpha z)^{-1}$. Let

$$f: \mathbb{C} \rightarrow \mathbb{C}, \quad f(z) = \text{trace } \varphi(z) = \text{trace } ((1 - \alpha z)^{-1}).$$

By Lemma 40.8, $f(z)$ is an entire function such that $f'(z) = \text{trace}(\alpha\varphi(z)^2)$ and

$$(40.2) \quad f(z) = \sum_{n=0}^{\infty} z^n \text{trace}(\alpha^n)$$

if $|z|$ is sufficiently small. In particular, (40.2) is the Taylor series of $f(z)$ around the origin. This implies that the series converges to $f(z)$ for all $z \in \mathbb{C}$. In particular,

$$(40.3) \quad \lim_{n \rightarrow \infty} \text{trace}(\alpha^n) = 0.$$

On the other hand, if $\alpha \neq 0$, Lemma 40.7 implies that $\text{trace}(\alpha^{2^m}) \geq 1$ for all $m \geq 0$. This contradicts the limit computed in (40.3). Hence $\alpha = 0$. \square

For a corollary, we need a consequence of Nakayama's lemma 27.5.

40.10. LEMMA. *Let R and S be unitary rings and $\iota: R \rightarrow S$ be a ring homomorphism. If*

$$S = \iota(R)x_1 + \cdots + \iota(R)x_n,$$

where each x_j is such that $x_j y = y x_j$ for all $y \in \iota(R)$, then $\iota(J(R)) \subseteq J(S)$.

PROOF. We claim that $J = \iota(J(R))$ acts trivially on each simple S -module M . Let M be a simple S -module. Write $M = Sm$ for some $m \neq 0$. Then M is an R -module with $r \cdot m = \iota(r)m$. Since

$$M = Sm = (\iota(R)x_1 + \cdots + \iota(R)x_n)m = \iota(R)(x_1m) + \cdots + \iota(R)(x_nm),$$

M is finitely generated as an $\iota(R)$ -module. Moreover, $J(R) \cdot M = JM = \iota(J)M$ is an S -submodule of M , as

$$x_j(JM) = (x_j J)M = (Jx_j)M = J(x_j M) \subseteq JM.$$

Since $M \neq \{0\}$, Nakayama's lemma implies that $J(R) \cdot M \subsetneq M$. Since M is a simple S -module, we conclude that $J(R)M = \{0\}$. \square

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

PROOF. Let $\iota: \mathbb{R}[G] \rightarrow \mathbb{C}[G]$ be the canonical inclusion. Since

$$\mathbb{C}[G] = \mathbb{R}[G] + i\mathbb{R}[G],$$

Now Lemma 40.10 and Rickart's theorem imply that $\iota(J(\mathbb{R}[G])) \subseteq J(\mathbb{C}[G]) = \{0\}$. We conclude that $J(\mathbb{R}[G]) = 0$, as the map ι is injective. \square

§ 41. Project: Hurewicz' theorem

Let R be a unitary commutative ring and G be a group. Recall that **group ring** is a free R -module which is also a ring. As a free R -module, G is a basis for $R[G]$. Thus every element $\alpha \in R[G]$ can be written uniquely as a sum of the form

$$\alpha = \sum_{g \in G} r_g g, \quad r_g \in R.$$

Note that the elements of R (more precisely, the elements of the form $r1_G$ for $r \in R$) are central in $R[G]$.

41.1. EXERCISE. Let R be a commutative ring and G be a group. Let

$$f: R[G] \rightarrow R, \quad \sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g.$$

Prove the following statements:

- 1) f is a surjective ring homomorphism.
- 2) $\{g - 1_G : 1_G \neq g \in G\}$ is a basis for the free R -module $\ker f$.

The kernel of the homomorphism of Exercise 41.1 is called the **augmentation ideal** of the group ring. We used this ideal before (e.g. Propositions 29.12 and Appendix 50).

41.2. THEOREM (Hurewicz). *Let G be a group and I be the augmentation ideal of $\mathbb{Z}[G]$. Then $G/[G, G] \simeq I/I^2$ as (abelian) groups.*

PROOF. Let $\varphi: G \rightarrow I/I^2$, $g \mapsto g - 1_G + I^2$. Since $g - 1_G \in I$ for all $g \in G$, φ is well-defined. The map φ is a group homomorphism. Since $(g - 1_G)(h - 1_G) \in I^2$,

$$\begin{aligned} \varphi(gh) &= gh - 1_G + I^2 \\ &= gh - 1_G - (g - 1_G)(h - 1_G) + I^2 + I^2 \\ &= g - 1_G + h - 1_G + I^2 \\ &= \varphi(g) + \varphi(h) \end{aligned}$$

holds for all $g, h \in G$.

Since $[G, G] \subseteq \ker \varphi$, there exists a group homomorphism

$$\bar{\varphi}: G/[G, G] \rightarrow I/I^2, \quad g[G, G] \mapsto g - 1_G + I^2.$$

We claim that $\bar{\varphi}$ is an isomorphism. Let us construct the inverse of $\bar{\varphi}$. Let

$$\psi: I \rightarrow G/[G, G], \quad \sum_{g \in G} m_g (g - 1_G) \mapsto \left(\prod_{g \in G} g^{m_g} \right) [G, G].$$

Since $G/[G, G]$ is abelian, the map ψ is well-defined, that is the order of the factors in $\prod_{g \in G} g^{m_g}$ does not matter. Note that $I^2 \subseteq \ker \psi$, as $\{(g - 1_G)(h - 1_G) : g, h \in G\}$ generates the additive group I^2 and

$$\begin{aligned} \psi((g - 1_G)(h - 1_G)) &= \psi((gh - 1_G) - (g - 1_G) - (h - 1_G)) \\ &= (ghg^{-1}h^{-1})[G, G] \\ &= [G, G]. \end{aligned}$$

Therefore there exists a group homomorphism

$$\bar{\psi}: I/I^2 \rightarrow G/[G, G], \quad \sum_{g \in G} m_g(g - 1_G) + I^2 \mapsto \left(\prod_{g \in G} g^{m_g} \right) [G, G].$$

A direct calculation shows that $\bar{\psi}$ is the inverse of $\bar{\varphi}$. □

§ 42. Project: Dedekind-finite rings

A standard reference for Dedekind-finite rings is Lam's book [28].

42.1. DEFINITION. Let R be a ring with one. We say that R is **Dedekind-finite** if for $a, b \in R$ such that $ab = 1$ one has $ba = 1$.

Trivially, commutative rings are Dedekind finite.

42.2. EXERCISE. Give an example of a ring that is not Dedekind-finite.

42.3. EXERCISE. Let R be a commutative unitary ring. Prove that $M_n(R)$ is Dedekind-finite.

42.4. PROPOSITION. *Let R be a unitary ring. Then R is Dedekind-finite if and only if the left regular module ${}_R R$ is Hopfian, that is every surjective R -module homomorphism $R \rightarrow R$ is injective.*

PROOF. Assume first that R is Dedekind-finite. Let $f: R \rightarrow R$ be a surjective R -module homomorphism. There exists $a \in R$ such that $1 = f(a) = af(1)$ and hence $f(1)a = 1$. Let $x \in \ker f$. Then $0 = f(x)a = xf(1)a = x$. Thus f is injective. Conversely, let $a, b \in R$ be such that $ab = 1$. Let $f: R \rightarrow R$, $f(r) = rb$. Then f is surjective, as $f(ra) = (ra)b = r(ab) = r$ for all $r \in R$. By assumption, f is injective. In particular, $ba = 1$, as $b = f(1) = f(ba)$. \square

42.5. EXERCISE. Let R be a unitary ring. An R -module is said to be **Dedekind-finite** if $M \simeq M \oplus N$ for some R -module N implies that $N = \{0\}$. Prove the following statements:

- 1) M is Dedekind-finite if and only if the ring $\text{End}(M)$ is Dedekind-finite.
- 2) ${}_R R$ is Dedekind-finite if and only if the ring R is Dedekind-finite.

42.6. EXERCISE. Prove that an R -module that is not Dedekind-finite contains a submodule of the form $N \oplus N \oplus N \oplus \cdots$ for some non-zero R -module N .

42.7. EXERCISE. Let R be a unitary ring.

- 1) Let $a, b \in R$ be such that $ab = 1$. For $i, j \geq 1$, let $e_{ij} = b^{i-1}a^{j-1} - b^i a^j$. Prove that $e_{ij}e_{kl} = \delta_{jk}e_{il}$, where δ_{ij} is the Kronecker function.
- 2) Prove that e_{1n} is nilpotent for all $n \geq 2$.
- 3) Prove that if R is not Dedekind-finite, then R contains infinitely many nilpotent elements.

42.8. EXERCISE. A ring R is said to be **reversible** if for all $a, b \in R$ $ab = 0$ implies $ba = 0$. Prove that a unitary reversible ring is Dedekind-finite.

The previous exercise implies that reduced rings are Dedekind-finite.

42.9. EXERCISE. Prove that every left noetherian ring is Dedekind-finite.

The previous exercise and the Hopkins–Levitzki theorem imply that artinian unitary rings are Dedekind-finite. Can you write a proof without using the Hopkins–Levitzki theorem?

42.10. EXERCISE. Prove that every algebraic algebra is a Dedekind-finite ring. In particular, finite-dimensional algebras are Dedekind-finite.

42.11. EXERCISE. Let R be a unitary ring. Prove that if $R/J(R)$ is Dedekind-finite, then R is Dedekind finite.

Recall that an element a of a ring admits a right inverse if there exists an element b such that $ab = 1$.

42.12. EXERCISE. Let R be a unitary ring and $a \in R$ that admits a right inverse. Prove that the following statements are equivalent:

- 1) a admits at least two right inverses.
- 2) a is not a unit.
- 3) a is a left zero divisor.

Note that an element that admits at least two right inverses cannot be a unit.

42.13. THEOREM (Kaplansky). *Let R be a unitary ring. If $u \in R$ has more than one right inverse, then u has infinitely many right inverses.*

PROOF. Let $S = \{x \in R : ux = 1\}$. Assume that u admits finitely right inverses, that is S is a finite set. Let $s \in S$ and $T = \{xy - 1 + s : x \in S\}$. By assumption, $|S| \geq 2$. Note that $T \subseteq S$, as

$$u(xu - 1 + s) = (ux)u - u + us = 1.$$

Let $f: S \rightarrow T$, $x \mapsto xu - 1 + s$. Then f is injective:

$$f(x) = f(y) \implies xu - 1 + s = yu - 1 + s \implies xu = yu \implies xy,$$

because u admits a right inverse. Then $|S| \leq |T| \leq |S| < \infty$ and hence $S = T$. In particular, $s \in T$ and therefore $s = xu - 1 + s$ for some $x \in S$, that is $xu = 1$. For $t \in S \setminus \{x\}$,

$$x = x(ut) = (xu)t = t,$$

a contradiction. Therefore S is an infinite set. □

The following exercise gives another elementary proof of Kaplansky's theorem; see [35].

42.14. BONUS EXERCISE. Let R be a unitary ring. Prove the following statements:

- 1) If $a_1, \dots, a_n \in R$ are distinct elements such that $ba_i = 1$, then the set

$$\{a_1 - a_i : 1 \leq i \leq n\} \cup \{1 - a_i b : 1 \leq i \leq n\}$$

contains at least $n + 1$ solutions of $bx = 0$.

- 2) If b has $n \geq 2$ right inverses, then $bx = 0$ has at least $n + 1$ solutions and hence b has $n + 1$ right inverses.

§ 43. Project: The Skolem–Noether theorem

We now present an elementary proof of the Skolem–Noether theorem. We refer to [7] for more information.

43.1. DEFINITION. 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.

43.2. PROPOSITION. *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

43.3. EXAMPLE. \mathbb{H} is a real central algebra.

43.4. EXAMPLE. \mathbb{C} is a complex central algebra but it is not a real central algebra.

A celebrated theorem by Frobenius states that every finite-dimensional real central division algebra is isomorphic to \mathbb{R} or \mathbb{H} (see Theorem 38.1).

43.5. PROPOSITION. *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 $a, b \in A$.

43.6. DEFINITION. 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 $a, b \in A$.

43.7. LEMMA. *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. \square

43.8. LEMMA. 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. \square

43.9. LEMMA. 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 43.8 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

43.10. DEFINITION. 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.

43.11. EXAMPLE. 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.

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

43.13. THEOREM (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 43.9, $f = \sum_{i=1}^n L_{a_i} R_{b_i}$. 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 43.8, $f(x)a_1 - a_1 x = 0$ 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

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

§ 44. Project: The Brauer group

Fix a field K . Recall that a K -algebra A is **simple** if $\{0\}$ and A are the only ideals of A . For example, if D is a division algebra, then D and $M_n(D)$ are simple algebras.

44.1. EXAMPLE. If $a, b \in K \setminus \{0\}$, let $H_K(a, b)$ be the K -algebra with basis $\{1, i, j, k\}$ and multiplication given by

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k.$$

The quaternion algebra $H_K(a, b)$ is a simple K -algebra, as either $H_K(a, b)$ is a division algebra or $H_K(a, b) \simeq M_2(K)$.

A well-known particular case: $\mathbb{H} = H_{\mathbb{R}}(-1, -1)$.

44.2. DEFINITION. A **central simple algebra** is a finite-dimensional algebra K -algebra such that A is simple and $Z(A) = K$.

For example, \mathbb{C} is a complex central simple algebra and it is not a real central simple algebra, as $Z(\mathbb{C}) = \mathbb{C}$. Moreover, \mathbb{H} and \mathbb{R} are central simple algebras over \mathbb{R} .

44.3. EXERCISE. Prove that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq M_4(\mathbb{R})$.

The previous exercise shows that the tensor product of central simple algebras is not necessarily a central simple algebra.

Wedderburn's theorem states that every finite-dimensional simple algebra is isomorphic to $M_n(D)$ for some n and some division algebra D .

44.4. EXERCISE. Prove that the n in Wedderburn's theorem is unique and the division algebra D is unique up to isomorphism.

Let A and B be central simple K -algebras. By Wedderburn's theorem, $A \simeq M_n(D)$ and $B \simeq M_m(E)$ for some $m, n > 0$ and division algebras D and E . We define

$$A \sim B \iff D \simeq E.$$

44.5. EXERCISE. Prove that \sim is an equivalence relation.

If D is a central division K -algebra, then $D = M_1(D) \sim M_n(D)$ for all n .

44.6. EXERCISE. Let D be a K -algebra. Prove that $D \otimes_K M_n(K) \simeq M_n(D)$ as K -algebras

44.7. EXERCISE. Prove that $M_n(K) \otimes_K M_m(K) \simeq M_{nm}(K)$.

If A is a central simple algebra, $[A]$ will denote the equivalence class of A under the relation \sim , that is $[A] = \{B : B \sim A\}$.

44.8. EXERCISE. Prove that the collection of equivalence classes of central simple algebras is a set.

One way to solve the previous exercise is to recall that, by definition, central simple algebras are finite-dimensional. Then that the underlying vector space of a central simple

algebra over K is K^n for some n . Algebra structures over K^n form a set, as they are indeed a subset of $\text{Hom}(K^n \otimes K^n, K^n)$.

44.9. THEOREM. *Let $\text{Br}(K)$ be the set of equivalence classes of central simple K -algebras. Then $\text{Br}(K)$ with the operation*

$$(44.1) \quad [A][B] = [A \otimes_K B]$$

is an abelian group.

SKETCH OF THE PROOF. We need to show that the product of $\text{Br}(K)$ is well-defined. There are several things to prove:

- 1) $A \otimes_K B$ is a finite-dimensional central simple K -algebra.
- 2) The multiplication $[A][B] = [A \otimes_K B]$ is well-defined, that is $A \sim A_1$ and $B \sim B_1$ imply that $A \otimes_K B \sim A_1 \otimes_K B_1$.

To prove 1) we note that $A \otimes_K B$ is a finite-dimensional K -algebra, as

$$\dim_K(A \otimes_K B) = (\dim_K A)(\dim_K B).$$

It is central, as $Z(A \otimes_K B) \simeq Z(A) \otimes_K Z(B)$. Finally, it is simple, as there exists a bijective correspondence between ideals of A and ideals of $A \otimes_K B$.

Let us prove 2). Write $A \simeq M_n(D)$, $A_1 \simeq M_{n_1}(D)$, $B \simeq M_m(E)$ and $B_1 \simeq M_{m_1}(E)$ for some division K -algebras D and E . Since the tensor product is associative and commutative,

$$\begin{aligned} A \otimes_K B &\simeq M_n(D) \otimes_K M_m(E) \\ &\simeq D \otimes_K M_n(K) \otimes_K E \otimes_K M_m(K) \\ &\simeq D \otimes_K E \otimes_K M_{nm}(K) \\ &\simeq M_{nm}(D \otimes_K E). \end{aligned}$$

Note that $D \otimes_K E$ is maybe not a division algebra, but it is indeed a finite-dimensional central simple algebra. By Wedderburn's theorem, $D \otimes_K E \simeq M_p(F)$ for some division K -algebra F and some p . This implies that

$$A \otimes_K B \simeq M_{nmp}(F).$$

Similarly, $A_1 \otimes_K B_1 \simeq M_{n_1 m_1 p}(F)$ and thus $A \otimes_K B \sim A_1 \otimes_K B_1$.

Now we need to prove that $\text{Br}(K)$ is a group. The multiplication (44.1) is associative and commutative since the tensor product \otimes_K is associative and multiplicative. The identity of $\text{Br}(K)$ is $[K]$, as $[A][K] = [A \otimes_K K] = [A]$. Finally, the inverse of $[A]$ is $[A^{\text{op}}]$, as

$$[A][A^{\text{op}}] = [A \otimes_K A^{\text{op}}] = [M_n(K)]. \quad \square$$

44.10. EXERCISE. Let D be a division algebra. Compute the center of $M_n(D)$.

Let us compute some examples:

44.11. PROPOSITION. $\text{Br}(\mathbb{C}) = \{0\}$.

PROOF. Let A be a complex central simple algebra. Then $A \simeq M_n(D)$ for some complex division algebra D . We claim that $D \simeq \mathbb{C}$. Let $m = \dim D$ and $\alpha \in D$. Since $\{1, \alpha, \dots, \alpha^m\}$ has $m+1$ elements, it is a linearly dependent set. This means that there exists $\lambda_0, \dots, \lambda_m \in \mathbb{C}$ not all zero such that $0 = \sum_{i=0}^m \lambda_i \alpha^i$. Thus the non-zero polynomial $f = \sum_{i=0}^m \lambda_i X^i \in \mathbb{C}[X]$

is such that $f(\alpha) = 0$. Since \mathbb{C} is algebraically closed, there exist $\alpha_0, \dots, \alpha_N \in \mathbb{C}$ and $a \in \mathbb{C} \setminus \{0\}$ such that

$$f = a \prod_{i=0}^N (X - \alpha_i).$$

Since D is a division algebra, there exists $i \in \{0, \dots, m\}$ such that $\alpha = \alpha_i$. In particular, $\alpha \in \mathbb{C}$. Therefore $[A] = [\mathbb{C}]$ and hence $\text{Br}(A) = \{0\}$. \square

An application of Wedderburn's little theorem:

44.12. PROPOSITION. *Let F be a finite field. Then $\text{Br}(F) = \{0\}$.*

PROOF. Let A be a central simple algebra over F . Then $A \simeq M_n(D)$ for some division F -algebra D . Since $\dim_F D < \infty$ and F is finite, $F = Z(A) \simeq Z(M_n(D)) \simeq Z(D) = D$ by Wedderburn's little theorem and hence $[A] = [F]$. \square

An application of Frobenius' theorem:

44.13. PROPOSITION. *$\text{Br}(\mathbb{R})$ is the cyclic group of order two.*

PROOF. Let A be a central simple real algebra. Then $A \simeq M_n(D)$ where either $D \simeq \mathbb{R}$ or $D \simeq \mathbb{H}$ by Frobenius' theorem, as

$$\mathbb{R} \simeq Z(A) \simeq Z(M_n(D)) \simeq Z(D)$$

and $Z(\mathbb{C}) = \mathbb{C}$. Thus $\text{Br}(\mathbb{R})$ has only two elements, that is $\text{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$. \square

Let L/K be a Galois extension of degree n . Extending scalars we obtain a group homomorphism

$$\text{res}: \text{Br}(K) \rightarrow \text{Br}(L), \quad [A] \mapsto [A \otimes_K L],$$

known as the **restriction homomorphism**.

44.14. EXERCISE. Prove that res is well-defined.

44.15. DEFINITION. Let L/K be a Galois extension of degree n . The **restricted Brauer group** is $\text{Br}(L/K)$ is defined as the kernel of the restriction homomorphism.

Recall that the Galois group G of L/K is a finite group. Let $Z^2(G, L^\times)$ be the set of maps $\alpha: G \times G \rightarrow L^\times$ such that

$$\alpha(g, h)\alpha(gh, k) = g(\alpha(h, k))\alpha(g, hk)$$

for all $g, h, k \in G$.

We say that $\alpha \in Z^2(G, L^\times)$ and $\beta \in Z^2(G, L^\times)$ are equivalent if and only if there exists $\{\delta_g : g \in G\} \subseteq L$ such that

$$\beta(g, h) = \delta_g g(\delta_h) \alpha(g, h) \delta_{gh}^{-1}$$

for all $g, h \in G$.

The second cohomology group $H^2(G, L^\times)$ is defined as the set of equivalence classes of $Z^2(G, L^\times)$. One proves that $H^2(G, L^\times)$ is indeed an abelian group.

44.16. EXERCISE. Let G be a finite group. For $\alpha \in Z^2(G, L^\times)$ let us consider the crossed product $L_t^\alpha G$ of G by K given by

$$L_t^\alpha G = \left\{ \sum_{g \in G} \lambda_g e_g : \lambda_g \in L \right\}.$$

1) Prove that the product

$$(\lambda_g e_g)(\lambda_h e_h) = \lambda_g g(\lambda_h) \alpha(g, h) e_{gh}.$$

is associative.

2) Prove that $e = \alpha(1, 1)^{-1} e_1$ is such that $ee_g = e_g e = e_g$ for all $g \in G$.

3) Prove that each e_g is invertible with inverse

$$e_g^{-1} = \alpha(g^{-1}, g)^{-1} \alpha(1, 1)^{-1} e_{g^{-1}}.$$

44.17. THEOREM. Let L/K be a Galois extension of degree n and group G . Then

$$\text{Br}(L/K) \simeq H^2(G, L^\times).$$

The isomorphism of the theorem is given by

$$H^2(G, L^\times) \rightarrow \text{Br}(L/K) \subseteq \text{Br}(K), \quad [\alpha] \mapsto [L_t^\alpha G],$$

We do not have time to prove the theorem in detail, as it requires some tools that are outside the scope of our course.

44.18. COROLLARY. $\text{Br}(K)$ is a torsion group.

SKETCH OF THE PROOF. The theorem implies that for every finite Galois extension L/K one has $\text{Br}(L/K) \simeq H^2(G, L^\times)$ is a torsion group, as $|G|H^2(G, L^\times) = \{0\}$. To finish the proof note that $\text{Br}(K) = \bigcup \text{Br}(L/K)$, where the union is taken over all finite Galois extensions L/K . \square

The theorem can be used to compute Brauer groups. Let us give an example. We know that \mathbb{C}/\mathbb{R} is a Galois extension with Galois group isomorphic to $\mathbb{Z}/2$. Thus

$$\text{Br}(\mathbb{R}) = \text{Br}(\mathbb{C}/\mathbb{R}) \simeq H^2(\mathbb{Z}/2, \mathbb{C}^\times) \simeq \mathbb{Z}/2.$$

§ 45. Project: The Andrunakevic–Rjabuhin theorem

45.1. DEFINITION. A ring R is **reduced** if has no non-zero nilpotent elements.

Every commutative domain is reduced.

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

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

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

45.5. EXERCISE. 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 $R[X_1, \dots, X_n]$.

45.6. EXAMPLE. Let $R = \mathbb{Z}/3 \times \mathbb{Z}/3$ with operations

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b)(c, d) = (ac, ad + bc).$$

Then R is a commutative ring with identity $(1, 0)$. Since $(0, 1)$ is a non-zero nilpotent element, R is not reduced.

45.7. DEFINITION. 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, $ba \in I$.

45.8. THEOREM (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 $\{r \in R : rS \subseteq I\}$.

45.9. LEMMA. *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 45.8. 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 $a \in A$, $M \subsetneq A$. Similarly, since $b \in B$, $M \subsetneq B$. Moreover, $AB \subseteq M$. Since $x \in A \cap B$, $x^2 \in AB \subseteq M$. Since M is reduced, $x \in M$, a contradiction. \square

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

§ 46. Project: Kolchin's theorem

In this section it will be useful to consider non-unitary algebras.

46.1. DEFINITION. Let A be an algebra (possibly without one). An element $a \in A$ is said to be **nilpotent** if $a^n = 0$ for some $n \geq 1$. The algebra A is said to be **nil** if every element $a \in A$ is nilpotent.

Nilpotent elements are also called nil elements.

46.2. EXAMPLE. Let $A = M_2(\mathbb{R})$. Then $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent.

46.3. DEFINITION. An algebra A is said to be **nilpotent** if there exists $n \geq 1$ such that every product $a_1 a_2 \cdots a_n$ of n elements of A is zero.

Nilpotent algebras are trivially nil, whereas nil algebras may not be nilpotent.

46.4. EXERCISE. Give an example of a nil algebra that is not nilpotent.

Note that nil algebras cannot be unitary.

46.5. EXERCISE. Let A be an algebra. There exists an algebra B with one 1_B and an ideal I of B such that $B/I \simeq \mathbb{C}$ and $I \simeq A$.

46.6. EXERCISE. Let A_1, \dots, A_k be algebras. Prove that the ideals of $A_1 \times \cdots \times A_k$ are of the form $I_1 \times \cdots \times I_k$, where each I_j is an ideal of A_j .

46.7. EXERCISE. Prove that the non-zero ideals of $\prod_{i=1}^k M_{n_i}(\mathbb{C})$ are unitary algebras.

46.8. PROPOSITION. *Let A be non-zero algebra (possibly without one). If A does not have non-zero nilpotent ideals, then A is a unitary algebra.*

PROOF. Let B be a unitary algebra such that there exists an ideal I of B with $B/I \simeq \mathbb{C}$ and $I \simeq A$ (see Exercise 46.5). Let J be a nilpotent ideal of B . Since $J \cap I \subseteq I$ is a nilpotent ideal of A , $J \cap I = \{0\}$. Thus

$$J \simeq J/(J \cap I) \simeq (I + J)/I$$

is a nilpotent ideal of $B/I \simeq \mathbb{C}$. Thus $J = \{0\}$ and hence B is semisimple. By Artin–Wedderburn, $B \simeq \prod_{i=1}^k M_{n_i}(\mathbb{C})$. Since A is isomorphic to an ideal of B , Exercise 46.7 shows that A is a unitary algebra. \square

Now we prove another nice result of Wedderburn:

46.9. THEOREM (Wedderburn). *Let A be a complex finite-dimensional algebra. If A is generated (as a vector space) by nilpotent elements, then A is nilpotent.*

We shall need a lemma.

46.10. LEMMA. *The vector space $M_n(\mathbb{C})$ does not have a basis of nilpotent matrices.*

PROOF. If $\{A_1, \dots, A_{n^2}\}$ is a basis of $M_n(\mathbb{C})$ consisting of nilpotent matrices, then there exist $\lambda_1, \dots, \lambda_{n^2} \in \mathbb{C}$ such that

$$(46.1) \quad E_{11} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \sum_{i=1}^{n^2} \lambda_i A_i.$$

Note $\text{trace}(A_i) = 0$ for all $i \in \{1, \dots, n\}$, as every A_i is nilpotent. Apply trace to (46.1) to obtain that $1 = \text{trace}(E_{11}) = \sum \lambda_i \text{trace}(A_i) = 0$, a contradiction. \square

Now we prove Wedderburn's theorem. Note that the theorem can be extended to any algebraically closed field. We state and prove Wedderburn's theorem in the case of complex numbers to simplify the presentation.

PROOF OF THEOREM 46.9. We proceed by induction on $\dim A$. If $\dim A = 1$ and there exists a nilpotent element $a \in A$ such that $\{a\}$ is a basis of A , then A is nilpotent, as every element of A is nilpotent, as it is of the form λa for some $\lambda \in \mathbb{C}$.

Assume now that $\dim A > 1$. Since $J(A)$ is nilpotent, $J(A)^n = \{0\}$ for some n .

If $J(A) = A$, the result trivially holds.

If $J(A) \neq \{0\}$, $\dim A/J(A) < \dim A$ and hence $A/J(A)$ is nilpotent by the inductive hypothesis, say $(A/J(A))^m = \{0\}$. Let

$$\pi: A \rightarrow A/J(A)$$

be the canonical map and $N = nm$. We claim that $A^N = \{0\}$. Let $a_1, \dots, a_N \in A$. Write $a_1 \cdots a_N = x_1 \cdots x_n$ for some $x_1 \cdots x_n \in A$. For example,

$$\begin{aligned} x_1 &= a_1 a_2 \cdots a_m, \\ x_2 &= a_{m+1} a_{m+2} \cdots a_{2m}, \\ &\vdots \end{aligned}$$

Since

$$\pi(x_1) = \pi(a_1 a_2 \cdots a_m) = \pi(a_1) \pi(a_2) \cdots \pi(a_m) = 0,$$

it follows that $x_1 \in J(A)$. Similarly, $\pi(x_j) \in J(A)$ for every $j \in \{1, \dots, n\}$. Thus,

$$a_1 a_2 \cdots a_N = x_1 x_2 \cdots x_n \in J(A)^n = \{0\}.$$

Thus A is nilpotent.

If $J(A) = \{0\}$, then A is semisimple. By Artin–Wedderburn, $A \simeq \prod_{i=1}^k M_{n_i}(\mathbb{C})$, a contradiction to the previous lemma. \square

46.11. DEFINITION. Let $V = \mathbb{C}^n$ (column vectors). A **complete flag** in V is a sequence (V_1, V_2, \dots, V_n) of vector spaces such that

$$\{0\} \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_n = V.$$

If (V_1, \dots, V_n) is a complete flag, then $\dim V_i = i$ for all $i \in \{1, \dots, n\}$. Let $\{e_1, \dots, e_n\}$ be the standard basis of \mathbb{C}^n . The **standard flag** is defined as the sequence (E_1, \dots, E_n) , where $E_i = \langle e_1, \dots, e_i \rangle$ for all $i \in \{1, \dots, n\}$.

Note that $\mathbf{GL}_n(\mathbb{C})$ acts on the set of complete flags of V by

$$g \cdot (V_1, \dots, V_n) = (T_g(V_1), \dots, T_g(V_n)),$$

where $T_g: V \rightarrow V$, $x \mapsto gx$.

The action is **transitive**, which means that if (V_1, \dots, V_n) is a complete flag, then there exists $g \in \mathbf{GL}_n(\mathbb{C})$ such that

$$g \cdot (E_1, \dots, E_n) = (V_1, \dots, V_n).$$

In fact, the matrix $g = (v_1|v_2|\dots|v_n)$, where $\{v_1, \dots, v_n\}$ is a basis of V , satisfies $ge_i = v_i$ for all $i \in \{1, \dots, n\}$.

Let $B_n(\mathbb{C})$ be the stabilizer

$$G_{(E_1, \dots, E_n)} = \{g \in \mathbf{GL}_n(\mathbb{C}) : T_g(E_i) = E_i \text{ for all } i\} = \{(b_{ij}) : b_{ij} = 0 \text{ if } i > j\}$$

of the standard flag. Then $B_n(\mathbb{C})$ is known as the **Borel subgroup**.

Let $U_n(\mathbb{C})$ be the subgroup of $\mathbf{GL}_n(\mathbb{C})$ of matrices (u_{ij}) such that

$$u_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i > j. \end{cases}$$

Let $T_n(\mathbb{C})$ be the subgroup of $\mathbf{GL}_n(\mathbb{C})$ diagonal matrices.

46.12. PROPOSITION. $B_n(\mathbb{C}) = U_n(\mathbb{C}) \rtimes T_n(\mathbb{C})$.

PROOF. It is trivial that $U_n(\mathbb{C}) \cap T_n(\mathbb{C}) = \{I\}$, where I is the $n \times n$ identity matrix. Clearly, $U_n(\mathbb{C})$ is a subgroup of $B_n(\mathbb{C})$. To prove that $U_n(\mathbb{C})$ is normal in $B_n(\mathbb{C})$ note that $U_n(\mathbb{C})$ is the kernel of the group homomorphism

$$f: B_n(\mathbb{C}) \rightarrow T_n(\mathbb{C}), \quad (b_{ij}) \mapsto \begin{pmatrix} b_{11} & & & \\ & b_{22} & & \\ & & \ddots & \\ & & & b_{nn} \end{pmatrix}.$$

It remains to show that $B_n(\mathbb{C}) = U_n(\mathbb{C})T_n(\mathbb{C})$. Let us prove that $B_n(\mathbb{C}) \subseteq U_n(\mathbb{C})T_n(\mathbb{C})$, as the other inclusion is trivial. Let $b \in B_n(\mathbb{C})$. Then $bf(b)^{-1} \in \ker f = U_n(\mathbb{C})$ and therefore $b = (bf(b)^{-1})f(b) \in U_n(\mathbb{C})T_n(\mathbb{C})$. \square

46.13. DEFINITION. A matrix $a \in \mathbf{GL}_n(\mathbb{C})$ is said to be **unipotent** if its characteristic polynomial is of the form $(X - 1)^n$.

The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is unipotent, as its characteristic polynomial is $(X - 1)^2$.

46.14. DEFINITION. A subgroup G of $\mathbf{GL}_n(\mathbb{C})$ is said to be **unipotent** if each $g \in G$ is unipotent.

Now an application of Wedderburn's theorem:

46.15. PROPOSITION. Let G be a unipotent subgroup of $\mathbf{GL}_n(\mathbb{C})$. Then there exists a non-zero $v \in \mathbb{C}^n$ such that $gv = v$ for all $g \in G$.

PROOF. Without loss of generality, we may assume that G is non-trivial. Let V be the subspace of $\mathbb{C}^{n \times n}$ generated by $\{g - I : g \in G\}$. If $g \in G$, then $(g - I)^n = 0$, as g is unipotent. Thus, every element of V is nilpotent. If $g, h \in G$, then

$$(g - I)(h - I) = (gh - I) - (g - I) - (h - I) \in V.$$

This means that V is closed under multiplication and hence V is an algebra generated (as a vector space) by nilpotent elements. By Wedderburn's theorem, V is nilpotent. Let m be minimal such that $(g_1 - I) \cdots (g_m - I) = 0$ for all $g_1, \dots, g_m \in G$. The minimality of m implies that there exist $h_1, \dots, h_{m-1} \in G$ such that

$$(h_1 - I) \cdots (h_{m-1} - I) \neq 0.$$

In particular, there exists a non-zero $w \in C^n$ such that $v = (h_1 - I) \cdots (h_{m-1} - I)w \neq 0$. For every $g \in G$,

$$(g - I)v = (g - I)(h_1 - I) \cdots (h_{m-1} - I)w = 0$$

and hence $gv = v$. □

46.16. THEOREM (Kolchin). *Every unipotent subgroup of $\mathbf{GL}_n(\mathbb{C})$ is conjugate to some subgroup of $U_n(\mathbb{C})$.*

PROOF. Let G be an unipotent subgroup of $\mathbf{GL}_n(\mathbb{C})$. Assume first that there exists a complete flag (V_1, \dots, V_n) of \mathbb{C}^n such that $G \subseteq G_{(V_1, \dots, V_n)}$. Let $g \in \mathbf{GL}_n(\mathbb{C})$ be such that $g \cdot (E_1, \dots, E_n) = (V_1, \dots, V_n)$. Then

$$G \subseteq G_{g \cdot (E_1, \dots, E_n)} = gG_{(E_1, \dots, E_n)}g^{-1} = gB_n(\mathbb{C})g^{-1}.$$

Since every unipotent element of $B_n(\mathbb{C})$ belongs to $U_n(\mathbb{C})$, it follows that

$$G \subseteq gU_n(\mathbb{C})g^{-1}.$$

We claim that $G \subseteq G_{(V_1, \dots, V_n)}$ for some complete flag (V_1, \dots, V_n) . We proceed by induction on n . If $n = 1$, the result is trivial. Assume the result holds for $n - 1$. By the previous proposition, there exists a non-zero $v \in \mathbb{C}^n$ such that $gv = v$ for all $g \in G$. Let $Q = \mathbb{C}^n / \langle v \rangle$ and $\pi: \mathbb{C}^n \rightarrow Q$ be the canonical map. Then $\dim Q = n - 1$. The group G acts on Q by

$$g \cdot (w + \langle v \rangle) = gw + \langle v \rangle.$$

The action is well-defined: if $w + \langle v \rangle = w_1 + \langle v \rangle$, then $w - w_1 = \lambda v$ for some $\lambda \in \mathbb{C}$. This implies that

$$gw - gw_1 = g(w - w_1) = \lambda(gv) = \lambda v \in \langle v \rangle$$

and hence $gw + \langle v \rangle = gw_1 + \langle v \rangle$.

By the inductive hypothesis, G stabilizes a complete flag (Q_1, \dots, Q_{n-1}) , where

$$Q_1 = \langle \pi(v_1) \rangle, \quad Q_2 = \langle \pi(v_1), \pi(v_2) \rangle, \quad \dots \quad Q_{n-1} = \langle \pi(v_1), \dots, \pi(v_{n-1}) \rangle.$$

Let

$$W_0 = \langle v \rangle, \quad W_1 = \langle v, v_1 \rangle, \quad W_2 = \langle v, v_1, v_2 \rangle, \quad \dots \quad W_{n-1} = \langle v, v_1, \dots, v_{n-1} \rangle.$$

Since (Q_1, \dots, Q_{n-1}) is a complete flag, the set $\{\pi(v_j) : 1 \leq j \leq n-1\}$ is linearly independent. We claim that $\{v, v_1, \dots, v_{n-1}\}$ is linearly independent. In fact, since $v \neq 0$, one obtains that

$$\sum_{i=1}^{n-1} \lambda_i v_i + \lambda v = 0 \implies \sum_{i=1}^{n-1} \lambda_i \pi(v_i) = 0 \implies \lambda_1 = \dots = \lambda_{n-1} = 0 \implies \lambda = 0.$$

Thus $\dim W_i = i + 1$ for all i .

Let $g \in G$. Clearly, $gW_0 \subseteq W_0$, as $gv = v$. Let $j \in \{1, \dots, n-1\}$. There exist $\lambda_1, \dots, \lambda_j \in \mathbb{C}$ such that $\pi(gv_j) = \sum_{i \leq j} \lambda_i \pi(v_i)$. This means that

$$gv_j - \sum_{i \leq j} \lambda_i v_i = \lambda v \in \langle v \rangle$$

for some $\lambda \in \mathbb{C}$. In particular,

$$gv_j = \sum_{i \leq j} \lambda_i v_i + \lambda v \in \langle v, v_1, \dots, v_j \rangle = W_j.$$

Therefore, $G \subseteq G_{(W_0, \dots, W_{n-1})}$. \square

The ideas behind the theorem are somewhat connected to Sylow's theory. The key is to consider an explicit version of Sylow's theorem for the group $\mathbf{GL}_n(p)$ of invertible matrices with coefficients in the field \mathbb{F}_p with p elements.

A group G acts linearly on a vector space V if $g \cdot (v + w) = g \cdot v + g \cdot w$ for all $g \in G$ and $v, w \in V$. Proposition 46.15 has the following version:

46.17. PROPOSITION. *Let P be a finite p -group acting on a finite-dimensional \mathbb{F}_p -vector space V linearly. Then there exists a non-zero $v \in V$ such that $x \cdot v = v$ for all $x \in P$.*

PROOF. Let $n = \dim V$. There are $p^n - 1$ non-zero vectors in V . Since the action is linear, P acts on $X = V \setminus \{0\}$. We decompose V into orbits and collect those orbits with only one element, say

$$X = X_0 \cup O(v_1) \cup \dots \cup O(v_m),$$

where $|O(v_j)| \geq 2$ for all $j \in \{1, \dots, m\}$. Since p divides the order of each $O(v_j)$ and $|X| = p^n - 1$ is not divisible by p , it follows that $X_0 \neq \emptyset$. In particular, there exists $v \in V$ such that $x \cdot v = v$ for all $x \in G$. \square

The analog of Kolchin's theorem is the following result:

46.18. PROPOSITION. *Every p -subgroup of $\mathbf{GL}_n(p)$ is conjugate to a subgroup of the unipotent subgroup $U_n(p)$.*

SKETCH OF THE PROOF. Let P be a p -subgroup of $\mathbf{GL}_n(p)$. Then P acts linearly on an n -dimensional \mathbb{F}_p -vector space V by left multiplication. The previous proposition implies that there exists a non-zero $v_1 \in V$ such that $xv_1 = v_1$ for all $x \in P$. Let $V_1 = \langle v_1 \rangle$. The group P acts on the $(n - 1)$ -dimensional vector space V/V_1 by

$$x \cdot (v + V_1) = xv + V_1.$$

This action is well-defined. As before, there exists a non-zero vector of V/V_1 fixed by P . Thus there exists $v_2 \in V \setminus V_1$ such that $xv_2 + V_1 = v_2 + V_1$. Note that $\{v_1, v_2\}$ is linearly independent, as applying the canonical map $V \rightarrow V/V_1$ to $\alpha v_1 + \beta v_2 = 0$ one obtains that $\beta = 0$ and therefore $\alpha = 0$. This process produces a basis $\{v_1, \dots, v_n\}$ of V and a sequence $\{0\} \subsetneq V_1 \subsetneq V_2 \subsetneq \dots \subsetneq V_n = V$, where $V_j = \langle v_1, \dots, v_j \rangle$ for all $j \in \{1, \dots, n\}$. Moreover, $PV_j \subseteq V_j$ and $Pv_j = v_j + V_{j-1}$ for all j . This means precisely that in the basis $\{v_1, \dots, v_n\}$ every element of P is an upper triangular matrix with ones in the main diagonal. \square

Proposition 46.18 is deeply connected to Sylow's theorems.

46.19. EXERCISE. Prove that the normalizer of $U_n(p)$ in $\mathbf{GL}_n(p)$ is the Borel subgroup $B_n(p)$ of upper triangular matrices.

Now we have the following explicit Sylow theory for $\mathbf{GL}_n(p)$. The first two Sylow theorems appear in the following result.

46.20. EXERCISE. Prove that $U_n(p)$ is a Sylow p -subgroup of $\mathbf{GL}_n(p)$.

What about the third Sylow's theorem? First, note that the number n_p of conjugates of $U_n(p)$ in $\mathbf{GL}_n(p)$ is the number of complete flags in \mathbb{F}_p^n .

46.21. EXERCISE. Prove that $n_p \equiv 1 \pmod{p}$.

§ 47. Project: Passman's theorem

Let K be a field and G be a group. A unit $u \in K[G]$ is said to be **trivial** if $u = \lambda g$ for some $\lambda \in K \setminus \{0\}$ and $g \in G$.

47.1. EXERCISE. Prove that $\mathbb{C}[C_2]$ and $\mathbb{C}[C_5]$ have non-trivial units.

The following question is usually attributed to Kaplansky.

47.2. QUESTION (Units in groups algebras). Let K be a field and G be a torsion-free group. Is it true that all units of $K[G]$ are trivial?

Question 47.2 was negatively answered by Gardam.

47.3. THEOREM (Gardam). Let \mathbb{F}_2 be the field of two elements. Consider the elements $x = a^2$, $y = b^2$ and $z = (ab)^2$ of P and let

$$\begin{aligned} p &= (1+x)(1+y)(1+z^{-1}), & q &= x^{-1}y^{-1} + x + y^{-1}z + z, \\ r &= 1 + x + y^{-1}z + xyz, & s &= 1 + (x + x^{-1} + y + y^{-1})z^{-1}. \end{aligned}$$

Then $u = p + qa + rb + sab$ is a non-trivial unit in $\mathbb{F}_2[P]$.

PROOF. See [11]. □

47.4. DEFINITION. A ring R is **reduced** if for all $r \in R$ such that $r^2 = 0$ one has $r = 0$.

Integral domains and boolean rings are reduced. The ring $\mathbb{Z}/8$ of integers modulo eight and $M_2(\mathbb{R})$ are not reduced.

47.5. EXAMPLE. The ring over the abelian group \mathbb{Z}^n with multiplication

$$(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1b_1, \dots, a_nb_n)$$

is reduced.

The structure of reduced rings is described by the Andrunakevic-Rjabuhin theorem. It states that a ring is reduced if and only if it is a subdirect products of domains. See [12, 3.20.5] for a proof.

47.6. QUESTION (Reduced group algebras). Let K be a field and G be a torsion-free group. Is it true that $K[G]$ is reduced?

Recall that if R is a unitary ring, one proves that the Jacobson radical $J(R)$ is the set of elements x such that $1 + \sum_{i=1}^n r_i x s_i$ is invertible for all n and all $r_i, s_i \in R$.

47.7. QUESTION (Semisimple group algebras). Let K be a field and G be a torsion-free group. Is it true that $J(K[G]) = \{0\}$ if G is non-trivial?

Recall that an element e of a ring is said to be **idempotent** if $e^2 = e$. Examples of idempotents are 0 and 1 and these are known as the **trivial idempotents**.

47.8. QUESTION (Idempotents in group algebras). Let G be a torsion-free group and $\alpha \in K[G]$ be an idempotent. Is it true that $\alpha \in \{0, 1\}$?

47.9. EXERCISE. Prove that if $K[G]$ has no zero-divisors and $\alpha \in K[G]$ is an idempotent, then $\alpha \in \{0, 1\}$.

47.10. EXERCISE. Let K be a field of characteristic two. Prove that $K[C_4]$ contains non-trivial zero divisors and every idempotent of $K[C_4]$ is trivial. What happens if the characteristic of K is not two?

For completeness, let us recall the following important question.

47.11. QUESTION (Zero divisors in group algebras). Let K be a field and G be a torsion-free group. Is it true that $K[G]$ is a domain?

Our goal is to prove the following implications:

$$47.7 \Leftarrow 47.2 \Rightarrow 47.6 \Longleftrightarrow 47.11$$

We first prove that an affirmative solution to Question 47.2 yields a solution to Question 47.6.

47.12. THEOREM. *Let K be a field of characteristic $\neq 2$ and G be a non-trivial group. Assume that $K[G]$ has only trivial units. Then $K[G]$ is reduced.*

PROOF. Let $\alpha \in K[G]$ be such that $\alpha^2 = 0$. We claim that $\alpha = 0$. Since $\alpha^2 = 0$,

$$(1 - \alpha)(1 + \alpha) = 1 - \alpha^2 = 1,$$

it follows that $1 - \alpha$ is a unit of $K[G]$. Since units of $K[G]$ are trivial, there exist $\lambda \in K \setminus \{0\}$ and $g \in G$ such that $1 - \alpha = \lambda g$. We claim that $g = 1$. If not,

$$0 = \alpha^2 = (1 - \lambda g)^2 = 1 - 2\lambda g + \lambda^2 g^2,$$

a contradiction. Therefore $g = 1$ and hence $\alpha = 1 - \lambda \in K$. Since K is a field, one concludes that $\alpha = 0$. \square

47.13. EXERCISE. What happens in Theorem 47.12 if K is a field of characteristic two?

We now prove that an affirmative solution to Question 47.2 also yields a solution to Question 47.7.

47.14. THEOREM. *Let K be a field and G be a non-trivial group. Assume that $K[G]$ has only trivial units. If $|K| > 2$ or $|G| > 2$, then $J(K[G]) = \{0\}$.*

PROOF. Let $\alpha \in J(K[G])$. There exist $\lambda \in K \setminus \{0\}$ and $g \in G$ such that $1 - \alpha = \lambda g$. We claim that $g = 1$. Assume $g \neq 1$. If $|K| \geq 3$, then there exist $\mu \in K \setminus \{0, 1\}$ such that

$$1 - \alpha\mu = 1 - \mu + \lambda\mu g$$

is a non-trivial unit, a contradiction. If $|G| \geq 3$, there exists $h \in G \setminus \{1, g^{-1}\}$ such that

$$1 - \alpha h = 1 - h + \lambda gh$$

is a non-trivial unit, a contradiction. Thus $g = 1$ and hence $\alpha = 1 - \lambda \in K$. Therefore $1 + \alpha h$ is a trivial unit for all $h \neq 1$ and hence $\alpha = 0$. \square

47.15. EXERCISE. Prove that if $G = \langle g \rangle \simeq \mathbb{Z}/2$, then $J(\mathbb{F}_2[G]) = \{0, g - 1\} \neq \{0\}$.

We now want to prove that an affirmative answer to Question 47.6 yields an affirmative answer to Question 47.11. We first need some preliminaries.

For a group G we consider

$$\Delta(G) = \{g \in G : (G : C_G(g)) < \infty\}.$$

47.16. EXERCISE. Prove that $\Delta(\Delta(G)) = \Delta(G)$.

47.17. PROPOSITION. *If G is a group, then $\Delta(G)$ is a characteristic subgroup of G .*

PROOF. We first prove that $\Delta(G)$ is a subgroup of G . If $x, y \in \Delta(G)$ and $g \in G$, then

$$g(xy^{-1})g^{-1} = (g x g^{-1})(g y g^{-1})^{-1}.$$

Moreover, $1 \in \Delta(G)$. Let us show now that $\Delta(G)$ is characteristic in G . If $f \in \text{Aut}(G)$ and $x \in G$, then, since

$$f(g x g^{-1}) = f(g) f(x) f(g)^{-1},$$

it follows that $f(x) \in \Delta(G)$. □

47.18. EXERCISE. Prove that if $G = \langle r, s : s^2 = 1, s r s = r^{-1} \rangle$ is the infinite dihedral group, then $\Delta(G) = \langle r \rangle$.

The following exercise uses the transfer map and is need in Proposition 47.20.

47.19. EXERCISE. If G is a group such that $Z(G)$ has finite index n , then $(gh)^n = g^n h^n$ for all $g, h \in G$.

47.20. PROPOSITION. *If G is a torsion-free group such that $\Delta(G) = G$, then G is abelian.*

PROOF. Let $x, y \in G = \Delta(G)$ and $S = \langle x, y \rangle$. The group $Z(S) = C_S(x) \cap C_S(y)$ has finite index, say n , in S . By Exercise 47.19, the map $S \rightarrow Z(S)$, $s \mapsto s^n$, is a group homomorphism. Thus

$$[x, y]^n = (x y x^{-1} y^{-1})^n = x^n y^n x^{-n} y^{-n} = 1$$

as $x^n \in Z(S)$. Since G is torsion-free, $[x, y] = 1$. □

47.21. LEMMA (Neumann). *Let H_1, \dots, H_m be subgroups of G . Assume there are finitely many elements $a_{ij} \in G$, $1 \leq i \leq m$, $1 \leq j \leq n$, such that*

$$G = \bigcup_{i=1}^m \bigcup_{j=1}^n H_i a_{ij}.$$

Then some H_i has finite index in G .

PROOF. We proceed by induction on m . The case $m = 1$ is trivial. Let us assume that $m \geq 2$. If $(G : H_1) = \infty$, there exists $b \in G$ such that

$$H_1 b \cap \left(\bigcup_{j=1}^n H_1 a_{1j} \right) = \emptyset.$$

Since $H_1b \subseteq \bigcup_{i=2}^m \bigcup_{j=1}^n H_i a_{ij}$, it follows that

$$H_1 a_{1k} \subseteq \bigcup_{i=2}^m \bigcup_{j=1}^n H_i a_{ij} b^{-1} a_{1k}.$$

Hence G can be covered by finitely many cosets of H_2, \dots, H_m . By the inductive hypothesis, some of these H_j has finite index in G . \square

We now consider a projection operator of group algebras. If G is a group and H is a subgroup of G , let

$$\pi_H: K[G] \rightarrow K[H], \quad \pi_H \left(\sum_{g \in G} \lambda_g g \right) = \sum_{g \in H} \lambda_g g.$$

If R and S are rings, a (R, S) -bimodule is an abelian group M that is both a left R -module and a right S -module and the compatibility condition

$$(rm)s = r(ms)$$

holds for all $r \in R$, $s \in S$ and $m \in M$.

47.22. EXERCISE. Let G be a group and H be a subgroup of G . Prove that if $\alpha \in K[G]$, then π_H is a $(K[H], K[H])$ -bimodule homomorphism with usual left and right multiplications,

$$\pi_H(\beta\alpha\gamma) = \beta\pi_H(\alpha)\gamma$$

for all $\beta, \gamma \in K[H]$.

47.23. LEMMA. Let X be a left transversal of H in G . Every $\alpha \in K[G]$ can be written uniquely as

$$\alpha = \sum_{x \in X} x\alpha_x,$$

where $\alpha_x = \pi_H(x^{-1}\alpha) \in K[H]$.

PROOF. Let $\alpha \in K[G]$. Since $\text{supp } \alpha$ is finite, $\text{supp } \alpha$ is contained in finitely many cosets of H , say x_1H, \dots, x_nH , where each x_j belongs to X . Write $\alpha = \alpha_1 + \dots + \alpha_n$, where $\alpha_i = \sum_{g \in x_iH} \lambda_g g$. If $g \in x_iH$, then $x_i^{-1}g \in H$ and hence

$$\alpha = \sum_{i=1}^n x_i(x_i^{-1}\alpha_i) = \sum_{x \in X} x\alpha_x$$

with $\alpha_x \in K[H]$ for all $x \in X$. For the uniqueness, note that for each $x \in X$ the previous exercise implies that

$$\pi_H(x^{-1}\alpha) = \pi_H \left(\sum_{y \in X} x^{-1}y\alpha_y \right) = \sum_{y \in X} \pi_H(x^{-1}y)\alpha_y = \alpha_x,$$

as

$$\pi_H(x^{-1}y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases} \quad \square$$

47.24. LEMMA. Let G be a group and H be a subgroup of G . If I is a non-zero left ideal of $K[G]$, then $\pi_H(I) \neq \{0\}$.

PROOF. Let X be a left transversal of H in G and $\alpha \in I \setminus \{0\}$. By Lemma 47.23 we can write $\alpha = \sum_{x \in X} x\alpha_x$ with $\alpha_x = \pi_H(x^{-1}\alpha) \in K[H]$ for all $x \in X$. Since $\alpha \neq 0$, there exists $y \in X$ such that $0 \neq \alpha_y = \pi_H(y^{-1}\alpha) \in \pi_H(I)$ ($y^{-1}\alpha \in I$ since I is a left ideal). \square

Lemma 47.24 can also be proved directly, without using Lemma 47.23. The proof goes as follows: if $\alpha \neq 0$, then by taking g in the support of α , we have that $\pi_H(g^{-1}\alpha) \neq 0$.

47.25. EXERCISE. Let G be a group, H be a subgroup of G and $\alpha \in K[H]$. The following statements hold:

- 1) α is invertible in $K[H]$ if and only if α is invertible in $K[G]$.
- 2) α is a zero divisor of $K[H]$ if and only if α is a zero divisor of $K[G]$.

47.26. LEMMA (Passman). Let G be a group and $\gamma_1, \gamma_2 \in K[G]$ be such that $\gamma_1 K[G] \gamma_2 = \{0\}$. Then $\pi_{\Delta(G)}(\gamma_1) \pi_{\Delta(G)}(\gamma_2) = \{0\}$.

PROOF. It is enough to show that $\pi_{\Delta(G)}(\gamma_1) \gamma_2 = \{0\}$, as in this case

$$\{0\} = \pi_{\Delta(G)}(\pi_{\Delta(G)}(\gamma_1) \gamma_2) = \pi_{\Delta(G)}(\gamma_1) \pi_{\Delta(G)}(\gamma_2).$$

Write $\gamma_1 = \alpha_1 + \beta_1$, where

$$\begin{aligned} \alpha_1 &= a_1 u_1 + \cdots + a_r u_r, & u_1, \dots, u_r &\in \Delta(G), \\ \beta_1 &= b_1 v_1 + \cdots + b_s v_s, & v_1, \dots, v_s &\notin \Delta(G), \\ \gamma_2 &= c_1 w_1 + \cdots + c_t w_t, & w_1, \dots, w_t &\in G. \end{aligned}$$

The subgroup $C = \bigcap_{i=1}^r C_G(u_i)$ has finite index in G . Assume that

$$0 \neq \pi_{\Delta(G)}(\gamma_1) \gamma_2 = \alpha_1 \gamma_2.$$

Let $g \in \text{supp}(\alpha_1 \gamma_2)$. If v_i is a conjugate in G of some $g w_j^{-1}$, let $g_{ij} \in G$ be such that $g_{ij}^{-1} v_i g_{ij} = g w_j^{-1}$. If v_i and $g w_j^{-1}$ are not conjugate, we take $g_{ij} = 1$.

For every $x \in C$ it follows that $\alpha_1 \gamma_2 = (x^{-1} \alpha_1 x) \gamma_2$. Since

$$x^{-1} \gamma_1 x \gamma_2 \in x^{-1} \gamma_1 K[G] \gamma_2 = 0,$$

it follows that

$$\begin{aligned} (a_1 u_1 + \cdots + a_r u_r) \gamma_2 &= \alpha_1 \gamma_2 = x^{-1} \alpha_1 x \gamma_2 = -x^{-1} \beta_1 x \gamma_2 \\ &= -x^{-1} (b_1 v_1 + \cdots + b_s v_s) x (c_1 w_1 + \cdots + c_t w_t). \end{aligned}$$

Now $g \in \text{supp}(\alpha_1 \gamma_2)$ implies that there exist i, j such that $g = x^{-1} v_i x w_j$. Thus v_i and $g w_j^{-1}$ are conjugate and hence $x^{-1} v_i x = g w_j^{-1} = g_{ij}^{-1} v_i g_{ij}$, that is $x \in C_G(v_i) g_{ij}$. This proves that

$$C \subseteq \bigcup_{i,j} C_G(v_i) g_{ij}.$$

Since C has finite index in G , it follows that G can be covered by finitely many cosets of the $C_G(v_i)$. Every $v_i \notin \Delta(G)$, so each $C_G(v_i)$ has infinite index in G , a contradiction to Neumann's lemma. \square

47.27. EXERCISE. Let K be a field and G be a torsion-free abelian group. Prove that $K[G]$ has no non-zero divisors.

47.28. THEOREM (Passman). *Let K be a field and G be a torsion-free group. If $K[G]$ is reduced, then $K[G]$ is a domain.*

PROOF. Assume that $K[G]$ is not a domain. Let $\gamma_1, \gamma_2 \in K[G] \setminus \{0\}$ be such that $\gamma_2\gamma_1 = 0$. If $\alpha \in K[G]$, then

$$(\gamma_1\alpha\gamma_2)^2 = \gamma_1\alpha\gamma_2\gamma_1\alpha\gamma_2 = 0$$

and thus $\gamma_1\alpha\gamma_2 = 0$, as $K[G]$ is reduced. In particular, $\gamma_1K[G]\gamma_2 = \{0\}$. Let I be the left ideal of $K[G]$ generated by γ_2 . Since $I \neq \{0\}$, it follows from Lemma 47.24 that $\pi_{\Delta(G)}(I) \neq \{0\}$. Hence $\pi_{\Delta(G)}(\beta\gamma_2) \neq \{0\}$ for some $\beta \in K[G]$. Similarly, $\pi_{\Delta(G)}(\gamma_1\alpha) \neq \{0\}$ for some $\alpha \in K[G]$. Since

$$\gamma_1\alpha K[G]\beta\gamma_2 \subseteq \gamma_1K[G]\gamma_2 = \{0\},$$

it follows that $\pi_{\Delta(G)}(\gamma_1\alpha)\pi_{\Delta(G)}(\beta\gamma_2) = \{0\}$ by Passman's lemma. Hence $K[\Delta(G)]$ has zero divisors, a contradiction since $\Delta(G)$ is an abelian group. \square

§ 48. Project: Gardam's theorem

The unit problem is still open for fields of characteristic zero. However, it was recently solved by Gardam [11] in the case of K the field of two elements. We will present Gardam's theorem as a computer calculation. We will use GAP [9].

48.1. LEMMA. *The group $G = \langle a, b : a^{-1}b^2a = b^{-2}, b^{-1}a^2b = a^{-2} \rangle$ is torsion-free. Moreover, the subgroup $N = \langle a^2, b^2, (ab)^2 \rangle$ is normal in G , free-abelian of rank three and $G/N \simeq C_2 \times C_2$.*

PROOF. We first construct the group.

```
gap> F := FreeGroup(2);;
gap> A := F.1;;
gap> B := F.2;;
gap> rels := [(B^2)^A*B^2, (A^2)^B*A^2];;
gap> G := F/rels;;
gap> a := G.1;;
gap> b := G.2;;
```

Now we construct the subgroup N generated by a^2 , b^2 and $(ab)^2$. It is easy to check that N is normal in G and that $G/N \simeq C_2 \times C_2$. It is even easier to do this with the computer.

```
gap> N := Subgroup(G, [a^2, b^2, (a*b)^2]);;
gap> IsNormal(G, N);
true
gap> StructureDescription(G/N);
"C2 x C2"
```

It is easy to check by hand that N is abelian, and not so easy to do it with the computer. For example,

$$b^{-2}a^2b^{-2} = b^{-1}a^{-2}b = (b^{-1}a^2b)^{-1} = (a^{-2})^{-1} = a^2.$$

We use the computer to show that N is free abelian of rank three.

```
gap> AbelianInvariants(N);
[ 0, 0, 0 ]
```

Let us prove that G is torsion-free. Let $x = a^2$, $y = b^2$ and $z = (ab)^2$. Since $(G : N) = 4$, the group G decomposes as a disjoint union $G = N \cup aN \cup bN \cup (ab)N$. Let $g \in G$ be a non-trivial element of finite order. Since N is torsion-free, $g \in aN \cup bN \cup (ab)N$. Without loss of generality we may assume that $g \in aN$, so $g = an$ for some $n \in N$. Let $\pi : G \rightarrow G/N$ be the canonical map. Since $g \notin N$ and $\pi(g) \in G/N \simeq C_2 \times C_2$,

$$\pi(g^2) = \pi(g)^2 = 1$$

so $g^2 \in N$ and hence $g^2 = 1$, as N is torsion-free. Thus

$$1 = g^2 = (an)^2 = (an)(an) = a^2(a^{-1}na)n = x(a^{-1}na)n.$$

Write $n = x^i y^j z^k$ for some $i, j, k \in \mathbb{Z}$. Then

$$a^{-1}na = (a^{-1}x^i a)(a^{-1}y^j a)(a^{-1}z^k a) = x^i t^{-j} z^{-k}$$

and hence $(a^{-1}na)n = x^{2i}$. Then $1 = g^2 = x(a^{-1}na)n = x^{2i+1}$, a contradiction. \square

Let P be the group generated by

$$a = \begin{pmatrix} 1 & 0 & 0 & 1/2 \\ 0 & -1 & 0 & 1/2 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & -1 & 1/2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The group P appears in the literature with various names. For us P will be the **Promislow group**. It is easy to check that there exists a surjective group homomorphism $G \rightarrow P$.

48.2. EXERCISE. Prove that $G \simeq P$.

A solution to Exercise 48.2 appears in [33].

48.3. THEOREM (Gardam). *Let \mathbb{F}_2 be the field of two elements. Consider the elements $x = a^2$, $y = b^2$ and $z = (ab)^2$ of P and let*

$$\begin{aligned} p &= (1+x)(1+y)(1+z^{-1}), & q &= x^{-1}y^{-1} + x + y^{-1}z + z, \\ r &= 1 + x + y^{-1}z + xyz, & s &= 1 + (x + x^{-1} + y + y^{-1})z^{-1}. \end{aligned}$$

Then $u = p + qa + rb + sab$ is a non-trivial unit in $\mathbb{F}_2[P]$.

PROOF. We claim that the inverse of u is the element $v = p_1 + q_1a + r_1b + s_1ab$, where

$$p_1 = x^{-1}(a^{-1}pa), \quad q_1 = -x^{-1}q, \quad r_1 = -y^{-1}r, \quad s_1 = z^{-1}(a^{-1}sa).$$

We only need to show that $uv = vu = 1$. We will perform this calculation with GAP. We first need to create the group $P = \langle a, b \rangle$.

```
gap> a := [[1,0,0,1/2],[0,-1,0,1/2],[0,0,-1,0],[0,0,0,1]];;
gap> b := [[-1,0,0,0],[0,1,0,1/2],[0,0,-1,1/2],[0,0,0,1]];;
gap> P := Group([a,b]);
```

Now we create the group algebra $F[P]$ and the embedding $P \hookrightarrow F[P]$. The field \mathbb{F}_2 will be $\text{GF}(2)$ and the embedding will be denoted by \mathbf{f} .

```
gap> R := GroupRing(GF(2),P);;
gap> f := Embedding(P, R);;
```

We first need the elements x , y and z that were defined in the statement.

```
gap> x := Image(f, a^2);;
gap> y := Image(f, b^2);;
gap> z := Image(f, (a*b)^2);;
```

Now we define the elements p , q , r and s . Note that the identity of the group algebra \mathbf{R} is $\text{One}(\mathbf{R})$.

```
gap> p := (One(R)+x)*(One(R)+y)*(One(R)+Inverse(z));;
gap> r := One(R)+x+Inverse(y)*z+x*y*z;;
gap> q := Inverse(x)*Inverse(y)+x+Inverse(y)*z+z;;
gap> s := One(R)+(x+Inverse(x)+y+Inverse(y))*Inverse(z);;
```

Rather than trying to compute the inverse of u we will show that $uv = vu = 1$. For that purpose we need to define p_1 , q_1 , r_1 and s_1 .

```
gap> p1 := Inverse(x)*p^Image(f, a);;  
gap> q1 := -Inverse(x)*q;;  
gap> r1 := -Inverse(y)*r;;  
gap> s1 := Inverse(z)*s^Image(f, a);;
```

Now it is time to prove the theorem.

```
gap> u := p+q*a+r*b+s*a*b;;  
gap> v := p1+q1*a+r1*b+s1*a*b;;  
gap> IsOne(u*v);  
true  
gap> IsOne(v*u);  
true
```

This completes the proof of the theorem. □

Our proof of Theorem 48.3 is exactly as that of [11].

48.4. BONUS EXERCISE. Let p be a prime number and \mathbb{F}_p be the field of size p . Use the technique for proving Gardam's theorem to prove Murray's theorem on the existence on non-trivial units in $\mathbb{F}_p[P]$. Reference: [arXiv:2106.02147](#).

§ 49. Project: When a group algebra is prime?

If S is a finite subset of a group G , then we define $\hat{S} = \sum_{x \in S} x$.

49.1. LEMMA. Let N be a finite normal subgroup of G . Then $\hat{N} = \sum_{x \in N} x$ is central in $K[G]$ and $\hat{N}(\hat{N} - |N|1) = 0$.

PROOF. Assume that $N = \{n_1, \dots, n_k\}$. Let $g \in G$. Since $N \rightarrow N, n \mapsto gng^{-1}$, is bijective,

$$g\hat{N}g^{-1} = g(n_1 + \dots + n_k)g^{-1} = gn_1g^{-1} + \dots + gn_kg^{-1} = \hat{N}.$$

Since $nN = N$ if $n \in N$, it follows that $n\hat{N} = \hat{N}$. Thus $\hat{N}\hat{N} = \sum_{j=1}^k n_j\hat{N} = |N|\hat{N}$. \square

If G is a group, let

$$\Delta^+(G) = \{x \in \Delta(G) : x \text{ has finite order}\}.$$

49.2. EXERCISE (Dietzmann's theorem). Let G be a group and $X \subseteq G$ be a finite subset of G closed by conjugation. If there exists n such that $x^n = 1$ for all $x \in X$, then $\langle X \rangle$ is a finite subgroup of G .

49.3. PROPOSITION. If G is a group, then $\Delta^+(G)$ is a characteristic subgroup of G .

PROOF. Clearly, $1 \in \Delta^+(G)$. Let $x, y \in \Delta^+(G)$ and H be the subgroup of G generated by the set C formed by all finite conjugates of x and y . If $|x| = n$ and $|y| = m$, then $c^{nm} = 1$ for all $c \in C$. Since C is finite and closed under conjugation, Dietzmann's theorem (Exercise 49.2) implies that H is finite and hence $H \subseteq \Delta^+(G)$. In particular, $xy^{-1} \in \Delta^+(G)$. It is now clear that $\Delta^+(G)$ is a characteristic subgroup, as for every $f \in \text{Aut}(G)$ and $x \in \Delta^+(G)$ it follows that $f(x) \in \Delta^+(G)$. \square

To prove Connel's theorem we need a lemma.

49.4. LEMMA. Let G be a group and $x \in \Delta^+(G)$. There exists a finite normal subgroup H of G such that $x \in H$.

PROOF. Let H be the subgroup generated by the conjugates of x . Since x has finitely many conjugates, H is finitely generated. Moreover, H is normal in G and it is generated by torsion elements. All these generators of H have the same order, say n . By Dietzmann's theorem (Exercise 49.2), H is finite. \square

Recall that a ring R is said to be **prime** if for $x, y \in R$ such that $xRy = \{0\}$ it follows that $x = 0$ or $y = 0$. Prime rings are non-commutative analogs of domains.

49.5. THEOREM (Connell). Let K be a field of characteristic zero. Let G be a group. The following statements are equivalent:

- 1) $K[G]$ is prime.
- 2) $Z(K[G])$ is prime.
- 3) G does not contain non-trivial finite normal subgroups.
- 4) $\Delta^+(G) = \{1\}$.

PROOF. We first prove that 1) \implies 2). Since $Z(K[G])$ is commutative, we need to prove that there are no non-trivial zero divisors. Let $\alpha, \beta \in Z(K[G])$ be such that $\alpha\beta = 0$. Let $A = \alpha K[G]$ and $B = \beta K[G]$. Since both α and β are central, both A and B are ideals

of $K[G]$. Since $AB = \{0\}$, it follows that either $A = \{0\}$ or $B = \{0\}$, as $K[G]$ is prime by assumption. Thus either $\alpha = 0$ or $\beta = 0$.

We now prove that 2) \implies 3). Let N be a normal finite subgroup of G . By Lemma 49.1, $\hat{N} = \sum_{x \in N} x$ is central in $K[G]$ and $\hat{N}(\hat{N} - |N|1) = 0$. Since $\hat{N} \neq 0$ (recall that K has characteristic zero) and $Z(K[G])$ is a domain, $\hat{N} = |N|1$, that is $N = \{1\}$.

Let us prove that 3) \implies 4). Let $x \in \Delta^+(G)$. By Lemma 49.4, there exists a finite normal subgroup H of G that contains x . By assumption, H is trivial. Hence $x = 1$.

Finally, let us prove that 4) \implies 1). Let A and B be ideals of $K[G]$ such that $AB = \{0\}$. Assume that $B \neq \{0\}$ and let $\beta \in B \setminus \{0\}$. If $\alpha \in A$, then, since

$$\alpha K[G]\beta \subseteq \alpha B \subseteq AB = \{0\},$$

Passman's lemma (see Lemma 47.26) implies that $\pi_{\Delta(G)}(\alpha)\pi_{\Delta(G)}(\beta) = \{0\}$. By assumption, $\Delta^+(G)$ is trivial. Thus $\Delta(G)$ is torsion-free. As $\Delta(\Delta(G)) = \Delta(G)$, it follows from Proposition 47.20 that $\Delta(G)$ is abelian. Therefore $K[\Delta(G)]$ has no zero divisors and therefore $\alpha = 0$. \square

We now need to recall Hopkins–Levitzky's theorem. The theorem states that unitary left artinian rings are left noetherian.

49.6. THEOREM (Connel). *Let K be a field of characteristic zero. If G is a group, then $K[G]$ is left artinian if and only if G is finite.*

PROOF. If G is finite, $K[G]$ is left artinian, as it is a finite-dimensional algebra.

Let us assume that $K[G]$ is left artinian. If $K[G]$ is prime, Wedderburn's theorem implies that $K[G]$ is simple and hence G is trivial (otherwise, $K[G]$ is not simple as the augmentation ideal is a non-zero ideal of $K[G]$).

Since $K[G]$ is left artinian, it is left noetherian by the Hopkins–Levitzky theorem. Thus $K[G]$ admits a composition series. We proceed by induction on the length of this composition series of $K[G]$. If the length is one, $\{0\}$ is the only ideal of $K[G]$ and hence the result follows as $K[G]$ is prime. If we assume the result holds for length n and $K[G]$ is not prime, then, Connel's theorem implies that G contains a finite non-trivial normal subgroup H . The canonical map $K[G] \rightarrow K[G/H]$ implies that $K[G/H]$ is left artinian and has length $< n$. By using the inductive hypothesis, G/H is a finite group. Since H is also finite, it follows that G is finite. \square

§ 50. Project: When a group algebra is local?

50.1. PROPOSITION. Let R be a commutative ring with one. Let $f: G \rightarrow H$ be a group homomorphism with kernel K . Then

$$\varphi: R[G] \rightarrow R[H], \quad \sum \lambda_i g_i \mapsto \sum \lambda_i f(g_i),$$

is a ring homomorphism with kernel the ideal of $R[G]$ generated by $\{k - 1 : k \in K\}$.

PROOF. A direct calculation shows that the map φ is a well-defined ring homomorphism. Let $S = \{k - 1 : k \in K\}$. Then $(S) \subseteq \ker \varphi$.

Let us show that $\ker \varphi \subseteq (S)$. Let $\alpha = \sum r_i g_i \in \ker \varphi$. Then

$$\varphi(\alpha) = \sum r_i f(g_i) = 0.$$

Let $\{Kg_{i_1}, \dots, Kg_{i_k}\}$ be the subset of pairwise distinct cosets of Kg_1, \dots, Kg_n . Write

$$\alpha = \sum \sum s_{ij} k_{ij} g_{i_j}$$

for some $s_{ij} \in R$ and $k_{ij} \in K$. Then

$$(50.1) \quad 0 = \varphi(\alpha) = \sum \sum s_{ij} \varphi(k_{ij} g_{i_j}) = \sum \sum s_{ij} f(g_{i_j}),$$

as $K = \ker f$. Note that

$$f(g_{i_j}) = f(g_{i_k}) \implies g_{i_j} g_{i_k}^{-1} \in K \implies g_{i_j} K = g_{i_k} K.$$

Thus $f(g_{i_j}) \neq f(g_{i_k})$ for $j \neq k$. Since $R[H]$ is a free R -module with basis $\{h : h \in H\}$, Equality (50.1) implies that $\sum_i s_{ij} = 0$ for all j . Thus

$$\alpha = \sum \sum s_{ij} k_{ij} g_{i_j} = \sum \sum s_{ij} (k_{ij} - 1) g_{i_j} \in (S). \quad \square$$

50.2. COROLLARY. Let R be a commutative ring with one. If G is a group and N is a normal subgroup of G , then

$$R[G/N] \simeq R[G]/I,$$

where I is the ideal of $R[G]$ generated by $\{n - 1 : n \in N\}$.

PROOF. Apply the previous proposition to the canonical map $\pi: G \rightarrow G/N$ to get a ring homomorphism $\varphi: R[G] \rightarrow R[G/N]$. The kernel of φ is the ideal I generated by the set

$$\{g - 1 : g \in \ker \pi = N\}.$$

Since π is surjective, φ is surjective. By the first isomorphism theorem, the claim follows. \square

Let K be a field and G be a group. We write $A(K[G])$ to denote the ideal of $K[G]$ generated by the set $\{g - 1 : g \in G\}$. This ideal is known as the **augmentation ideal** of $K[G]$.

50.3. COROLLARY. Let K be a field. Let G be a group and N be a central subgroup of G . If $K[N]$ and $K[G/N]$ are local, then $K[G]$ is local.

PROOF. By Corollary 50.2, $K[G/N] \simeq K[G]/I$, where I is the ideal of $K[G]$ generated by $\{n - 1 : n \in N\}$. Since $N \subseteq Z(G)$, I is central in $K[G]$. Note that

$$I = A(K[N])K[G].$$

Let $\alpha \in A(K[G])$. Since $K[G/N]$ is local, $A(K[G/N])$ is nil by Theorem 26.2. Since

$$K[G]/I \simeq K[G/N],$$

this implies that there exists m such that $\alpha^m \in I$. Since $K[N]$ is local, $A(K[N])$ is nil by Theorem 26.2. Moreover, $K[N]$ is central in $K[G]$, because $N \subseteq Z(G)$. This implies that $I = A(K[N])K[G]$ is also nil. In particular, α is nil. Hence $K[G]$ is nil and therefore $K[G]$ is local by Theorem 26.2. \square

50.4. EXERCISE. Let R be a unitary commutative ring and G be a group. Prove that the map $R[G] \rightarrow R$, $\sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g$, is a surjective ring homomorphism with kernel $A(R[G])$.

50.5. LEMMA. Let K be a field and G be a finite group. The following statements are equivalent:

- 1) $K[G]$ is local.
- 2) $A(K[G]) \subseteq J(K[G])$.
- 3) $A(K[G])$ is nil.
- 4) $A(K[G]) = J(K[G])$.

PROOF. Let us prove that 1) \implies 2). Since $K[G]$ is local, $R \setminus \mathcal{U}(K[G]) = J(K[G])$ by Theorem 26.2. Since $K[G] \setminus \mathcal{U}(K[G])$ contains every proper ideal of $K[G]$,

$$A(K[G]) \subseteq J(K[G]).$$

We now prove that 2) \implies 3). Since G is finite, $K[G]$ is artinian. By Lemma 26.7, $J(K[G])$ is nil. Hence $A(K[G])$ is nil.

We now prove that 3) \implies 4). Since $J(K[G])$ contains every nil ideal (see Proposition 9.6), $A(K[G]) \subseteq J(K[G])$. On the other hand, $K[G]/A(K[G]) \simeq K$. Since K is a field, the correspondence theorem implies that $A(K[G]) = J(K[G])$.

Finally, we prove that 4) \implies 1). Since $A(K[G]) = J(K[G])$, Exercise 50.4 implies that $K[G]/J(K[G]) \simeq K$. Since K is a field, it is, in particular, a division ring. Thus $K[G]$ is local by Theorem 26.2. \square

50.6. EXERCISE. Let p be a prime number, K be a field of characteristic p and G be a cyclic group of order p . Prove that $K[G]$ is local.

50.7. EXERCISE. Let K be a field and G be a finite group. Then $K[G]$ is a domain if and only if $|G| = 1$.

50.8. THEOREM. Let K be a field and G be a non-trivial finite group. Then $K[G]$ is local if and only if K is of characteristic $p > 0$ and G is a p -group.

PROOF. Let us first prove \implies . Assume first that K is a field of characteristic zero. By Maschke's theorem, $J(K[G]) = \{0\}$. By Theorem 26.2, $K[G]$ is a division ring. In particular, $K[G]$ is a domain, a contradiction (see Exercise 50.7).

Assume now that K is of characteristic $p > 0$. Let q be a prime divisor of $|G|$ and $g \in G$ an element of order q . Since

$$(1 - g)(1 + \cdots + g^{q-1}) = 1 - g^q = 0,$$

$1 - g \notin \mathcal{U}(K[G])$ and $1 + \cdots + g^{q-1} \notin \mathcal{U}(K[G])$. It follows that $1 - g^m \notin \mathcal{U}(K[G])$ for all $m \geq 0$. By Theorem 26.2, $K[G] \setminus J(K[G])$ is an ideal. Thus

$$q1_G = 1 + \cdots + g^{q-1} + \sum_{m=1}^{q-1} (1 - g^m) \notin \mathcal{U}(K[G])$$

If $q \neq 0$ in K , then $q1_G \in \mathcal{U}(K[G])$. Hence $q = 0$ in K and therefore p divides q . We conclude that G is a p -group.

We now prove \Leftarrow . Let G be a p -group and K be a field of characteristic $p > 0$. We proceed by induction on $|G|$. If $|G| = p$, $K[G]$ is a local ring (see Exercise 50.6). If $|G| > p$, let $Z = Z(G)$. Since G is a p -group, $|Z| \geq p$. Let N be a subgroup of Z of order p . Then $|N| < |G|$ and $|G/N| < |G|$. By the inductive hypothesis, both $K[N]$ and $K[G/N]$ are local. By Corollary 50.3, $K[G]$ is local too. \square

§ 51. Project: When a group algebra is reduced?

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

51.2. OPEN PROBLEM. Let G be a torsion-free group. Is $K[G]$ is reduced?

Problem 51.2 is related to other important open problems about group algebras (e.g. zero-divisors, units, idempotents and semisimplicity of group rings).

51.3. EXERCISE. Prove that idempotents of reduced rings are central.

The previous exercise is used to solve the following problem.

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

Exercise 51.4 is hard. Even harder is the following exercise:

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

51.6. EXERCISE. Reduced rings are semiprime.

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

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 51.3), $g\alpha g^{-1} = \alpha$ 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

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

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

then $\alpha^2 = 0$.

51.9. EXERCISE. Prove that the converse of Theorem 51.7 does not hold.

§ 52. Project: Bi-ordered groups

Recall that a **total order** is a partial order in which any two elements are comparable. This means that a total order is a binary relation \leq on some set X such that for all $x, y, z \in X$ one has the following properties:

- 1) $x \leq x$.
- 2) $x \leq y$ and $y \leq z$ imply $x \leq z$.
- 3) $x \leq y$ and $y \leq x$ imply $x = y$.
- 4) $x \leq y$ or $y \leq x$.

A set equipped with a total order is a **totally ordered set**.

52.1. DEFINITION. A group G is **bi-ordered** if there exists a total order $<$ in G such that $x < y$ implies that $xz < yz$ and $zx < zy$ for all $x, y, z \in G$.

52.2. EXAMPLE. The group $\mathbb{R}_{>0}$ of positive real numbers is bi-ordered.

The multiplicative group $\mathbb{R} \setminus \{0\}$ is not bi-ordered. Why?

52.3. EXERCISE. Let G be a bi-ordered group and $x, x_1, y, y_1 \in G$. Prove that $x < y$ and $x_1 < y_1$ imply $xx_1 < yy_1$.

Clearly, bi-orderability is preserved under taking subgroups.

52.4. EXERCISE. Let G be a bi-ordered group and $g, h \in G$. Prove that $g^n = h^n$ for some $n > 0$ implies $g = h$.

The following result goes back to Neumann.

52.5. EXERCISE. Let G be a bi-ordered group and $g, h \in G$. Prove that $g^n \in C_G(h)$ if and only if $g \in C_G(h)$.

Bi-ordered groups do not behave nicely under extensions:

52.6. EXERCISE. Let $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$ be an exact sequence of groups. Assume that K and Q are bi-ordered. Prove that G is bi-ordered if and only if $x < y$ implies $gxg^{-1} < gyg^{-1}$ for all $x, y \in K$ and $g \in G$.

52.7. DEFINITION. Let G be a bi-ordered group. The **positive cone** of G is the set $P(G) = \{x \in G : 1 < x\}$.

52.8. PROPOSITION. *Let G be a bi-ordered group and let P be its positive cone.*

- 1) P is closed under multiplication, i.e. $PP \subseteq P$.
- 2) $G = P \cup P^{-1} \cup \{1\}$ (disjoint union).
- 3) $xPx^{-1} = P$ for all $x \in G$.

PROOF. If $x, y \in P$ and $z \in G$, then, since $1 < x$ and $1 < y$, it follows that $1 < xy$. Thus $1 = z1z^{-1} < zxxz^{-1}$. It remains to prove the second claim. If $g \in G$, then $g = 1$ or $g > 1$ or $g < 1$. Note that $g < 1$ if and only if $1 < g^{-1}$, so the claim follows. \square

The previous proposition admits a converse statement.

52.9. PROPOSITION. Let G be a group and P be a subset of G such that P is closed under multiplication, $G = P \cup P^{-1} \cup \{1\}$ (disjoint union) and $xPx^{-1} = P$ for all $x \in G$. Let $x < y$ whenever $yx^{-1} \in P$. Then G is bi-ordered with positive cone is P .

PROOF. Let $x, y \in G$. Since $yx^{-1} \in G$ and $G = P \cup P^{-1} \cup \{1\}$ (disjoint union), either $yx^{-1} \in P$ or $xy^{-1} = (yx^{-1})^{-1} \in P$ or $yx^{-1} = 1$. Thus either $x < y$ or $y < x$ or $x = y$. If $x < y$ and $z \in G$, then $zx < zy$, as $(zy)(zx)^{-1} = z(yx^{-1})z^{-1} \in P$ and $zPz^{-1} = P$. Moreover, $xz < yz$ since $(yz)(xz)^{-1} = yx^{-1} \in P$. To prove that P is the positive cone of G note that $x1^{-1} = x \in P$ if and only if $1 < x$. \square

An important property:

52.10. PROPOSITION. Bi-ordered groups are torsion-free.

PROOF. Let G be a bi-ordered group and $g \in G \setminus \{1\}$. If $g > 1$, then $1 < g < g^2 < \dots$. If $g < 1$, then $1 > g > g^2 > \dots$. Hence $g^n \neq 1$ for all $n \neq 0$. \square

The converse of the previous proposition does not hold.

52.11. EXERCISE. Let $G = \langle x, y : yxy^{-1} = x^{-1} \rangle$.

- 1) Prove that x and y are torsion-free.
- 2) Prove that G is torsion-free.
- 3) Prove that $G \simeq \langle a, b : a^2 = b^2 \rangle$.

52.12. EXAMPLE. The torsion-free group $G = \langle x, y : yxy^{-1} = x^{-1} \rangle$ is not bi-ordered. If not, let P be the positive cone. If $x \in P$, then $yxy^{-1} = x^{-1} \in P$, a contradiction. Hence $x^{-1} \in P$ and $x = y^{-1}x^{-1}y \in P$, a contradiction.

Bi-ordered groups provide an answer to Kaplansky's unit problem (see Question 47.2).

52.13. THEOREM. Let G be a bi-ordered group. Then $K[G]$ is a domain such that only has trivial units. Moreover, if G is non-trivial, then $J(K[G]) = \{0\}$.

PROOF. Let $\alpha, \beta \in K[G]$ be such that

$$\begin{aligned} \alpha &= \sum_{i=1}^m a_i g_i, & g_1 < g_2 < \dots < g_m, & & a_i \neq 0 & & \forall i \in \{1, \dots, m\}, \\ \beta &= \sum_{j=1}^n b_j h_j, & h_1 < h_2 < \dots < h_n, & & b_j \neq 0 & & \forall j \in \{1, \dots, n\}. \end{aligned}$$

Then

$$g_1 h_1 \leq g_i h_j \leq g_m h_n$$

for all i, j . Moreover, $g_1 h_1 = g_i h_j$ if and only if $i = j = 1$. The coefficient of $g_1 h_1$ in $\alpha\beta$ is $a_1 b_1 \neq 0$. In particular, $\alpha\beta \neq 0$. If $\alpha\beta = \beta\alpha = 1$, then the coefficient of $g_m h_n$ in $\alpha\beta$ is $a_m b_n$. Hence $m = n = 1$ and therefore $\alpha = a_1 g_1$ and $\beta = b_1 h_1$ with $a_1 b_1 = b_1 a_1 = 1$ in K and $g_1 h_1 = 1$ in G . \square

52.14. THEOREM (Levi). Let A be an abelian group. Then A is bi-ordered if and only if A is torsion-free.

PROOF. If A is bi-ordered, then A is torsion-free. Let us prove the non-trivial implication, so assume that A is torsion-free abelian. Let \mathcal{S} be the class of subsets P of A such that $0 \in P$, are closed under the addition of A and satisfy the following property: if $x \in P$ and $-x \in P$, then $x = 0$. Clearly, $\mathcal{S} \neq \emptyset$, as $\{0\} \in \mathcal{S}$. The inclusion turns \mathcal{S} into a partially ordered set and $\bigcup_{i \in I} P_i$ is an upper bound for the chain $\{P_i : i \in I\}$. By Zorn's lemma, \mathcal{S} admits a maximal element $P \in \mathcal{S}$.

CLAIM. If $x \in A$ is such that $kx \in P$ for some $k > 0$, then $x \in P$.

Let $Q = \{x \in A : kx \in P \text{ for some } k > 0\}$. We will show that $Q \in \mathcal{S}$. Clearly, $0 \in Q$. Moreover, Q is closed under addition, as $k_1x_1 \in P$ and $k_2x_2 \in P$ imply $k_1k_2(x_1 + x_2) \in P$. Let $x \in A$ be such that $x \in Q$ and $-x \in Q$. Thus $kx \in P$ and $l(-x) \in P$ for some $k, l > 0$. Since $klx \in P$ and $kl(-x) \in P$, it follows that $klx = 0$, a contradiction since A is torsion-free. Hence $x \in Q \subseteq P$.

CLAIM. If $x \in A$ is such that $x \notin P$, then $-x \in P$.

Assume that $-x \notin P$ and let $P_1 = \{y + nx : y \in P, n \geq 0\}$. We will show that $P_1 \in \mathcal{S}$. Clearly, $0 \in P_1$ and P_1 is closed under addition. If $P_1 \notin \mathcal{S}$, there exists

$$0 \neq y_1 + n_1x = -(y_2 + n_2x),$$

where $y_1, y_2 \in P$ and $n_1, n_2 \geq 0$. Thus $y_1 + y_2 = -(n_1 + n_2)x$. If $n_1 = n_2 = 0$, then $y_1 = -y_2 \in P$ and $y_1 = y_2 = 0$, so it follows that $y_1 + n_1x = 0$, a contradiction. If $n_1 + n_2 > 0$, then, since

$$(n_1 + n_2)(-x) = y_1 + y_2 \in P,$$

it follows from the first claim that $-x \in P$, a contradiction. Let us show that $P_1 \in \mathcal{S}$. Since $P \subseteq P_1$, the maximality of P implies that $x \in P = P_1$.

By Proposition 52.9, $P^* = P \setminus \{0\}$ is the positive cone of a bi-order in A . In fact, P^* is closed under addition, as $x, y \in P^*$ implies that $x + y \in P$ and $x + y = 0$ implies $x = y = 0$, as $x = -y \in P$. Moreover, $G = P^* \cup -P^* \cup \{0\}$ (disjoint union), as the second claim states that $x \notin P^*$ implies $-x \in P$. \square

Our proof of Passman's theorem (see Theorem 47.28) used the fact that the group algebra $K[G]$ of a torsion-free abelian group G has no non-zero divisors.

52.15. EXERCISE. Let A be a non-trivial torsion-free abelian group. Prove that $K[A]$ is a domain that only admits trivial units and $J(K[A]) = \{0\}$.

52.16. EXERCISE. Let N be a central subgroup of G . If N and G/N are bi-ordered, then G is bi-ordered. Prove with an example that N needs to be central, normal is not enough.

52.17. EXERCISE. Let G be a group that admits a sequence

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that each G_k is normal in G_{k+1} and each quotient G_{k+1}/G_k is torsion-free abelian. Prove that if G is nilpotent, then G is bi-ordered.

52.18. EXERCISE. Prove that torsion-free nilpotent groups are bi-ordered.

§ 53. Project: Locally indicable groups

53.1. DEFINITION. A group G is **indicable** if there exists a non-trivial group homomorphism $G \rightarrow \mathbb{Z}$.

We know that braid groups are indicable. The free group F_n in n letters is indicable.

53.2. DEFINITION. A group G is **locally indicable** if every non-trivial finitely generated subgroup is indicable.

53.3. THEOREM (Burns–Hale). *Let G be a group. Then G is left ordered if and only if for each finitely generated non-trivial subgroup H of G there exists a left ordered group L and a non-trivial group homomorphism $H \rightarrow L$.*

PROOF. If G is a left ordered group, take $L = G$.

Conversely, suppose that for each finitely generated non-trivial subgroup H of G there exists a left ordered group L and a non-trivial group homomorphism $H \rightarrow L$. We claim that for all $\{x_1, \dots, x_n\} \subseteq G \setminus \{1\}$ there exist $\epsilon_1, \dots, \epsilon_n \in \{-1, 1\}$ such that

$$1 \notin S(x_1^{\epsilon_1}, \dots, x_n^{\epsilon_n}),$$

where $S(x_1^{\epsilon_1}, \dots, x_n^{\epsilon_n})$ denotes the semigroup generated by the set $\{x_1^{\epsilon_1}, \dots, x_n^{\epsilon_n}\}$. We proceed by induction on n . If $n = 1$, then $x_1 \in G \setminus \{1\}$. Let $\epsilon_1 = 1$. If $1 \in S(x_1)$, then x_1 is an element of finite order and hence $\langle x_1 \rangle \rightarrow L$ is the trivial homomorphism for every left ordered group L . Hence $1 \notin S(x_1)$. Now assume that the claim holds for some $n \geq 1$. Let $\{x_1, \dots, x_{n+1}\} \subseteq G \setminus \{1\}$. By assumption, there exists a non-trivial group homomorphism $h: \langle x_1, \dots, x_{n+1} \rangle \rightarrow L$ for some left ordered group L . In particular, $h(x_i) \neq 1$ for some $i \in \{1, \dots, n+1\}$. Without loss of generality, we may assume that there exists an integer $1 \leq k \leq n+1$ such that $h(x_j) \neq 1$ for all $j \in \{1, \dots, k\}$ and $h(x_j) = 1$ for all $j > k$. Suppose that L is left ordered with respect to a total order \leq . Since $h(x_j) \neq 1$ for all $j \leq k$, there are elements $\epsilon_j \in \{-1, 1\}$ such that $1 \leq h(x_j^{\epsilon_j})$ for all $j \leq k$. By the inductive hypothesis, there are elements $\epsilon_{k+1}, \dots, \epsilon_{n+1} \in \{-1, 1\}$ such that $1 \notin S(x_{k+1}^{\epsilon_{k+1}}, \dots, x_{n+1}^{\epsilon_{n+1}})$. Note that for every $x \in S(x_1^{\epsilon_1}, \dots, x_{n+1}^{\epsilon_{n+1}}) \setminus S(x_{k+1}^{\epsilon_{k+1}}, \dots, x_{n+1}^{\epsilon_{n+1}})$, $1 \leq h(x) \neq 1$. Hence $1 \notin S(x_1^{\epsilon_1}, \dots, x_{n+1}^{\epsilon_{n+1}})$, and the claim follows by induction.

Consider the set \mathcal{F} of pairs (F, f) , where F is a finite subset of $G \setminus \{1\}$ and $f: F \rightarrow \{-1, 1\}$ is a map such that for every finite subset B of $G \setminus \{1\}$ containing F , there exists a map $g: B \rightarrow \{-1, 1\}$ such that $1 \notin S(a^{g(a)} : a \in B)$ and $g(x) = f(x)$ for all $x \in F$.

Let $\mathcal{C} = \{(A, f) : A \subseteq G \setminus \{1\} \text{ and } f: A \rightarrow \{-1, 1\} \text{ such that } (F, f|_F) \in \mathcal{F} \text{ for all finite subset } F \text{ of } A\}$. We define an order on \mathcal{C} by $(A, f) \leq (B, g)$ if and only if $A \subseteq B$ and $g(a) = f(a)$ for all $a \in A$, i. e. $f = g|_A$. Note that there is a unique map $f_\emptyset: \emptyset \rightarrow \{-1, 1\}$. We have shown that $(\emptyset, f_\emptyset) \in \mathcal{C}$. Hence $\mathcal{C} \neq \emptyset$. Furthermore, every chain of elements in \mathcal{C} has an upper bound in \mathcal{C} . Thus, by Zorn's lemma, there exists a maximal element $(A, f) \in \mathcal{C}$. Suppose that $A \neq G \setminus \{1\}$. Let $x \in G \setminus (A \cup \{1\})$. Let $g_1: A \cup \{x\} \rightarrow \{-1, 1\}$ and $g_{-1}: A \cup \{x\} \rightarrow \{-1, 1\}$ be the maps defined $g_i(a) = f(a)$ for all $a \in A$ and $g_i(x) = i$ for $i \in \{-1, 1\}$. By the maximality of (A, f) , we have that $(A \cup \{x\}, g_i) \notin \mathcal{C}$. Hence there exist finite subsets F_1 and F_{-1} of $A \cup \{x\}$ and finite subsets B_1 and B_{-1} of $G \setminus \{1\}$ such that $F_1 \subseteq B_1$, $F_{-1} \subseteq B_{-1}$, $1 \in S(a^{h_1(a)} : a \in B_1)$ and $1 \in S(a^{h_{-1}(a)} : a \in B_{-1})$ for all $h_1: B_1 \rightarrow \{-1, 1\}$ and all $h_{-1}: B_{-1} \rightarrow \{-1, 1\}$ such that $g_i(a) = h_i(a)$ for all $a \in F_i$. Let $C = \bigcup_{i \in \{-1, 1\}} (A \cap F_i)$. Note that $C \cup \{x\} = F_1 \cup F_{-1} \subseteq B_1 \cup B_{-1}$. Since $(C, f|_C) \in \mathcal{F}$, there exists $h: B_1 \cup B_{-1} \rightarrow \{-1, 1\}$ such that $1 \notin S(a^{h(a)} : a \in B_1 \cup B_{-1})$ and $h(a) = f(a)$ for

all $a \in C$. Let $i = h(x) \in \{-1, 1\}$. We have that $h(x) = g_i(x)$, and thus $h(a) = g_i(a)$ for all $a \in F_i$, a contradiction because $S(a^{h(a)} : a \in B_i) \subseteq S(a^{h(a)} : a \in B_1 \cup B_{-1})$. Therefore $A = G \setminus \{1\}$.

Let $P = \{a \in G \setminus \{1\} : f(a) = 1\}$. Note that if $b \in G \setminus \{1\}$ then

$$1 \notin S(b^{f(b)}, (b^{-1})^{f(b^{-1})}),$$

and thus $f(b)f(b^{-1}) = -1$. Hence G is the disjoint union of P , $P^{-1} = \{a^{-1} : a \in P\}$ and $\{1\}$. Note that for all $a, b \in P$, $1 \notin S(a, b, (ab)^{f(ab)})$. Hence $f(ab) = 1$ and thus $ab \in P$. This proves that P is a subsemigroup of G . We define a binary relation \leq on G by, for all $a, b \in G$,

$$a \leq b \text{ if and only if } a^{-1}b \in P \cup \{1\}.$$

It is straightforward to check that \leq is a total order on G and that G is a left ordered group with respect to \leq . \square

As a consequence, locally indicable groups are left-ordered.

53.4. EXAMPLE. Since subgroups of free groups are free, it follows that F_n is locally indicable.

There are groups that are left-ordered and not locally indicable, see for example [4]. The braid group \mathbb{B}_n for $n \geq 5$ is another example of a left-ordered group that is not locally indicable.

53.5. PROPOSITION. *Let*

$$1 \longrightarrow K \xrightarrow{\alpha} G \xrightarrow{\beta} Q \longrightarrow 0$$

be an exact sequence of groups and group homomorphisms. If K and Q are locally indicable, then G is locally indicable.

PROOF. Let $g_1, \dots, g_n \in G$ and $L = \langle g_1, \dots, g_n \rangle$. Assume first that $\beta(L) \neq \{1\}$. Since Q is locally indicable, there exists a non-trivial group homomorphism $\beta(L) \rightarrow \mathbb{Z}$. Then the composition $L \rightarrow \beta(Q) \rightarrow \mathbb{Z}$ is then a non-trivial group homomorphism. Assume now that $\beta(L) = \{1\}$. Then there exist $k_1, \dots, k_n \in K$ such that $\alpha(k_i) = g_i$ for all $i \in \{1, \dots, n\}$. Note that $\alpha: \langle k_1, \dots, k_n \rangle \rightarrow L$ is a group isomorphism. Since K is locally indicable, there exists a non-trivial group homomorphism $\langle k_1, \dots, k_n \rangle \rightarrow \mathbb{Z}$. Thus the composition

$$L \rightarrow \langle k_1, \dots, k_n \rangle \rightarrow \mathbb{Z}$$

is a non-trivial group homomorphism and hence G is locally indicable. \square

As a consequence of the previous proposition, if G and H are locally indicable groups and $\sigma: G \rightarrow \text{Aut}(H)$ is a group homomorphism, then $G \rtimes_{\sigma} H$ is locally indicable. In particular, the direct product of locally indicable groups is locally indicable.

53.6. EXAMPLE. The group $G = \langle x, y : x^{-1}yx = y^{-1} \rangle$ is locally indicable. We know that G is torsion-free. Let $K = \langle y \rangle \simeq \mathbb{Z}$. Then $G/K \simeq \mathbb{Z}$ and then, since there is an exact sequence $1 \rightarrow \mathbb{Z} \rightarrow G \rightarrow \mathbb{Z} \rightarrow 1$ it follows from Proposition 53.5 that G is locally indicable.

53.7. EXERCISE. Prove that \mathbb{B}_3 is locally indicable.

The previous exercise uses the fact that $[\mathbb{B}_3, \mathbb{B}_3]$ is isomorphic to the free group in two letters, see Exercise 56.7. An alternative solution to the previous fact goes as follows: \mathbb{B}_3

is the fundamental group of the trefoil knot and fundamental groups of knots are locally indicable.

53.8. EXERCISE. Prove that \mathbb{B}_4 is locally indicable.

The previous exercise might be harder than Exercise 53.7. One possible solution is based on using the Reidemeister–Schreier method to prove that $[\mathbb{B}_4, \mathbb{B}_4]$ is a certain semidirect product between free groups in two generators. Another solution: Let $f: \mathbb{B}_4 \rightarrow \mathbb{B}_3$ be the group homomorphism given by $f(\sigma_1) = f(\sigma_3) = \sigma_1$ and $f(\sigma_2) = \sigma_2$. Then

$$\ker f = \langle \sigma_1 \sigma_3^{-1}, \sigma_2 \sigma_1 \sigma_3^{-1} \sigma_2^{-1} \rangle$$

is isomorphic to the free group in two letters. Now use the exact sequence

$$1 \rightarrow \ker f \rightarrow \mathbb{B}_4 \rightarrow \mathbb{B}_3 \rightarrow 1.$$

53.9. EXERCISE. Let $n \geq 5$. Consider the elements of \mathbb{B}_n given by

$$\beta_1 = \sigma_1^{-1} \sigma_2, \quad \beta_2 = \sigma_2 \sigma_1^{-1}, \quad \beta_3 = \sigma_1 \sigma_2 \sigma_1^{-2}, \quad \beta_4 = \sigma_3 \sigma_1^{-1}, \quad \beta_5 = \sigma_4 \sigma_1^{-1}.$$

Prove the following relations:

- 1) $\beta_1 \beta_5 = \beta_5 \beta_2$.
- 2) $\beta_2 \beta_5 = \beta_5 \beta_3$.
- 3) $\beta_1 \beta_3 = \beta_2$.
- 4) $\beta_1 \beta_4 \beta_3 = \beta_4 \beta_2 \beta_4$.
- 5) $\beta_4 \beta_5 \beta_4 = \beta_5 \beta_4 \beta_5$.

53.10. EXERCISE. Let $n \geq 5$. Prove that \mathbb{B}_n is not locally indicable.

For the previous exercise one needs to show that every group homomorphism

$$f: \langle \beta_1, \dots, \beta_5 \rangle \rightarrow \mathbb{Z}$$

is trivial. Hint: consider the abelianization of $\langle \beta_1, \dots, \beta_5 \rangle$.

§ 54. Project: Left-ordered groups

54.1. DEFINITION. A group G is **left-ordered** if there is a total order $<$ in G such that $x < y$ implies $zx < zy$ for all $x, y, z \in G$.

If G is left-ordered, the **positive cone** of G is defined as $P(G) = \{x \in G : 1 < x\}$.

54.2. EXERCISE. Let G be left-ordered with positive cone P . Prove that P is closed under multiplication and that $G = P \cup P^{-1} \cup \{1\}$ (disjoint union).

54.3. EXERCISE. Let G be a group and P be a subset closed under multiplication. Assume that $G = P \cup P^{-1} \cup \{1\}$ (disjoint union). Prove that $x < y$ if and only if $x^{-1}y \in P$ turns G into a left-ordered group with positive cone P .

Left-ordered groups behave nicely with respect to extensions. Let G be a group and N be a left-ordered normal subgroup of G . If $\pi: G \rightarrow G/N$ is the canonical map and G/N is left-ordered, then G is left-ordered with $x < y$ if and only if either $\pi(x) < \pi(y)$ or $\pi(x) = \pi(y)$ and $1 < x^{-1}y$.

54.4. PROPOSITION. Let G be a group and N be a normal subgroup of G . If N and G/N are left-ordered, then so is G .

PROOF. Since N and G/N are both left-ordered, there exist positive cones $P(N)$ and $P(G/N)$. Let $\pi: G \rightarrow G/N$ be the canonical map and

$$P(G) = \{x \in G : \pi(x) \in P(G/N) \text{ or } x \in P(N)\}.$$

A routine calculation shows that $P(G)$ is closed under multiplication and that G decomposes as $G = P(G) \cup P(G)^{-1} \cup \{1\}$ (disjoint union). It follows from Exercise 54.3 that G is left-ordered. \square

We now present a criterion for detecting left-ordered groups. We shall need a lemma.

54.5. LEMMA. Let G be a finitely generated group. If H is a finite-index subgroup, then H is finitely generated.

PROOF. Assume that G is generated by $\{g_1, \dots, g_m\}$. Assume that for each i there exists k such that $g_i^{-1} \in H$. Let $\{t_1, \dots, t_n\}$ be a transversal of H in G . For $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, m\}$ write

$$t_i g_j = h(i, j) t_{k(i, j)}.$$

We claim that H is generated by the $h(i, j)$. For $x \in H$, write

$$\begin{aligned} x &= g_{i_1} \cdots g_{i_s} \\ &= (t_1 g_{i_1}) g_{i_2} \cdots g_{i_s} \\ &= h(1, i_1) t_{k_1} g_{i_2} \cdots g_{i_s} \\ &= h(1, i_1) h(k_1, i_2) t_{k_2} g_{i_3} \cdots g_{i_s} \\ &= h(1, i_1) h(k_1, i_2) \cdots h(k_{s-1}, i_s) t_{k_s}, \end{aligned}$$

where $k_1, \dots, k_{s-1} \in \{1, \dots, n\}$. Since $t_{k_s} \in H$, it follows that $t_{k_s} = t_1 \in H$. \square

Now the theorem.

54.6. THEOREM. *Let G be a finitely generated torsion-free group. If A is an abelian normal subgroup such that G/A is finite and cyclic, then G is left-ordered.*

PROOF. Note that if A is trivial, then so is G . Let us assume that $A \neq \{1\}$. Since $(G : A)$ is finite, A is finitely generated by the previous lemma. We proceed by induction on the number of generators of A . Since G/A is cyclic, there exists $x \in G$ such that $G = \langle A, x \rangle$. Then $[x, A] = \langle [x, a] : a \in A \rangle$ is a normal subgroup of G such that $A/C_A(x) \simeq [x, A]$ (because $a \mapsto [x, a]$ is a group homomorphism $A \rightarrow A$ with image $[x, A]$ and kernel $C_A(x)$). If $\pi : G \rightarrow G/[x, A]$ is the canonical map, then $G/[x, A] = \langle \pi(A), \pi(x) \rangle$ and thus $G/[x, A]$ is abelian, as $[\pi(x), \pi(A)] = \pi[x, A] = 1$. Moreover, $G/[x, A]$ is finitely generated, as G is finitely generated. Since $(G : A) = n$ and G is torsion-free, it follows that $1 \neq x^n \in A$. Hence $x^n \in C_A(x)$ and therefore $1 \leq \text{rank } C_A(x) < \text{rank } A$ (if $\text{rank } C_A(x) = \text{rank } A$, then $[x, A]$ would be a torsion subgroup of A , a contradiction since $x \notin A$). So

$$\text{rank}[x, A] = \text{rank}(A/C_A(x)) \leq \text{rank } A - 1$$

and hence $\text{rank}(A/[x, A]) \geq 1$. We proved that $A/[x, A]$ is infinite and hence $G/[x, A]$ is infinite.

Since $G/[x, A]$ is infinite, abelian and finitely generated, there exists a normal subgroup H of G such that $[x, A] \subseteq H$ and $G/H \simeq \mathbb{Z}$. The subgroup $B = A \cap H$ is abelian, normal in H and such that H/B is cyclic (because it is isomorphic to a subgroup of G/A). Since $\text{rank } B < \text{rank } A$, the inductive hypothesis implies that H is left-ordered. Hence G is left-ordered. \square

Lagrange and Rhemtulla proved that the integral isomorphism problem has an affirmative solution for left-ordered groups. More precisely, if G is left-ordered and H is a group such that $\mathbb{Z}[G] \simeq \mathbb{Z}[H]$, then $G \simeq H$, see [26].

54.7. THEOREM (Malcev–Neumann). *Let G be left-ordered group. Then $K[G]$ has no zero divisors and no non-trivial units.*

PROOF. If $\alpha = \sum_{i=1}^n a_i g_i \in K[G]$ and $\beta = \sum_{j=1}^m b_j h_j \in K[G]$, then

$$(54.1) \quad \alpha\beta = \sum_{i=1}^n \sum_{j=1}^m a_i b_j (g_i h_j).$$

Without loss of generality we may assume that $a_i \neq 0$ for all i and $b_j \neq 0$ for all j . Moreover, we may assume that $g_1 < g_2 < \dots < g_n$. Let i, j be such that

$$g_i h_j = \min\{g_i h_j : 1 \leq i \leq n, 1 \leq j \leq m\}.$$

Then $i = 1$, as $i > 1$ implies $g_1 h_j < g_i h_j$, a contradiction. Since $g_1 h_j \neq g_1 h_k$ whenever $k \neq j$, there exists a unique minimal element in the left hand side of Equality (54.1). The same argument shows that there is a unique maximal element in (54.1). Thus $\alpha\beta \neq 0$, as $a_1 b_j \neq 0$, and therefore $K[G]$ has no zero divisors. If, moreover, $n > 1$ or $m > 1$, then (54.1) contains at least two terms that cancel out and thus $\alpha\beta \neq 1$. It follows that units of $K[G]$ are trivial. \square

Formanek proved that the zero divisors conjecture is true in the case of torsion-free super solvable. Brown and, independently, Farkas and Snider proved that the conjecture is true in the case of groups algebras (over fields of characteristic zero) of polycyclic-by-finite torsion-free groups. These results can be found in Chapter 13 of Passman's book [33].

§ 55. Project: Unique product groups

Let G be a group and $A, B \subseteq G$ be non-empty subsets. An element $g \in G$ is a **unique product** in AB if $g = ab = a_1b_1$ for some $a, a_1 \in A$ and $b, b_1 \in B$ implies that $a = a_1$ and $b = b_1$.

55.1. DEFINITION. A group G has the **unique product property** if for every finite non-empty subsets $A, B \subseteq G$ there exists at least one unique product in AB .

55.2. PROPOSITION. *Left-ordered groups have the unique product property.*

PROOF. Let G be a left-ordered group. Let A be a non-empty finite subset of G and $B = \{b_1, \dots, b_n\} \subseteq G$. Assume that $b_1 < b_2 < \dots < b_n$. Let $c \in A$ be such that cb_1 is the minimum of $Ab_1 = \{ab_1 : a \in A\}$. We claim that cb_1 admits a unique representation of the form $\alpha\beta$ with $\alpha \in A$ and $\beta \in B$. If $cb_1 = ab$, then, since $ab = cb_1 \leq ab_1$, it follows that $b \leq b_1$. Hence $b = b_1$ and $a = c$. \square

55.3. EXERCISE. Prove that groups with the unique product property are torsion-free.

The converse does not hold. Promislow's group is a celebrated counterexample.

55.4. THEOREM (Promislow). *The group $G = \langle a, b : a^{-1}b^2a = b^{-2}, b^{-1}a^2b = a^{-2} \rangle$ does not have the unique product property.*

PROOF. Let

$$(55.1) \quad S = \{a^2b, b^2a, aba^{-1}, (b^2a)^{-1}, (ab)^{-2}, b, (ab)^2a, (ab)^2, (aba)^{-1}, \\ bab, b^{-1}, a, aba, a^{-1}\}.$$

We use [9] and the representation $G \rightarrow \mathbf{GL}_4(\mathbb{Q})$ given by

$$a \mapsto \begin{pmatrix} 1 & 0 & 0 & 1/2 \\ 0 & -1 & 0 & 1/2 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & -1 & 1/2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

to check that G does not have unique product property, as each

$$s \in S^2 = \{s_1s_2 : s_1, s_2 \in S\}$$

admits at least two different decompositions of the form $s = xy = uv$ for $x, y, u, v \in S$. We first create the matrix representations of a and b .

```
gap> a := [[1,0,0,1/2],[0,-1,0,1/2],[0,0,-1,0],[0,0,0,1]];
gap> b := [[-1,0,0,0],[0,1,0,1/2],[0,0,-1,1/2],[0,0,0,1]];
```

Now we create a function that produces the set S .

```
gap> Promislow := function(x, y)
> return Set([
> x^2*y,
> y^2*x,
> x*y*Inverse(x),
> (y^2*x)^(-1),
> (x*y)^(-2),
```

```

> y,
> (x*y)^2*x,
> (x*y)^2,
> (x*y*x)^(-1),
> y*x*y,
> y^(-1),
> x,
> x*y*x,
> x^(-1)
]);
end;;

```

So the set S of (55.1) will be `Promislow(a,b)`. We now create a function that checks whether every element of a Promislow subset admits more than one representation.

```

gap> is_UPP := function(S)
> local l,x,y;
> l := [];
> for x in S do
> for y in S do
> Add(l,x*y);
> od;
> od;
> if ForAll(Collected(l), x->x[2] <> 1) then
> return false;
> else
> return fail;
> fi;
> end;;

```

Finally, we check whether every element of S^2 admits more than one representation.

```

gap> S := Promislow(a,b);;
gap> is_UPP(S);
false

```

This completes the proof. □

55.5. EXERCISE. Let G be a group and $A, B \subseteq G$ be finite non-empty subsets. Prove that if $|A| = 1$, then AB contains a unique product.

The size of the set A can be extended.

55.6. EXERCISE. Let G be a group and $A, B \subseteq G$ be finite non-empty subsets. Prove that AB has no unique products if and only if $(gA)(Bh)$ has no unique product for all $g, h \in G$.

55.7. EXERCISE. Let G be a torsion-free group and $A, B \subseteq G$ be finite non-empty subsets. Prove that if $|A| = 2$, then AB contains a unique product.

The case where the set A has size three is still open. One can prove, for example, that if $|A| = 3$, then $|B| \geq 7$.

55.8. DEFINITION. A group G has the **double property of unique products** if for every finite non-empty subsets $A, B \subseteq G$ such that $|A| + |B| > 2$ there are at least two unique products in AB .

55.9. THEOREM (Strojnowski). *Let G be a group. The following statements are equivalent:*

- 1) G has the double property of unique products.
- 2) Every non-empty finite subset $A \subseteq G$ contains at least one unique product in

$$AA = \{a_1a_2 : a_1, a_2 \in A\}.$$

- 3) G has the unique product property.

PROOF. The implication (1) \implies (2) is trivial.

We now prove that (2) \implies (3). Suppose that G satisfies (2). Let A, B be finite non-empty subsets of G . Let $C = BA$. By (2), there exist a unique $g \in G$ such that $g = (b_1a_1)(b_2a_2)$ for unique $b_1a_1, b_2a_2 \in C$, where $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Note that this implies that $a_1b_2 = ab$ for $a \in A$ and $b \in B$ if and only if $a = a_1$ and $b = b_2$. Hence G satisfies the unique product property.

We finally prove that (3) \implies (1). Suppose that G satisfies the unique product property but not the double unique product property. Thus there exist finite non-empty subsets $A, B \subseteq G$ with $|A| + |B| > 2$ and there is a unique $g \in G$ such that $g = ab$ for unique elements $a \in A$ and $b \in B$. Let $C = a^{-1}A$ and $D = Bb^{-1}$. Then $1 \in C \cap D$. Note that if $c \in C$, $d \in D$ and $cd \neq 1$, then there exist $a_1 \in A$ and $b_1 \in B$ such that $c = a^{-1}a_1$, $d = b_1b^{-1}$ and $ab \neq a_1b_1$. Hence there exist $a_2 \in A \setminus \{a_1\}$ and $b_2 \in B \setminus \{b_1\}$ such that $a_1b_1 = a_2b_2$. Let $c_1 = a^{-1}a_2$ and $d_1 = b_2b^{-1}$. We have that $c \neq c_1$, $d \neq d_1$ and

$$cd = a^{-1}a_1b_1b^{-1} = a^{-1}a_2b_2b^{-1} = c_1d_1.$$

Let $E = D^{-1}C$ and $F = DC^{-1}$. Every element of EF is of the form $(d_1^{-1}c_1)(d_2c_2^{-1})$, where $c_1, c_2 \in C$ and $d_1, d_2 \in D$. Suppose that $c_1d_2 \neq 1$. We have seen that then there exist $c_3 \in C \setminus \{c_1\}$ and $d_3 \in D \setminus \{d_2\}$ such that $c_1d_2 = c_3d_3$. Hence $d_1^{-1}c_3 \in E \setminus \{d_1^{-1}c_1\}$, $d_3c_2^{-1} \in F \setminus \{d_2c_2^{-1}\}$ and

$$(d_1^{-1}c_1)(d_2c_2^{-1}) = (d_1^{-1}c_3)(d_3c_2^{-1}).$$

Suppose that $c_2d_1 \neq 1$. Then there exist $c_4 \in C \setminus \{c_2\}$ and $d_4 \in D \setminus \{d_1\}$ such that $c_2d_1 = c_4d_4$. Hence $d_4^{-1} \cdot 1 \in E \setminus \{d_1^{-1} \cdot 1\}$, $1 \cdot c_4^{-1} \in F \setminus \{1 \cdot c_2^{-1}\}$ and

$$(d_1^{-1} \cdot 1)(1 \cdot c_2^{-1}) = (d_4^{-1} \cdot 1)(1 \cdot c_4^{-1}).$$

Since $|C| + |D| = |A| + |B| > 2$, either there exists $c \in C \setminus \{1\}$ or there exists $d \in D \setminus \{1\}$. In the first case, we have

$$(1 \cdot 1)(1 \cdot 1) = (1 \cdot c)(1 \cdot c^{-1}),$$

and in the second case, we have

$$(1 \cdot 1)(1 \cdot 1) = (d^{-1} \cdot 1)(d \cdot 1).$$

Thus, we have found two finite non-empty subsets $E, F \subseteq G$ such that for every $e \in E$ and $f \in F$, there exist $e_1 \in E \setminus \{e\}$ and $f_1 \in F \setminus \{f\}$ such that $ef = e_1f_1$, a contradiction, because G satisfies the unique product property. Therefore G also satisfies the double unique product property. \square

55.10. EXERCISE. Prove that if a group G satisfies the unique product property, then $K[G]$ contains only trivial units.

In general it is extremely hard to check whether a given group has the unique product property. As a geometrical way to attack this problem, Bowditch introduced **diffuse groups**. If G is a torsion-free group and $A \subseteq G$ is a subset, we say that A is **antisymmetric** if $A \cap A^{-1} \subseteq \{1\}$, where $A^{-1} = \{a^{-1} : a \in A\}$. The set of **extremal elements** of A is defined as $\Delta(A) = \{a \in A : Aa^{-1} \text{ is antisymmetric}\}$. Thus

$$a \in A \setminus \Delta(A) \iff \text{there exists } g \in G \setminus \{1\} \text{ such that } ga \in A \text{ and } g^{-1}a \in A.$$

55.11. DEFINITION. A group G is **diffuse** if for every finite subset $A \subseteq G$ such that $2 \leq |A| < \infty$ one has $|\Delta(A)| \geq 2$.

This means that a group G is diffuse if for every finite non-empty subset $A \subseteq G$ there exists $a \in A$ such that for all $g \in G \setminus \{1\}$ either $ga \notin A$ or $g^{-1}a \notin A$.

55.12. PROPOSITION. *Left-ordered groups are diffuse.*

PROOF. Let G be a left-ordered group and $A = \{a_1, \dots, a_n\}$ be such that

$$a_1 < a_2 < \dots < a_n.$$

We claim that $\{a_1, a_n\} \subseteq \Delta(A)$. If $a_1 \in A \setminus \Delta(A)$, there exists $g \in G \setminus \{1\}$ such that $ga_1 \in A$ and $g^{-1}a_1 \in A$. Thus $a_1 \leq ga_1$ and $a_1 \leq g^{-1}a_1$. It follows that $1 \leq a^{-1}ga_1$ and $1 \leq a_1^{-1}g^{-1}a_1 = (a_1^{-1}ga_1)^{-1}$, a contradiction. Similarly, $a_n \in \Delta(A)$. \square

There are diffuse groups that are not left-ordered, see [22].

55.13. PROPOSITION. *Diffuse groups have double unique products.*

PROOF. Let G be a diffuse group that does not have double unique products. There exist non-empty subsets $A, B \subseteq G$ with $|A| + |B| > 2$ such that $C = AB$ admits at most one unique product. Then $|C| \geq 2$. Since G is diffuse, $|\Delta(C)| \geq 2$. If $c \in \Delta(C)$, then c admits a unique expression of the form $c = ab$ with $a \in A$ and $b \in B$ (otherwise, if $c = a_0b_0 = a_1b_1$ with $a_0 \neq a_1$ and $b_0 \neq b_1$). If $g = a_0a_1^{-1}$, then $g \neq 1$,

$$gc = a_0a_1^{-1}a_1b_1 = a_0b_1 \in C.$$

Moreover, $g^{-1}c = a_1a_0^{-1}a_0b_0 = a_1b_0 \in C$. Hence $c \notin \Delta(c)$, a contradiction. \square

55.14. OPEN PROBLEM. Find a non-diffuse group with the unique product property.

§ 56. Project: The braid group

56.1. DEFINITION. Let $n \geq 1$. The **braid group** \mathbb{B}_n is the group with generators $\sigma_1, \dots, \sigma_{n-1}$ and relations

$$\begin{aligned} \sigma_i \sigma_{i+1} \sigma_i &= \sigma_{i+1} \sigma_i \sigma_{i+1} & \text{if } 1 \leq i \leq n-2, \\ \sigma_i \sigma_j &= \sigma_j \sigma_i & \text{if } |i-j| > 1. \end{aligned}$$

Note that $\mathbb{B}_1 = \{1\}$ and $\mathbb{B}_2 \simeq \mathbb{Z}$. The braid group \mathbb{B}_3 is generated by σ_1 and σ_2 with relations $\sigma_1 \sigma_2 \sigma_1 = \sigma_2 \sigma_1 \sigma_2$.

56.2. EXERCISE. Prove that there exists a group homomorphism $\mathbb{B}_n \rightarrow \mathbb{S}_n$ given by $\sigma_i \mapsto (i \ i+1)$ for all $i \in \{1, \dots, n-1\}$.

Note that if $n \geq 3$, then \mathbb{B}_n is a non-abelian group, as there exists a surjective group homomorphism $\mathbb{B}_n \rightarrow \mathbb{S}_n$.

56.3. EXERCISE. Let $n \geq 2$. Prove that the map $\deg: \mathbb{B}_n \rightarrow \mathbb{Z}$, $\sigma_i \mapsto 1$, is a group homomorphism. Moreover, $\ker \deg = [\mathbb{B}_n, \mathbb{B}_n]$.

The previous result implies, in particular, that \mathbb{B}_n is an infinite group for all $n \geq 2$. Moreover, $\sigma_i^m \neq 1$ for all $m \in \mathbb{Z} \setminus \{0\}$ and all i .

56.4. EXERCISE. Prove that $\mathbb{B}_3 \simeq \langle x, y : x^2 = y^3 \rangle$ and that $\mathbb{B}_3 / Z(\mathbb{B}_3) \simeq \mathbf{PSL}_2(\mathbb{Z})$.

56.5. EXERCISE. Prove that the center $Z(\mathbb{B}_3)$ of \mathbb{B}_3 is the cyclic group generated by $(\sigma_1 \sigma_2 \sigma_1)^2$.

More generally, one can prove that the center of \mathbb{B}_n is generated by Δ_n^2 , where

$$\Delta_n = (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1 \sigma_2) \sigma_1,$$

see for example [21, Theorem 1.24]. As a corollary, $\mathbb{B}_n \simeq \mathbb{B}_m$ if and only if $n = m$.

56.6. EXERCISE. Let $n \geq 3$. Prove that \mathbb{B}_n is not bi-ordered.

One can prove that the natural map $\mathbb{B}_n \rightarrow \mathbb{B}_{n+1}$ is an injective group homomorphism, this is not an easy proof (see [21, Corollary 1.14]). Moreover, the diagram

$$\begin{array}{ccc} \mathbb{B}_n & \longrightarrow & \mathbb{S}_n \\ \downarrow & & \downarrow \\ \mathbb{B}_{n+1} & \longrightarrow & \mathbb{S}_{n+1} \end{array}$$

commutes.

56.7. EXERCISE. Use the Reidemeister–Schreier’s method to prove that $[\mathbb{B}_3, \mathbb{B}_3]$ is isomorphic to the free group in two letters.

A celebrated theorem of Dehornoy states that the braid group \mathbb{B}_n is left-ordered (see for example [21, Theorem 7.15]). The proof of this fact is quite hard. However, there is a nice short proof of the fact that \mathbb{B}_3 is left-ordered, see [8, §7.2].

56.8. OPEN PROBLEM (Bureau's representation). Let $\mathbb{B}_4 \rightarrow \mathbf{GL}_4(\mathbb{Z}[t, t^{-1}])$ be the group homomorphism given by

$$\sigma_1 \mapsto \begin{pmatrix} 1-t & t & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \sigma_2 \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1-t & t & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \sigma_3 \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1-t & t \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Is this homomorphism injective?

In general, the Bureau's representation $\mathbb{B}_n \rightarrow \mathbf{GL}_n(\mathbb{Z}[t, t^{-1}])$ is defined by

$$\sigma_j \mapsto I_{j-1} \oplus \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix} \oplus I_{n-j-1},$$

where I_k denotes the $k \times k$ identity matrix.

It is known that the Bureau's representation of \mathbb{B}_n is faithful for $n \leq 3$ and not faithful for $n \geq 5$. Only the case $n = 4$ remains open.

Using a different representation, Krammer [24] and Bigelow [5] independently proved that braid groups are linear.

Some other topics for final projects

We collect here some other topics for final presentations. Some topics can also be used as bachelor or master theses.

The 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 theorem give conditions under which one can conclude that the equality occurs; see [7, Chapter 4].

The 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 [7, 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 [20, I.8.3]; see [20, I.7] for the basic theory of Ore’s extensions.

The 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 [16] of Herstein.

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 [27] for more information. In 1968, Dixmier conjectured that any endomorphism of a Weyl algebra is an automorphism; the conjecture is still open.

The Jacobson–Herstein theorem. There exist more theorems similar to the Jacobson’s commutativity theorem; see [27] and [34]. For example, the Jacobson–Herstein theorem states that if R is a ring such that for every $x, y \in R$ there exists some $n(x, y) \geq 2$ such that

$$(xy - yx)^{n(x,y)} = xy - yx,$$

then R is commutative.

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] G. M. Bergman. Errata: “A ring primitive on the right but not on the left”. *Proc. Amer. Math. Soc.*, 15:1000, 1964.
- [3] G. M. Bergman. A ring primitive on the right but not on the left. *Proc. Amer. Math. Soc.*, 15:473–475, 1964.
- [4] G. M. Bergman. Right orderable groups that are not locally indicable. *Pacific J. Math.*, 147(2):243–248, 1991.
- [5] S. J. Bigelow. Braid groups are linear. *J. Amer. Math. Soc.*, 14(2):471–486, 2001.
- [6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I: The user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997.
- [7] M. Brešar. *Introduction to noncommutative algebra*. Universitext. Springer, Cham, 2014.
- [8] A. Clay and D. Rolfsen. *Ordered groups and topology*, volume 176 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2016.
- [9] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.13.1*, 2024.
- [10] D. García-Lucas, L. Margolis, and A. del Río. Non-isomorphic 2-groups with isomorphic modular group algebras. *J. Reine Angew. Math.*, 783:269–274, 2022.
- [11] G. Gardam. A counterexample to the unit conjecture for group rings. *Ann. of Math. (2)*, 194(3):967–979, 2021.
- [12] B. J. Gardner and R. Wiegandt. *Radical theory of rings*, volume 261 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 2004.
- [13] R. W. Gilmer, Jr. If $R[X]$ is Noetherian, R contains an identity. *Amer. Math. Monthly*, 74:700, 1967.
- [14] M. Henriksen. A simple characterization of commutative rings without maximal ideals. *Amer. Math. Monthly*, 82:502–505, 1975.
- [15] I. N. Herstein. A counterexample in Noetherian rings. *Proc. Nat. Acad. Sci. U.S.A.*, 54:1036–1037, 1965.
- [16] 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.
- [17] M. Hertweck. A counterexample to the isomorphism problem for integral group rings. *Ann. of Math. (2)*, 154(1):115–138, 2001.
- [18] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.
- [19] N. Jacobson. *Structure of rings*. American Mathematical Society Colloquium Publications, Vol. 37. American Mathematical Society, Providence, R.I., revised edition, 1964.
- [20] C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
- [21] C. Kassel and V. Turaev. *Braid groups*, volume 247 of *Graduate Texts in Mathematics*. Springer, New York, 2008. With the graphical assistance of Olivier Dodane.
- [22] S. Kionke and J. Raimbault. On geometric aspects of diffuse groups. *Doc. Math.*, 21:873–915, 2016. With an appendix by Nathan Dunfield.
- [23] G. Köthe. Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist. *Math. Z.*, 32(1):161–186, 1930.
- [24] D. Krammer. Braid groups are linear. *Ann. of Math. (2)*, 155(1):131–156, 2002.
- [25] J. Krempa. Logical connections between some open problems concerning nil rings. *Fund. Math.*, 76(2):121–130, 1972.
- [26] R. H. Lagrange and A. H. Rhemtulla. A remark on the group rings of order preserving permutation groups. *Canad. Math. Bull.*, 11:679–680, 1968.
- [27] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.
- [28] T. Y. Lam. *Exercises in modules and rings*. Problem Books in Mathematics. Springer, New York, 2007.
- [29] L. Margolis. The modular isomorphism problem: a survey. *Jahresber. Dtsch. Math.-Ver.*, 124(3):157–196, 2022.

- [30] M. Mirzakhani. A simple proof of a theorem of Schur. *Am. Math. Mon.*, 105(3):260–262, 1998.
- [31] 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.
- [32] P. P. Nielsen. Simplifying Smoktunowicz’s extraordinary example. *Comm. Algebra*, 41(11):4339–4350, 2013.
- [33] D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.
- [34] J. Pinter-Lucke. Commutativity conditions for rings: 1950–2005. *Expo. Math.*, 25(2):165–174, 2007.
- [35] I. Rosenholtz. A pigeonhole proof of Kaplansky’s theorem. *Amer. Math. Monthly*, 99(2):132–133, 1992.
- [36] W. R. Scott. *Group theory*. Dover Publications, Inc., New York, second edition, 1987.
- [37] A. Smoktunowicz. Polynomial rings over nil rings need not be nil. *J. Algebra*, 233(2):427–436, 2000.
- [38] A. Smoktunowicz. On some results related to Köthe’s conjecture. *Serdica Math. J.*, 27(2):159–170, 2001.
- [39] A. Smoktunowicz. Some results in noncommutative ring theory. In *International Congress of Mathematicians. Vol. II*, pages 259–269. Eur. Math. Soc., Zürich, 2006.
- [40] D. E. Taylor. Some classical theorems on division rings. *Enseign. Math. (2)*, 20:293–298, 1974.
- [41] M. Teleuca. Zsigmondy’s theorem and its applications in contest problems. *Internat. J. Math. Ed. Sci. Tech.*, 44(3):443–451, 2013.
- [42] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.

Akizuki's theorem, 34
 Algebra, 4
 algebraic, 5
 central, 75
 central simple, 78
 commutative, 4
 dimension, 4
 ideal, 5
 of multipliers, 75
 opposite, 9
 semisimple, 7
 simple, 11
 Algebraic element, 5
 Amitsur's theorem, 28
 Andrunakevic–Rjabuhin theorem, 82
 Artin–Wedderburn theorem, 10, 40
 Automorphism
 inner, 76

 Braid group, 118
 Brauer's problem, 14
 Brown's theorem, 113
 Burau's representation, 119
 Burns–Hale theorem, 109
 Burnside's theorem, 54

 Central idempotent, 47
 Characteristic of a ring, 24
 Chinese Remainder Theorem, 16
 Composition series
 equivalence, 33
 Connel's theorem, 99, 100

 Dehornoy's theorem, 118
 Dietzmann's theorem, 99
 Division algebra, 8
 Domain, 38

 Element
 left quasi-regular, 20
 quasi-regular, 20

 Farkas–Snider theorem, 113
 Feit–Thompson's theorem, 54
 Fermat's last theorem for finite rings, 63
 Flag
 complete, 85
 standard, 85
 Formanek's theorem, 55, 60, 113
 Frobenius'
 theorem, 63

 Gardam's theorem, 90, 97
 Gilmer's theorem, 30

Index

Group
 bi-ordered, 105
 diffuse, 117
 double unique product, 116
 indicable, 109
 left-ordered, 112
 locally finite, 53
 locally indicable, 109
 solvable, 54
 torsion, 54
 unique product, 114
 Gustafson's theorem, 46

 Henriksen's theorem, 24
 Herstein's theorem, 55
 Homomorphism
 of algebras, 4
 Hopkins–Levitzki theorem, 43
 Hopkins–Levitzky's theorem, 100
 Hurewicz' theorem, 71

 Ideal
 maximal, 17
 nil, 19
 nilpotent, 19
 prime, 40
 primitive, 18
 reduced, 82
 regular, 17
 Idempotent, 44, 90
 Involution, 68

 Jacobson radical, 19
 Jacobson's commutativity theorem, 66
 Jacobson's conjecture, 29
 Jacobson's density theorem, 37
 Jacobson–Herstein conjecture, 29
 Jordan–Hölder theorem, 33

 Köthe conjecture, 29
 Kaplansky's theorem, 74
 Kolchin's theorem, 87

 Lagrange–Rhemtulla's theorem, 113
 Left ideal
 maximal, 17
 nil, 19
 nilpotent, 19
 regular, 17
 Levi's theorem, 106

 Malcev–Neumann theorem, 113
 Maschke's theorem, 52
 Minimal element, 31

- Minimal left ideal, 17
- Module, 5
 - artinian, 31
 - composition series, 32
 - Dedekind-finite, 73
 - faithful, 18
 - homomorphism, 5
 - length, 34
 - noetherian, 31
 - of finite length, 34
 - semisimple, 6
 - simple, 6
- Mollien's theorem, 11
- Nakayama's lemma, 47
- Neumann's
 - lemma, 92
- Nil
 - algebra, 84
 - element, 84
- Nilpotent
 - algebra, 84
 - element, 84
- Passman's
 - lemma, 94
 - theorem, 95
- Prüfer's group, 53
- Promislow's group, 96
- Promislow's theorem, 114
- Reidemeister–Schreier's method, 118
- Rickart's theorem, 50, 69
- Ring
 - boolean, 65
 - Dedekind-finite, 73
 - left artinian, 32
 - local, 27, 44
 - nil, 25
 - prime, 38, 99
 - primitive, 18
 - radical, 23
 - reduced, 39, 73, 82, 90
 - reversible, 73
 - semilocal, 46
 - semiprime, 51
 - semisimple, 42
 - simple, 16
 - Von Neumann regular, 45
 - with an involution, 68
- Schur's lemma, 6
- Schur's theorem, 49
- Skolem–Noether theorem, 77
- Strojonowski's theorem, 116
- Subdirect product, 35
- Sylow's theorems, 88
- Trivial idempotent, 44
- Trivial units in group algebras, 90
- Unipotent element, 86
- Unipotent group, 86
- Wedderburn's little theorem, 61
- Wedderburn's theorem, 12, 40, 84
- Zsigmondy's theorem, 62