Leandro Vendramin

Associative algebras

Notes

Wednesday 17th November, 2021

Preface

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

The material is heavility based on [2], [4] and [9].

This version was compiled on Wednesday 17$^{\text{th}}$ November, 2021 at 21:47.

Leandro Vendramin
Brussels, Belgium

Contents

List of topics

Lecture 1

§1. Semisimple algebras

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

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

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

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

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

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

Any field K is an algebra over K.

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

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

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

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

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

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

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

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

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

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

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

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

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

Similarly one defines left and right ideals of an algebra.

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

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

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

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

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

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

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

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

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

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

Similarly one defines submodules and module homomorphisms.

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

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

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

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

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

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

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

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

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

Clearly, a finite direct sum of semisimples is semisimple.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

is also semisimple. $\square$

Lecture 2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

it follows that the map is an isomorphism. Thus

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

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

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

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

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

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

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

then each n_j is uniquely determined.

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

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

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

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

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

lem:A^op

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

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

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

lem:Mn_op

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

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

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

lem:simple

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

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

as algebras.

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

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

The reader should prove that the map

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Corollary 1.36 (Mollien). *If A is a finite-dimensional complex semisimple algebra, 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,

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

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

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

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

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

Lecture 3

03 **Definition 1.37.** An algebra A is **simple** if $A \neq \{0\}$ and $\{0\}$ and A are the only ideals of A.

Proposition 1.38. *Let A be a finite-dimensional simple algebra. There exists a non-zero left ideal I of minimal dimension. This ideal is a simple A-module and every simple A-module is isomorphic to I.*

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

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

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

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

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

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

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

Proposition 1.39. *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 knot 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. If $T \subseteq A$ is a simple submodule and $a \in A$, let $f\colon T \to Ta$, $t \mapsto ta$. Since f is a module homomorphism and T is simple, it follows that either $\ker f = \{0\}$ or $\ker T = T$. If $\ker T = T$, then $f(T) = Ta = \{0\} \subseteq S$. If $\ker f = \{0\}$, then $T \simeq f(T) = Ta$ and hence Ta is simple. Hence $Ta \subseteq S$.

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

Theorem 1.40 (Wedderburn). *Let A be a finite-dimensional algebra. If A is simple, then $A \simeq M_n(D)$ for some $n \in \mathbb{Z}_{>0}$ and some division algebra D.*

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

§2. Jacobson radical

Jacobson radical

We will consider rings possibly without identity. 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 ring (or a unitary ring). A **subring** S of R is an additive subgroup of R closed under multiplication.

Example 2.1. $2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$ is a ring.

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

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

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

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

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

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

Example 2.6. Division rings are simple.

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

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

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

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

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

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

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

Definition 2.8. 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 $M \neq \{0\}$.

lemma:simple **Lemma 2.9.** *Let M be a non-zero module. Then M is simple if and only if $M = R \cdot m$ for all $0 \neq m \in M$.*

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

Example 2.10. Let D be a division ring and let V be a non-zero vector space (over D). If $R = \mathrm{End}_D(V)$, then V is a simple R-module with $fv = f(v)$, $f \in R$. $v \in V$.

exa:I_k **Example 2.11.** Let $n \geq 2$. If D is a division ring and $R = M_n(D)$, then each

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

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

Definition 2.12. A left ideal L of a ring R is said to be **minimal** if $L \neq \{0\}$ and L does not strictly contain other left ideals of R.

Similarly one defines right minimal ideals and minimal ideals.

Example 2.13. Let D be a division ring and let $R = M_n(D)$. Then $L = RE_{11}$ is a minimal left ideal.

Example 2.14. Let L be a non-zero left ideal. If $RL \neq \{0\}$, then L is minimal if and only if L is a simple R-module.

Definition 2.15. A left (resp. right) ideal L of R is said to be **regular** if there exists $e \in R$ such that $r - re \in L$ (resp. $r - er \in L$) for all $r \in R$.

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

Definition 2.16. A left (resp. right) ideal I of R is said to be **maximal** if $I \neq M$ and I is not properly contained in any other left (resp. right) ideal of R.

Similarly one defines maximal ideals.

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

proposition:R/I

Proposition 2.17. *Let R be a ring and M be a module. Then M is simple if and only if $M \simeq R/I$ for some maximal regular left ideal I.*

Proof. Assume that M is simple. Then $M = R \cdot m$ for some $m \neq 0$ by Lemma 2.9. The map $\phi\colon R \to M$, $r \mapsto r \cdot m$, is a surjective homomorphism of R-modules, so the first isomorphism theorem implies that $M \simeq R/\ker\phi$.

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

We claim that I is regular. Since $M = Rm$, 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 maximal left ideal that is regular. The correspondence theorem implies that R/I has no non-zero proper submodules.

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

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

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

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

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

Example 2.18. $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/n) = n\mathbb{Z}$.

Exercise 2.19. Let R be a ring and M be a module. If $N \subseteq M$ is a subset, then $\mathrm{Ann}_R(N)$ is a left ideal of R. If $N \subseteq M$ is a submodule of R, then $\mathrm{Ann}_R(N)$ is an ideal of R.

Definition 2.20. A module M is said to be **faithful** if $\mathrm{Ann}_R(M) = \{0\}$.

Example 2.21. If K is a field, then K^n is a faithful unitary $M_n(K)$-module.

Example 2.22. If V is vector space over a field K, then V is faithful unitary $\mathrm{End}_K(V)$-module.

Definition 2.23. 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.

xca:simple=>prim **Exercise 2.24.** If R is a simple unitary ring, then R is primitive.

xca:prim+conm=cuerpo **Exercise 2.25.** If R is a commutative ring (maybe without identity), then R is primitive if and only if R is a field.

Example 2.26. The ring $\mathbb{Z}$ is not primitive.

Lecture 4

04

Definition 2.27. An ideal P of a ring R is said to be **primitive** if $P = \mathrm{Ann}_R(M)$ for some simple R-module M.

lemma:primitivo

Lemma 2.28. *Let R be a ring and P be an ideal of R. Then P is primitive if and only if R/P is a primitive ring.*

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

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

Example 2.29. Let $R_1, \dots, R_n$ be primitive rings and $R = R_1 \times \cdots \times R_n$. Then each $P_i = R_1 \times \cdots \times R_{i-1} \times \{0\} \times R_{i+1} \times \cdots \times R_n$ is a primitive ideal of R since $R/P_i \simeq R_i$.

lemma:maxprim

Lemma 2.30. *Let R be a ring. If P is a primitive ideal, there exists a maximal left ideal I such that $P = \{x \in R : xR \subseteq I\}$. Conversely, if I is a maximal regular left ideal, then $\{x \in R : xR \subseteq L\}$ is a primitive ideal.*

Proof. Assume that $P = \mathrm{Ann}_R(M)$ for some simple R-module M. By Proposition 2.17, there exists a regular maximal left ideal I such that $M \simeq R/I$. Then $P = \mathrm{Ann}_R(R/I) = \{x \in R : xR \subseteq I\}$.

Conversely, let I a regular maximal left ideal. By Proposition 2.17, R/I is a simple R-module. Then

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

if a primitive ideal. □

xca:maximal=>prim

Exercise 2.31. Maximal ideals of unitary rings are primitive.

Exercise 2.32. Prove that every primitive ideal of a commutative ring is maximal.

Exercise 2.33. Prove that $M_n(R)$ is primitive if and only if R is primitive.

Let us discuss the Jacobson radical and radical rings.

Definition 2.34. Let R be a ring. The **Jacobson radical** $J(R)$ is the intersection of all the annihilators of simple left R-modules. If R does not have simple left R-modules, then $J(R) = R$.

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

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

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

Definition 2.35. An ideal I of R is **nilpotent** if $I^n = \{0\}$ for some $n \in \mathbb{Z}_{>0}$.

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

Definition 2.36. An element x of a ring is said to be **nil** (or nilpotent) if $x^n = 0$ for some $n \in \mathbb{Z}_{>0}$.

Definition 2.37. An ideal I of a ring is said to be nil if every element of I is nil.

Every nilpotent ideal is nil, as $I^n = 0$ implies $x^n = 0$ for all $x \in I$.

Example 2.38. Let $R = \mathbb{C}[x_1, x_2, \dots]/(x_1, x_2^2, x_3^3, \dots)$. The ideal $I = (x_1, x_2, x_3, \dots)$ is nil in R, as it is generated by nilpotent element. However, it is not nilpotente. 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 $x_{k+1}^k \neq 0$.

pro:nilJ **Proposition 2.39.** *Let R be a ring. Then every nil left ideal (resp. right ideal) is contained in $J(R)$.*

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

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

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

Definition 2.40. 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 $a + r + ar = 0$.

exercise:circ **Exercise 2.41.** Let R be a ring. Prove that $R \times R \to R$, $(r, s) \mapsto r \circ s = r + s + rs$, is an associative operation with neutral element 0.

Exercise 2.42. Let $R = \mathbb{Z}/3 = \{0,1,2\}$. Compute the multiplication table with respect to the circle operation given by the previous exercise.

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

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

Example 2.43. If $x \in R$ is a nilpotent element, then $y = \sum_{n\geq 1} x^n \in R$ is quasi-regular. En efecto, si existe N tal que $x^N = 0$, la suma que define al elemento y es finita y cumple que $y+(-x)+y(-x) = 0$.

Definition 2.44. A left ideal I of R is said to be **left quasi-regular** (resp. right quasi-regular) if every element of I is left quasi-regular (resp. right quasi-regular). A left ideal is said to be **quasi-regular** if it is left and right quasi-regular.

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

lemma:casiregular

Lemma 2.45. *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 $s \in R$ tal que $s\circ r = s+r+sr = 0$. Then s is right quasi-regular and

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

Let $(A,\leq)$ be a **partially order set**, this means that A is a set together with a reflexive, transitive and anti-symmetric binary relation R en $A\times A$, where $a\leq b$ if and only if $(a,b)\in R$. Recall that the relation is reflexive if $a\leq a$ for all $a\in A$, the relation is transitive if $a\leq b$ and $b\leq c$ imply that $a\leq c$ and the relation is anti-symmetric if $a\leq b$ and $b\leq a$ imply $a=b$. The elements $a,b\in A$ are said to be **comparable** if $a\leq b$ or $b\leq a$. An element $a\in A$ is said to be **maximal** if $c\leq a$ for all $c\in A$ that is comparable with a. An **upper bound** for a non-empty subset $B\subseteq A$ is an element $d\in A$ such that $b\leq d$ for all $b\in B$. A **chain** in A is a subset B such that every pair of elements of B are comparable. **Zorn's lemma** states the following property:

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

Our application of Zorn's lemma:

lemma:maxreg

Lemma 2.46. *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 $x\notin \operatorname{Ann}_R(R/M)$.*

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

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

Let $\mathcal{S}$ be the set of proper left ideals of R containing T partially ordered by inclusion. If $\{K_i : i \in I\}$ is a chain in $\mathcal{S}$, then $K = \cup_{i \in I} K_i$ is an upper bound for the chain (K is a proper, as $x \notin K$). Zorn's lemma implies that $\mathcal{S}$ admits a maximal element M. Thus M is a maximal left ideal such that $x \notin M$. Moreover, M is regular since $r - r(-x) \in T \subseteq M$ for all $r \in R$. Therefore R/M is a simple R-module by Proposition 2.17. Since $x(x + M) \neq 0$ (if $x^2 \in M$, then $x \in M$, as $x + x^2 \in T \subseteq M$), it follows that $x \notin \mathrm{Ann}_R(R/M)$. □

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

thm:casireg_eq

Theorem 2.47. *Let R be a ring and $x \in R$. The following statements are equivalent:*

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

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

We now prove (2) $\implies$ (3). If $x \notin J(R)$, then Lemma 2.46 implies that there exists a simple R-module M such that $xm \neq 0$ for some $m \in M$. The simplicity of M implies that $R(xm) = M$. Thus there exists $r \in R$ such that $rxm = -m$. There is an element $s \in R$ such that $s + rx + s(rx) = 0$ and hence

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

a contradiction.

Finally, to prove (3) $\implies$ (1) it is enough to note that x is left quasi-regular. Thus the left ideal generated by x is quasi-regular by Lemma 2.45. □

The theorem immediately implies the following corollary.

Corollary 2.48. *If R is a ring, then $J(R)$ if a quasi-regular ideal that contains every left quasi-regular ideal.*

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

thm:J(R)

Theorem 2.49. *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. We only prove the non-trivial inclusion. Let

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

By Proposition 2.17,

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

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

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

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

Example 2.50. Each maximal ideals of $\mathbb{Z}$ is of the form $p\mathbb{Z} = \{pm : m \in \mathbb{Z}\}$ for some prime number p. Thus $J(\mathbb{Z}) = \cap_p p\mathbb{Z} = \{0\}$.

We now review some basic results useful to compute radicals.

Proposition 2.51. *Let $\{R_i : i \in I\}$ be a family of rings. Then*

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

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

For the next result we shall need a lemma.

lemma:trickJ1

Lemma 2.52. *Let R be a ring and $x \in R$. If $-x^2$ is a left quasi-regular element, then x también.*

Proof. Sea $r \in R$ tal que $r + (-x^2) + r(-x^2) = 0$ y sea $s = r - x - rx$. Entonces x es casi-regular a izquierda pues

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

proposition:J(I)

Proposition 2.53. *If I is an ideal of R, then $J(I) = I \cap J(R)$.*

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

Let $x \in J(I)$ and $r \in R$. Since $-(rx)^2 = (-rxr)x \in I(J(I)) \subseteq J(I)$, the element $-(rx)^2$ is left quasi-regular a izquierda en I. Thus rx is left quasi-regular by Lemma 2.52. □

Definition 2.54. A ring R is said to be **radical** if $J(R) = R$.

Example 2.55. If R is a ring, then $J(R)$ is a radical ring, by Proposition 2.53.

Example 2.56. The Jacobson radical of $\mathbb{Z}/8$ is $\{0,2,4,6\}$.

There are several characterizations of radical rings.

theorem:anillo_radical

Theorem 2.57. *Let R be ring. The following statements are equivalent:*

1) *R is radical.*
2) *R admits no simple R-modules.*
3) *R no tiene ideales a izquierda maximales y regulares.*
4) *R no tiene ideales a izquierda primitivos.*
5) *Every element of R is quasi-regular.*
6) *$(R,\circ)$ is a group.*

Proof. The equivalence $(1) \iff (5)$ follows from Theorem 2.47.

The equivalence $(5) \iff (6)$ is left as an exercise.

Let us prove that $(1) \implies (2)$. Assume that there exists a simple R-module N. Since $R = J(R) \subseteq \mathrm{Ann}_R(N)$, $R = \mathrm{Ann}_S(N)$. Hence $RN = \{0\}$, a contradiction to the simplicity of N.

To prove $(2) \implies (3)$ we note that for each regular and maximal left ideal I, the quotient R/I is a simple R-module by Proposición 2.17.

To prove $(3) \implies (4)$ assume that there is a primitive left ideal $I = \mathrm{Ann}_R(M)$, where M is some simple R-module. Since $R = J(R) \subseteq I$, it follows that $I = R$, a contradiction to the simplicity of M.

Finally we prove $(4) \implies (2)$. If M is a simple R-module, then $\mathrm{Ann}_R(M)$ is a primitive left ideal. $\square$

Example 2.58. Let
$$A = \left\{ \frac{2x}{2y+1} : x, y \in \mathbb{Z} \right\}.$$
Then A is a radical ring, as the inverse of the element $\frac{2x}{2y+1}$ with respect to the circle operation $\circ$ is
$$\left(\frac{2x}{2y+1}\right)' = \frac{-2x}{2(x+y)+1}.$$

Definition 2.59. A ring R is said to be **nil** if for every $x \in R$ there exists $n = n(x)$ such that $x^n = 0$.

Exercise 2.60. Prove that a nil ring is a radical ring.

Exercise 2.61. 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.

thm:J(R/J)=0

Theorem 2.62. *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 module. Then M is a simple module over $R/J(R)$ with

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

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

Lecture 5

Theorem 2.63. *Let R be a ring and $n \in \mathbb{Z}_{>0}$. Then $J(M_n(R)) = M_n(J(R))$.*

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

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

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

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

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

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

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

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

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

Since $u^n=0$, the element

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

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

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

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

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

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

Exercise 2.64. Let R be a unitary ring. Then

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

xca:Jcon1

Exercise 2.65. Let R be a unitary ring. The following statements are equivalent:

1) $x\in J(R)$.
2) $xM=0$ 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) $1+\sum_{i=1}^n r_ixs_i$ is invertible for all n and all $r_i,s_i\in R$.
6) x belongs to every left maximal ideal maximal.

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

Exercise 2.66. A pair (X,r) is a **solution** to the Yang–Baxter equation if X is a set and $r\colon X\times X\to X\times X$ is a bijective map such that

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

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

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

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

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

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

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

Prove the following statements:

2) $\lambda\colon (R,\circ) \to \operatorname{Aut}(R,+)$, $x \mapsto \lambda_x$, is a group homomorphism.
3) $\mu\colon (R,\circ) \to \operatorname{Aut}(R,+)$, $y \mapsto \mu_y$, is a group antihomomorphism.
4) The map
$$r\colon R\times R \to R\times R, \quad r(x,y) = (\lambda_x(y), \mu_y(x)),$$
is an involutive non-degenerate solution.

Exercise 2.67. If D is a division ring and $R = D[X_1, \dots, X_n]$, then $J(R) = \{0\}$.

Example 2.68. A commutative and unitary ring R is **local** if it contains only one maximal ideal. If R is a local ring and M be 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.

xca:maximal_regular

Exercise 2.69. Let I be a proper left ideal that is left regular. Prove that I is contained in a maximal left ideal which is regular.

Theorem 2.70. *Let A be a K-algebra and I be a subset of A. Then I is a left regular maximal ideal of the algebra A if and only if I is a left regular maximal 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 $e \in R$ 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 maximal. There exists a left regular maximal ideal M of the ring A that contains I. Since M is left regular, it follows that M is a left regular maximal ideal of the ring A. Thus $M = I$ because I is maximal. $\square$

Exercise 2.71. Let A be an algebra. Prove that the Jacobson radical of the ring A coincides with the Jacobson radical of the algebra A.

§3. Amitsur's theorem

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

lemma:algebraico=nil

Lemma 3.1. *Let A be an algebra with one and let $x \in J(A)$. Then x is algebraic if and only if x is nil.*

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

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

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

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

for some $b_1, \dots, b_m \in K$. Since $1 + b_1 x + \cdots + b_m x^m$ is a unit by Exercise 2.65, it follows that $x^r = 0$. $\square$

An application:

pro:algebraica=>Jnil

Proposition 3.2. *If A is an algebraic algebra with one, then $J(A)$ is the largest nil ideal of A.*

Proof. The previous lemma implies that $J(A)$ is a nil ideal. Proposition 2.39 now implies that $J(A)$ is the largest nil ideal of A. $\square$

thm:Amitsur

Theorem 3.3 (Amitsur). *Let A be a K-algebra with one such that $\dim_K A < |K|$ (as cardinals). Then $J(A)$ is the largest nil ideal of A.*

Proof. If K is finite, then A is a finite-dimensional algebra. In particular, A is algebraic and hence $J(A)$ is a nil ideal by Proposition 3.2.

Assume that K is infinite and let $a \in J(A)$. Exercise 2.65 implies that every element of the form $1 - \lambda^{-1} a$, $\lambda \in K \setminus \{0\}$, is invertible. Thus

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

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

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

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

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

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

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

We claim that a is algebraic over K. Indeed,

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

is non-zero, as, for example, if $\beta_1\neq 1$, then $f(\lambda_1)=\beta_1(\lambda_1-\lambda_2)\cdots(\lambda_1-\lambda_n)\neq 0$ and $f(a)=0$. Since $a\in J(A)$ is algebraic, it follows a is nil by Lemma 3.1. □

Amitsur's theorem implies the following result.

Corollary 3.4. *Sea K un cuerpo no numerable y A una K-álgebra con base numerable. Entonces $J(A)$ es el mayor ideal nil de A.*

§4. Two open problems

We now conclude the lecture with two big open problems related with the Jacobson radical.

prob:Jacobson **Open problem 4.1 (Jacobson–Herstein).** Let R be a noetherian ring. Is then

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

Open problem 4.1 was originally formulated by Jacobson in 1956 [5] for one-sided noetherian rings. In 1965 Herstein [3] found a counterexample in the case of one-sided noetherian rings and reformulated the conjecture as it appears here.

Exercise 4.2 (Herstein). Let D be the ring of rationals with odd denominators. Let $R=\begin{pmatrix}D & \mathbb{Q}\\ 0 & \mathbb{Q}\end{pmatrix}$. Prove that R is right noetherian and $J(R)=\begin{pmatrix}J(D) & \mathbb{Q}\\ 0 & 0\end{pmatrix}$. Prove that $J(R)^n\supseteq\begin{pmatrix}0 & \mathbb{Q}\\ 0 & 0\end{pmatrix}$ and hence $\bigcap_n J(R)^n$ is non-zero.

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

prob:Koethe **Open problem 4.3 (Köthe).** Let R be a ring. Is the sum of two arbitrary nil left ideals of R is nil?

Open problem 4.3 is the well-known Köthe's conjecture. The conjecture was first formulated in 1930, see [6]. It is known to be true in several cases. In full generality, the problem is still open. In [7] 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 [10] Smoktunowicz found a counterexample to Amitsur's conjecture. This counterexample suggests that Köthe's conjecture might be false. A simplification of Smoktunowicz's example appears in [8]. See [11, 12] for more information on Köthe's conjecture and related topics.

Lecture 6

§5. Artinian modules

Definition 5.1. Let R be a ring. A module N is **artinian** if every decreasing sequence $N_1 \supseteq N_2 \supseteq \cdots$ of submodules of N stabilizes, that is there exists $n \in \mathbb{Z}_{>0}$ such that $N_n = N_{n+k}$ for all $k \in \mathbb{Z}_{>0}$.

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 $Y \subsetneq A$.

pro:artinian_minimal

Proposition 5.2. *A module N is artinian if and only if every non-empty subset of submodules of N contains a minimal element.*

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

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

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

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

Exercise 5.3. Prove that a ring R is left artinian if every sequence of left ideals $I_1 \supseteq I_2 \supseteq \cdots$ stabilizes.

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

Exercise 5.4. Let M be a module. The following statements are equivalent:

1) M is noetherian.
2) Every submodule of M is finitely generated.

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

Exercise 5.5. Prove that a ring R is left noetherian if every sequence of left ideals $I_1 \subseteq I_2 \subseteq \cdots$ stabilizes.

xca:AN_exact

Exercise 5.6. Let

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

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

Definition 5.7. A ring R is **left artinian** if the module ${}_R R$ is artinian.

Similarly one defines right artinian rings.

Example 5.8. 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.

def:serie_de_composicion

Definition 5.9. A **composition series** of the module M is a sequence

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

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

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

thm:serie_de_composicion

Theorem 5.10. *A non-zero module admits a composition series if and only if it is artinian and noetherian.*

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

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

is exact, it follows that M_{i+1} is artinian and noetherian, see Exercise 5.6.

Conversely, let M be an artinian and noetherian module. Let $M_0 = \{0\}$ and M_1 be minimal among the submodules of M (it exists by Proposition 5.2. If $M_1 \neq M$, let M_2 be minimal among those submodules of M such that $M_1 \subsetneq M_2$. This procedure produces a sequence

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

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

Definition 5.11. Let M be a module. We say that the composition series

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

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

thm:JordanHolder

Theorem 5.12 (Jordan–Hölder). *Any two composition series for a module are equivalent.*

Proof. Let M be a module and

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

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

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

Since V_1 has a composition series, V_1 is artinian and noetherian by Theorem 5.10. The submodule $U = V_1 \cap W_1$ is also artinian and noetherian and hence, by Theorem 5.10, it admits a composition series

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

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

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

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

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

Definition 5.13. Let M be a module with a composition series. The **length** $\ell(M)$ of M is defined as the length of any composition series of M.

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

Exercise 5.14. If N and Q are modules with composition series and

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

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

Exercise 5.15. If A and B are finite-length submodules of M, then

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

thm:Jnilpotente **Theorem 5.16.** *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 $r \in J^k \subseteq J(R)$ such that $rx = x$. Since $-r \in J(R)$ is left quasi-regular, there exists $s \in R$ such that $s - r - sr = 0$. Thus

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

a contradiction. □

Corollary 5.17. *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 2.39, L is contained in $J(R)$. Thus L is nilpotent, as $J(R)$ is nilpotent by Theorem 5.16. □

§6. 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 isomorphic to a (finite) direct sum of simple modules.

Definition 6.1. Let R be a ring. A left ideal L is said to be **minimal** if $L \neq \{0\}$ and there is no left ideal L_1 such that $\{0\} \subsetneq L_1 \subsetneq I$.

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

Proposition 6.2. *Let R be a left artinian ring. Then every non-zero left ideal contains a minimal left ideal.*

Proof. Let X be the family of non-zero left ideals contained in I. Then X is non-empty, as $I \in X$. Then X contains a minimal element by Proposition 5.2. □

A ring R with identity is **semisimple** if it is a direct sum of finitely many minimal left ideals. Note that ${}_RR$ is finitely generated by $\{1\}$. Minimal left ideals of R are exactly the simple submodules of ${}_RR$. This means that the ring R is semisimple if and only if the module ${}_RR$ is semisimple.

Proposition 6.3. *Let R be a semisimple ring. Then R is noetherian and artinian.*

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

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

is a composition series for ${}_RR$ with composition factors $L_1, \dots, L_n$. Since the module ${}_RR$ admits a composition series, it is artinian and noetherian by Theorem 5.10. It follows from the definitions that R is left artinian and left noetherian. □

Now it is possible to prove Artin–Wedderburn's theorem for rings. If R is a semisimple ring, then

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

for some $n_1, \dots, n_k \geq 1$ and some division rings $D_1, \dots, D_k$. The proof is somewhat the same we did for finite-dimensional algebras.

thm:SSartin=J

Theorem 6.4. *Let R be a unitary ring. Then R is semisimple if and only if R is left artinian and $J(R) = \{0\}$.*

We shall need a lemma.

lem:Jartiniano

Lemma 6.5. *Let R be a unitary left artinian ring. There exists finitely many maximal ideals $I_1, \dots, I_n$ of R such that $J(R) = I_1 \cap \cdots \cap I_n$.*

Proof. The set X of left ideals of the form $I_1 \cap \cdots \cap I_n$ for finitely many maximal ideals $I_1, \dots, I_n$ of R is non-empty, as R contains maximal ideals since it is a unitary ring. Since R is left artinian, Proposition 5.2 implies that X contains a minimal element, say $J = \bigcap_{i=1}^{k} I_i$. We claim that $J = J(R)$. Since R is unitary, $J(R)$ is the intersection of all maximal ideals of R and hence $J(R) \subseteq J$. Let us now prove that $J \subseteq J(R)$. If not, let $x \in J \setminus J(R)$. Then there exists a maximal ideal M such that $x \notin M$. This implies that $J \cap M \subsetneq J$, a contradiction to the minimality of J. □

We now prove the theorem.

Proof of Theorem 6.4. Assume first that R is semisimple. By Artin–Wedderburn's theorem,

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

for some $n_1, \dots, n_k \geq 1$ and some division rings $D_1, \dots, D_k$. In particular, R is left artinian and $J(R) = \prod_{i=1}^{k} J(M_{n_i}(D_i)) = \{0\}$ because each $M_{n_i}(D_i)$ is simple.

Conversely, the previous lemma implies that $\{0\} = J(R) = I_1 \cap \cdots \cap I_k$ for some maximal ideals $I_1, \dots, I_k$. Since each R/I_i is simple, it follows that $\prod_{i=1}^{k} R/I_i$ is semisimple. The map

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

is an ring homomorphism with kernel $I_1 \cap \cdots \cap I_k = \{0\}$. Thus it is injective and hence it follows that R is also semisimple. □

We now present an important result that uses semisimplicity.

thm:Hopkins-Levitski

Theorem 6.6 (Hopkins–Levitszki). *Let R be a unitary left artinian ring. Then R is left noetherian.*

Proof. Let $J = J(R)$. Since R is left artinian, J is a nilpotent ideal by Theorem 5.16. Let n be such that $J^n = \{0\}$. Now consider the sequence

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

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

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

if $x \in J$ and $y \in J^i$. Thus each J^i/J^{i+1} is a module over R/J. Since R/J is left artinian and $J(R/J) = \{0\}$ by Theorem 2.62, it follows from the previous proposition that R/J is semisimple. It follows that each J^i/J^{i+1} is semisimple and hence it is left noetheriano. Inductively one proves that each J^i is left noetherian and therefore R is left noetherian. □

Lecture 7

§7. Rickart's theorem

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

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

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

xc:K[G]notsimple

Exercise 7.1. If G is non-trivial, then $K[G]$ is not simple.

Exercise 7.2. Let $G=C_n$ be the (multiplicative) cyclic group of order n. Prove that $K[G]\simeq K[X]/(X^n-1)$.

Exercise 7.3. Let G be a finitely-generated torsion-free abelian group. Prove that $K[G]$ is a domain.

Exercise 7.4. Let G be a group and H be a subgroup of G. Let $\alpha\in K[H]$. Prove that α is invertible (resp. left zero divisor) in $K[H]$ if and only if α is invertible (resp. left zero divisor) in $K[G]$.

Exercise 7.5. Let G be a group and $\alpha=\sum_{g\in G}\lambda_g g\in K[G]$. The **support** of α is the set

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

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

Exercise 7.6. Let $G=C_2=\langle g\rangle\simeq\mathbb{Z}/2$ the (multiplicative) group with two elements. Note that every element of $K[G]$ is of the form $a1+bg$ for some $a,b\in K$. Prove the following statements:

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

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

is an algebra isomorhism.
2) If the characteristic of K is two, then

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

is an algebra isomorphism.

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

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

is an algebra homomorphism.

Exercise 7.7. Let $G = C_3$ be the (multiplicative) group of three elements. Prove that $\mathbb{R}[G] \simeq \mathbb{R} \times \mathbb{C}$.

Exercise 7.8. Let $G = \langle r, s : r^3 = s^2 = 1, srs = r^{-1} \rangle$ be the dihedral group of six elements. Prove the following statements:

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

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

s semisimplicity problem **Open problem 7.9.** Let G be a group and K be a field. When $J(K[G]) = \{0\}$?

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

thm:Rickart **Theorem 7.10 (Rickart).** *Let G be a group. Then $J(\mathbb{C}[G]) = \{0\}$.*

To prove the theorem we need a lemma.

Lemma 7.11. *Let G be a group. Then $J(\mathbb{C}[G])$ is nil.*

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

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

where $\lambda_1,\dots,\lambda_n \in \mathbb{C}$ and $g_1,\dots,g_n \in G$. Let $H = \langle g_1,\dots,g_n\rangle$. Then $g \in \mathbb{C}[H]$ and H is countable. We claim that $g \in J(\mathbb{C}[H])$. 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 $\mathbb{C}[H]$. 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 $\kappa(1-\beta\alpha) \in K \cap \mathbb{C}[H] = \{0\}$. Since $1 = \gamma_1(1-\beta\alpha)$, it follows that $\alpha \in J(\mathbb{C}[H])$ and the lemma follows from Amitsur's theorem. □

We now prove the theorem.

Proof of Theorem 7.10. For $\alpha = \sum_{i=1}^n \lambda_i g_i \in \mathbb{C}[G]$ let

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

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

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

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

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

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

To obtain a consequence of Rickart's theorem we need two lemmas.

lem:Nakayama **Lemma 7.12 (Nakayama).** *Let R be a unitary ring and M be a finitely generated module. If $J(R)\cdot M = M$, then $M = \{0\}$.*

Proof. Since M is finitely generated, we may assume that $M = (x_1,\dots,x_n)$. 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 $s(1-r_n) = 1$. Thus $x_n = \sum_{j=1}^{n-1}(sr_j)\cdot x_j$ and hence $M = (x_1,\dots,x_{n-1})$. Repeating this procedure several times one obtains $M = \{0\}$. □

lem:Rickart **Lemma 7.13.** *Let $\iota\colon R \to S$ be a homomorphism of unitary rings. If*

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

where each x_j is such that $x_j y = yx_j$ 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. If is M is a simple module over S, then, in particular, $M = S \cdot m$ for some $m \neq 0$. Now M is a module over R with $r \cdot m = \iota(r) \cdot m$. Since

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

it follows that M is finitely generated as a module over $\iota(R)$. Moreover,

$$J(R) \cdot M = J \cdot M = \iota(J) \cdot M$$

is an S-submodule of M, as

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

Since $M \neq \{0\}$, Nakayama's lemma implies that $J(R) \cdot M \subsetneq M$. The simplicity of the S-module M implies that $J(R) \cdot M = \{0\}$. $\square$

We now obtain the following consequence of Rickart's theorem.

Theorem 7.14. *If G is a group, then $J(\mathbb{R}[G]) = 0$.*

Proof. Let $\iota \colon \mathbb{R}[G] \to \mathbb{C}[G]$ be the canonical inclusion. Since

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

Lemma 7.13 and Rickart's theorem imply that $\iota(J(\mathbb{R}[G])) \subseteq J(\mathbb{C}[G]) = 0$. Thus $J(\mathbb{R}[G]) = 0$, as ι is injective. $\square$

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

Lemma 7.15. *Let M be a semisimple module and N be a submodule. Then N is a direct summand.*

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

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

pro:KGsemisimple **Proposition 7.16.** *If G is an infinite group, then $\mathbb{C}[G]$ is not semisimple.*

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

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

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

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

Thus $\lambda_h = \lambda_{g^{-1}h}$ for all $g, h \in G$, a contradiction because $f \neq 0$ implies that the sum that defines f should be an infinite sum. □

Theorem 7.17. *Let G be a group. Then $\mathbb{C}[G]$ is left artinian if and only if G is finite.*

Proof. If G is finite, then $\mathbb{C}[G]$ is left artinian because $\dim \mathbb{C}[G] = |G| < \infty$. So assume that G is infinite. By Rickart's theorem, $J(\mathbb{C}[G]) = 0$. Moreover, $\mathbb{C}[G]$ is not semisimple by the previous proposition. Thus $\mathbb{C}[G]$ is not left artinian by Theorem 6.4. □

§8. Maschke's theorem

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

Theorem 8.1 (Maschke). *Let G be a finite group. Then $J(K[G]) = 0$ if and only if the characteristic of K is zero or does not divide the order of G.*

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

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

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

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

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

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

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

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

Conversely, let K be a field of prime characteristic and that this primes 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,

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

it follows that I is a nilpotent non-zero ideal. Thus $J(K[G]) \neq \{0\}$, as Proposition 2.39 yields $I \subseteq J(K[G])$. □

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:

cor:GfinitoNOnil **Corollary 8.2.** *Sea G un grupo finito. Entonces $K[G]$ no contiene ideales a izquierda nil no nulos.*

§9. Herstein's theorem

Our aim now is to answer the following question: When a group algebra is algebraic? A partial answer is given by Herstein's theorem.

Definition 9.1. A group G is **locally finite** if every finitely generated subgroup of G is finite.

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

Example 9.2. Every finite group is locally finite

Example 9.3. The group $\mathbb{Z}$ is not locally finite because it is torsion-free.

Example 9.4. Let p be a prime number. The **Prüfer's group**

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

formed by of all p-roots of one, is locally finite.

Example 9.5. Let X be an infinite set and $\mathbb{S}_X$ be the set of bijective maps $X \to X$ moving only finitely many elements of X. Then $\mathbb{S}_X$ is locally finite.

pro:exact_LI

Proposition 9.6. *Let G be a group and N be a normal subgroup of G. If N and G/N are locally finite, then G is locally finite.*

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

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

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

$$g_ig_jg_l = u_{ij}g_kg_l = u_{ij}u_{kl}g_t = ug_t$$

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 $|H| \le m|U|$. □

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

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = G \tag{7.1}$$

eq:resoluble

where each G_i is normal in G_{i+1} and each quotient G_i/G_{i-1} is abelian. A group G is a **torsion** group if every element of G has finite order.

Proposition 9.7. *If G is a solvable torsion group, then G is locally finite.*

Proof. We proceed by induction on n, the length of the sequence (7.1). If $n = 1$, then G is finite because it is abelian and a torsion group. Now assume the result holds for group with resolubility length $n-1$ and let G be a solvable group with a sequence (7.1). By the inductive hypothesis, the normal subgroup G_{n-1} of G is locally finite. Since G/G_{n-1} is an abelian torsion group, it is locally finite, the result now follows from Proposition 9.6. □

We now prove Herstein's theorem.

Theorem 9.8 (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 thast G is locally finite. Let $\alpha \in K[G]$. The subgroup $H = \langle \operatorname{supp}\alpha\rangle$ is finite, as it is finitely generated. Since $\alpha \in K[H]$ and $\dim_K K[H] < \infty$, the set $\{1,\alpha,\alpha^2,\dots\}$ is linearly dependent. Thus α is algebraic over K.

Let $\{x_1,\dots,x_m\}$ be a finite subset of G. Adding inverses if needed, we may assume that $\{x_1,\dots,x_m\}$ generates the subgroup $H = \langle x_1,\dots,x_m\rangle$ as a semigroup. If $\alpha = x_1+\cdots+x_m \in K[G]$, then, since α is algebraic over K,

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

for some $n \geq 0$ and $a_0, \ldots, x_n \in K$. Let $w = x_{i_1} \cdots x_{i_{n+1}} \in H$ be a word of length $n+1$. There exist positive integers $c_{i_1 \cdots i_m}$ such that

$$\alpha^{n+1} = (x_1 + \cdots + x_m)^{n+1} = \sum_{\substack{i_1+\cdots+i_m=n+1 \\ i_j \text{ enteros positivos}}} c_{i_1 \cdots i_m} x_1^{i_1} \cdots x_m^{i_m}.$$

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

Lecture 8

§10. Formanek's theorem, I

xca:invertible_algebraic **Exercise 10.1.** Let A be an algebraic algebra and $a \in A$.

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

exa:norma **Exercise 10.2.** For $\alpha = \sum_{g \in G} \alpha_g g \in \mathbb{C}[G]$ let $|\alpha| = \sum_{g \in G} |\alpha_g| \in \mathbb{R}$. Prove the following statements:

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

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

thm:FormanekQ **Theorem 10.3 (Formanek).** *Let G be a group. If every element of $\mathbb{Q}[G]$ is invertible or a zero divisor, then G is locally finite.*

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

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

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

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

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

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

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

Then

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

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

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

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

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

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

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

§11. Formanek's theorem, II

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 it is clear from the context. For $u \in U$ and $v \in V$ we write $u\otimes v$ to denote the coset $(u,v)+T$.

Theorem 11.1. *Let U and V be vector spaces. Then there exists a bilinear map $U\times V \to U\otimes V$, $(u,v)\mapsto u\otimes v$, such that each element of $U\otimes V$ is a finite sum of the form*

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

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

Proof. By definition, the map

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

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

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

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

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

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

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

xca:tensorial_unicidad

Exercise 11.2. Prove that the properties of the previous theorem characterize tensor products up to isomorphism.

Some properties:

Proposition 11.3. *Let $\varphi\colon U\to U_1$ and $\psi\colon V\to V_1$ be linear maps. There exists a unique linear map $\varphi\otimes\psi\colon U\otimes V\to U_1\otimes V_1$ such that*

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

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

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

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

is well-defined. □

Exercise 11.4. Prove the following statements:

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

The following proposition is extremely useful:

Proposition 11.5. *If U and V are vector spaces, then $U\otimes V\simeq V\otimes U$.*

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

xca:UxVxW

Exercise 11.6. Prove that $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$.

xca:UxK

Exercise 11.7. Prove that $U \otimes K \simeq K \simeq K \otimes U$.

pro:U_LI

Proposition 11.8. *Let U and V be vector spaces. If $\{u_1, \dots, u_n\}$ is a linearly independent subset of U and $v_1, \dots, v_n \in V$ is such that $\sum_{i=1}^n u_i \otimes v_i = 0$, then $v_i = 0$ for all $i \in \{1, \dots, n\}$.*

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

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

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

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

xca:uxv=0

Exercise 11.9. Prove that $u \otimes v = 0$ and $v \neq 0$ imply $u = 0$.

Theorem 11.10. *Let U and V be vector spaces. If $\{u_i : i \in I\}$ is a basis of U and $\{v_j : j \in J\}$ is a basis of V, then $\{u_i \otimes v_j : i \in I, j \in J\}$ is a basis of $U \otimes V$.*

Proof. The $u_i \otimes v_j$ are generators of $U \otimes V$, as $u = \sum_i \lambda_i u_i$ and $v = \sum_j \mu_j v_j$ imply $u \otimes v = \sum_{i,j} \lambda_i \mu_j u_i \otimes v_j$. We now prove that the $u_i \otimes v_j$ are linearly independent. We need to show that each finite subset of the $u_i \otimes v_j$ is linearly independent. If $\sum_k \sum_l \lambda_{kl} u_{i_k} \otimes v_{j_l} = 0$, then $0 = \sum_k u_{i_k} \otimes \left(\sum_l \lambda_{kl} v_{j_l}\right)$. Since the u_{i_k} are linearly independent, Proposition 11.8 implies that $\sum_l \lambda_{kl} v_{j_l} = 0$. Thus $\lambda_{kl} = 0$ for all k, l, as the v_{j_l} are linearly independent. □

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

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

Corollary 11.11. *If $\{u_i : i \in I\}$ is basis of U, then every element of $U \otimes V$ can be written uniquely as a finite sum $\sum_i u_i \otimes v_i$.*

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

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

xca:tensor_algebras **Exercise 11.12.** Let A and B be algebras. Prove that $A \otimes B$ is an algebra with

$$(a \otimes b)(x \otimes y) = ax \otimes by.$$

Exercise 11.13. Prove the following statements:

1) $A \otimes B \simeq B \otimes A$.
2) $(A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$.
3) $A \otimes K \simeq A \simeq K \otimes A$.
4) If $A \otimes A_1$ and $B \otimes B_1$, then $A \otimes B \simeq A_1 \otimes B_1$.

Some examples:

Proposition 11.14. *If G and H are groups, then $K[G] \otimes K[H] \simeq K[G \times H]$.*

Proof. The set $\{g \otimes h : g \in G, h \in H\}$ is a basis of $K[G] \otimes K[H]$ and the elements of $G \times H$ form a basis of $K[G \times H]$. There exists a linear isomorphism

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

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

pro:AKX=AX **Proposition 11.15.** *If A is an algebra, then $A \otimes K[X] \simeq A[X]$.*

Proof. Each element of $A \otimes K[X]$ can be written uniquely as a finite sum of the form $\sum a_i \otimes X^i$. Routine calculations show that $A \otimes K[X] \mapsto A[X]$, $\sum a_i \otimes X^i \mapsto \sum a_i X^i$, is a linear algebra isomprhism. □

xca:AM=MA **Exercise 11.16.** Prove that if A is an algebra, then $A \otimes M_n(K) \simeq M_n(A)$. In particular, $M_n(K) \otimes M_m(K) \simeq M_{nm}(K)$.

Proposition 11.15 and Exercise 11.16 are examples of a procedure known as **scalar extensions**.

Theorem 11.17. *Let A be an algebra over K and E be an extension of K (this just simply means that K is a subfield of E). Then $A^E = E \otimes_K A$ is an algebra over E with respect to the scalar multiplication*

$$\lambda(\mu \otimes a) = (\lambda\mu) \otimes a,$$

for all $\lambda, \mu \in E$ and $a \in A$.

Proof. Let $\lambda \in E$. Since $E \times A \to E \otimes_K A$, $(\mu, a) \mapsto (\lambda\mu) \otimes a$, is K-bilinear, there exists a linear map $E \otimes_K A \to E \otimes_K A$, $\mu \otimes a \mapsto (\lambda\mu) \otimes a$. The scalar multiplication is then well-defined and

$$\lambda(u + v) = \lambda u + \lambda v$$

for all $\lambda \in E$ and $u, v \in E \otimes_K A$. Moreover,

$$(\lambda + \mu)u = \lambda u + \mu u, \quad (\lambda\mu)u = \lambda(\mu u), \quad \lambda(uv) = (\lambda u)v = u(\lambda v)$$

for all $u, v \in E \otimes_K A$ and $\lambda, \mu \in E$. □

Exercise 11.18. Prove the following statements:

1) $\{1\} \otimes A$ is a subalgebra of A^E isomorphic to A.
2) If $\{a_i : i \in I\}$ is a basis of A, then $\{1 \otimes a_i : i \in I\}$ is a basis of A^E.

Exercise 11.19. Prove that if G is a group and K is a subfield of E, then $E \otimes_K K[G] \simeq E[G]$.

Now we prove Formanek's theorem:

Theorem 11.20 (Formanek). *Let K be a field of characteristic zero and let G be a group. If every element of $K[G]$ is invertible or a zero divisor, then G is locally finite.*

Proof. Since K is of characteristic zero, $\mathbb{Q} \subseteq K$. Then $K[G] \simeq K \otimes_{\mathbb{Q}} \mathbb{Q}[G]$. Each $\beta \in K \otimes_{\mathbb{Q}} \mathbb{Q}[Q]$ can be written uniquely as

$$\beta = 1 \otimes \beta_0 + \sum k_i \otimes \beta_i,$$

where $\{1, k_1, k_2, \dots,\}$ is a basis of K as a $\mathbb{Q}$-vector space. Let $\alpha \in \mathbb{Q}[G]$ and let $\beta \in K[G]$ be such that $\alpha\beta = 1$. Since

$$1 \otimes 1 = (1 \otimes \alpha)\beta = 1 \otimes \alpha\beta_0 + \sum k_i \otimes \alpha\beta_i,$$

it follows that $\alpha\beta_0 = 1$. Similarly, if $\alpha\beta = 0$, then $\alpha\beta_j = 0$ for all j. Since each $\alpha \in \mathbb{Q}[G]$ is invertible or a zero divisor, Formanek's theorems for $\mathbb{Q}$ applies. □

§12. Primitive and semiprimitive rings

Definition 12.1. A ring R is **semiprimitive** (or Jacobson semisimple) if $J(R) = \{0\}$.

In §2 (Lecture 3) we defined primitive rings as those rings that have a faithful simple module. We claim that primitive rings are semiprimitive. If R is primitive, then $\{0\}$ is a primitive ideal. Since $J(R)$ is the intersection of primitive ideals, it follows that $J(R) = \{0\}$.

Example 12.2. If $R = \prod_{i \in I} R_i$ is a direct product of semiprimitive rings, then R is semiprimitive, as

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

Example 12.3. $\mathbb{Z}$ is semiprimitive, as $J(\mathbb{Z}) = \cap_p \mathbb{Z}/p = \{0\}$.

exa:C[a,b] **Example 12.4.** Let $R = C[a,b]$ be the ring of continuous maps $f\colon [a,b] \to \mathbb{R}$. In this case $J(R)$ is the intersection of all maximal ideals of R. Note that each maximal ideal of R is of the form

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

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

We proved in Theorem 2.62 (Lecture 4) that $R/J(R)$ is semiprimive.

Definition 12.5. Let $\{R_i : i \in I\}$ be a collection of rings. A subring R of $\prod_{i \in I} R_i$ is said to be a **subdirect product** of the collection if each $\pi_j\colon R \to R_j$, $(r_i)_{i \in I} \mapsto r_j$, is surjective.

thm:subdirecto **Theorem 12.6.** *Let R be a non-zero ring. Then R is semiprimitive if and only if R is isomorphic to a subdirect product of primitive rings.*

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

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

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

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

Example 12.7. $\mathbb{Z}$ is isomorphic to a subdirect product of the fields $\mathbb{Z}/p$, where p runs over all prime numbers.

Example 12.8. The ring $C[a,b]$ of Example 12.4 is isomorphic to a subdirect product of the fields $C[a,b]/U_c \simeq \mathbb{R}$.

Definition 12.9. A ring R **semiprime** if $aRa = \{0\}$ implies $a = 0$.

Proposition 12.10. *Let R be a ring. The following statements are equivalents:*

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 $I^2 = \{0\}$. By assumption, $RaR = I = \{0\}$. Thus Ra and aR are ideals such that $(Ra)R = R(aR) = \{0\}$. This implies that $\mathbb{Z}a$ is an ideal of R such that $(\mathbb{Z}a)R = \{0\}$ and hence $a = 0$. ◻

Two consequences:

Corollary 12.11. *A commutative ring is semiprime if and only if it does not contain non-zero nilpotent elements.*

Corollary 12.12. *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 2.39, it follows that $\mathbb{C}[G]$ does not contain non-trivial nil ideals. Thus $\mathbb{C}[G]$ does not contain non-trivial nilpotent ideals and hence $\mathbb{C}[G]$ is semiprime. ◻

Exercise 12.13. Prove that $Z(\mathbb{C}[G])$ is semiprime.

Exercise 12.14. Let D be a division ring.

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

§13. Jacobson's density theorem

Definition 13.1. Let D be a division ring and V be a vector space over D. A subring $R \subseteq \mathrm{End}_D(V)$ is **dense** in V if for all $n \in \mathbb{Z}_{>0}$, each linearly independent set $\{u_1, \dots, u_n\} \subseteq V$ and each (not necessarily linearly independent) subset $\{v_1, \dots, v_n\} \subseteq V$ there exists $f \in R$ such that $f(u_j) = v_j$ for all $j \in \{1, \dots, n\}$.

lem:unico_denso

Lemma 13.2. *Sea D un anillo de división V un D-espacio vectorial de dimensión finita. Entonces* $\operatorname{End}_D(V)$ *es el único anillo denso en* V.

Proof. Sea R denso en V y sea $\{v_1,\dots,v_n\}$ una base de V. Por definición, $R \subseteq \operatorname{End}_D(V)$. Si $g \in \operatorname{End}_D(V)$ entonces, como R es denso en V, existe $f \in R$ tal que $f(v_j) = g(v_j)$ para todo $j \in \{1,\dots,n\}$. Luego $g = f \in R$. □

lem:ideal_denso

Lemma 13.3. *Sea R un anillo denso en V y sea I un ideal no nulo de R. Entonces I es denso en V.*

Proof. Sea I un ideal no nulo de R. Sean $h \in I \setminus \{0\}$ y $u \in V$ tales que $h(u) = v \neq 0$. Sea $\{u_1,\dots,u_n\} \subseteq V$ un conjunto linealmente independiente y sea $\{v_1,\dots,v_n\} \subseteq V$. Como R es denso en V, existen $g_1,\dots,g_n \in R$ tales que $g_i(u_i) = u$ y $g_i(u_j) = 0$ si $i \neq j$. Existen además $f_1,\dots,f_n \in R$ tales que $f_i(v) = v_i$. Entonces $\gamma = \sum_{i=1}^n f_i h g_i \in I$ cumple que $\gamma(u_j) = v_j$ para todo $j \in \{1,\dots,n\}$. □

thm:density

Theorem 13.4 (Jacobson). *A ring R is primitive if and only if it is isomorphic to a dense ring in a vector space over a division ring.*

Proof. Si R es isomorfo a un anillo denso en un D-módulo V donde D es un anillo de división, entonces R es primitivo pues V es un módulo simple y fiel. Es fiel: si $f \in \operatorname{Ann}_R(V)$ entonces $f = 0$ pues $f(v) = 0$ para todo $v \in V$. Es simple pues si $W \subseteq V$ es un submódulo no nulo, $v \in V$ y $w \in W \setminus \{0\}$ entonces existe $f \in R$ tal que $v = f(w) \in W$.

Supongamos ahora que R es primitivo y sea V un módulo simple y fiel. Por el lema de Schur, $D = \operatorname{End}_R(V)$ es un anillo de división. Luego V es un D-espacio vectorial con las operaciones

$$\delta v = \delta(v), \quad \delta(rv) = r(\delta v), \quad v \in V, r \in R, \delta \in D.$$

Para $r \in R$ definimos

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

Es fácil ver que $\gamma_r \in \operatorname{End}_D(V)$ y que la función $R \to \operatorname{End}_D(V)$, $r \mapsto \gamma_r$, es un morfismo de anillos. Como V es fiel, $R \simeq \gamma(R) = \{\gamma_r : r \in R\}$ (si $\gamma_r = \gamma_s$ entonces $rv = \gamma_r(v) = \gamma_s(v) = sv$ para todo $v \in V$ y luego $r = s$ pues $(r-s)v = 0$ para todo $v \in V$).

Claim. Si U es un subespacio de V de dimensión finita, para cada $w \in V \setminus U$ existe $r \in R$ tal que $\gamma_r(U) = 0$ y $\gamma_r(w) \neq 0$.

Supongamos que la afirmación no es cierta y sea U un contraejemplo de la mínima dimensión posible. Entonces $\dim_D U \geq 1$ (pues el resultado es cierto para el subespacio nulo). Sea U_0 un subespacio de U tal que $\dim U_0 = \dim U - 1$ y sea

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

Como por la minimalidad de U nuestra afirmación es cierta para U_0, para cualquier $v \in V \setminus U_0$ se tiene que $Lv = V$ (pues existe $l \in L$ tal que $lv = \gamma_l(v) \neq 0$, y como L es ideal a izquierda de R sabemos que $Lv \subseteq V$ es un submódulo y V es simple).

Sea $w \in V \setminus U$ tal que nuestra afirmación no es cierta y sea $u \in U \setminus U_0$. La función

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

donde $v = lu \in Lu = V$ (que depende de u y w) está bien definida: si $l_1, l_2 \in L$ son tales que $v = l_1 u = l_2 u$ entonces $(l_1 - l_2)u = 0$ y luego

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

Además δ es morfismo de R-módulos pues si $l \in L$ es tal que $v = lu$ entonces

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

para todo $r \in R$.

Para todo $l \in L$ se tiene que

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

y entonces $L(\delta(u) - w) = 0$. Pero esto implica que $\delta(u) - w \notin V \setminus U_0$, es decir $\delta(u) - w \in U_0$. Luego

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

una contradicción.

Esta afirmación alcanza para demostrar el teorema. En efecto, sean $u_1, \dots, u_n \in V$ vectores linealmente independientes y sean $v_1, \dots, v_n \in V$ vectores arbitrarios. Si fijamos $i \in \{1, \dots, n\}$, la afirmación anterior con

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

y $w = u_i$ nos dice que existe $r_i \in R$ tal que $\gamma_{r_i}(u_j) = 0$ si $j \neq i$ y $\gamma_{r_i}(u_i) \neq 0$. Como además existe $s_i \in R$ tal que $\gamma_{s_i}\gamma_{r_i}(u_i) = v_i$, se concluye que el elemento $r = \sum_{j=1}^{n} s_j r_j \in R$ es tal que $\gamma_r(u_i) = v_i$ para todo $i \in \{1, \dots, n\}$. $\square$

Corollary 13.5. *Si R es un anillo primitivo, entonces existe un anillo de división D tal que $R \simeq \operatorname{End}_D(V)$ para algún D-espacio vectorial V de dimensión finita, o bien para todo $m \in \mathbb{Z}_{>0}$ existe un subanillo R_m de R y un morfismo de anillos sobreyectivo $R_m \to \operatorname{End}_D(V_m)$ para algún D-espacio vectorial V_m tal que $\dim_D V_m = m$.*

Proof. Sabemos que R admite un módulo V simple y fiel. Además, como R es primitivo, por el teorema **??** podemos suponer que existe un anillo de división D tal que R es denso en un D-espacio vectorial V. Sea $\gamma\colon R \to \operatorname{End}_D(V)$, $r \mapsto \gamma_r$, donde $\gamma_r(v) = rv$. Como V es fiel, γ es inyectiva. Luego $R \simeq \gamma(R)$.

Si V es de dimensión finita, el resultado se obtiene del lema 13.2. Supongamos entonces que V es de dimensión infinita y sea $\{u_1, u_2, \dots\}$ un conjunto linealmente independiente. Para cada $m \in \mathbb{Z}_{>0}$ sea V_m el subespacio generado por $\{u_1, \dots, u_m\}$ y sea $R_m = \{r \in R : rV_m \subseteq V_m\}$. Es fácil ver que R_m es un subanillo de R. Como R es denso en V, la función

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

es un morfismo sobreyectivo de anillos. □

En álgebra conmutativa los dominios juegan un papel fundamental. En álgebra no conmutativa las cosas no son tan similares ya que el anillo $M_n(K)$ no es un dominio. Nos interesa entonces encontrar un concepto similar al de dominio que funcione en el contexto no conmutativo.

Definition 13.6. Sea R un anillo (no necesariamente con unidad). Diremos que R es **primo** si dados $x, y \in R$ tales que $xRy = 0$ entonces $x = 0$ o bien $y = 0$.

Example 13.7. Recordemos que un anillo R es un **dominio** si $xy = 0$ implica que $x = 0$ o bien $y = 0$. Todo dominio es trivialmente un anillo primo.

Example 13.8. Un anillo conmutativo es primo si y sólo si es un dominio pues $ab = 0$ si y sólo si $aRb = 0$.

Example 13.9. Un ideal no nulo de un anillo primo es un anillo primo.

Lemma 13.10. *Sea R un anillo. Son equivalentes:*

1) *R es primo.*
2) *Si I y J son ideales a izquierda tales que $IJ = 0$ entonces $I = 0$ o bien $J = 0$.*
3) *Si I y J son ideales tales que $IJ = 0$ entonces $I = 0$ o bien $J = 0$.*

Proof. Veamos primero que (1) $\implies$ (2). Sean I y J ideales a izquierda tales que $IJ = 0$. Entonces $IRJ = I(RJ) \subseteq IJ = 0$. Supongamos que $J \neq 0$. Si $u \in I$ y $v \in J \setminus \{0\}$, entonces $uRv \in IRJ = 0$ y luego $u = 0$.

La implicación (2) $\implies$ (3) es trivial.

Veamos entonces que (3) $\implies$ (1). Sean $x, y \in R$ tales que $xRy = 0$. Sean $I = RxR$ y $J = RyR$. Como $IJ = (RxR)(RyR) = R(xRy)R = 0$, por hipótesis, podemos suponer que entonces $I = 0$. En particular Rx y xR son ideales pues $R(xR) = (Rx)R = 0$. Pero entonces $\mathbb{Z}x$ es un ideal de R tal que $(\mathbb{Z}x)R = 0$. Luego $x = 0$. □

Example 13.11. Todo anillo simple es trivialmente primo. La afirmación recíproca no es cierta: $\mathbb{Z}$ es un anillo primo (por ser un dominio) pero no es simple.

Example 13.12. Si R_1 y R_2 son anillos, $R = R_1 \times R_2$ no es primo pues $I = R_1 \times 0$ y $J = 0 \times R_2$ son ideales no nulos tales que $IJ = 0$.

lem:primoizqmin=>prim

Lemma 13.13. *Sea R un anillo primo y sea L un ideal a izquierda minimal de R. Entonces R es primitivo.*

Proof. Como L es ideal a izquierda minimal, es simple como R-módulo. Veamos que como R es primo, L es fiel. Sea $y \in L \setminus \{0\}$ y sea $x \in \mathrm{Ann}_R(L)$. Entonces, como $xRy \in xRL \subseteq xL = 0$, se concluye que $x = 0$. □

lem:denso_artiniano

Lemma 13.14. *Sea D un anillo de división y sea R un anillo denso en un D-espacio vectorial V. Si R es artiniano a izquierda, entonces V es de dimensión finita.*

Proof. Supongamos que V tiene dimensión infinita y sea $\{u_1, u_2, \dots,\}$ un subconjunto de V linealmente independiente. Como $R \subseteq \operatorname{End}_D(V)$, V es un R-módulo con $f \cdot v = f(v)$, donde $f \in R$ y $v \in V$. Para cada $n \in \mathbb{Z}_{>0}$ sea

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

Los I_j son ideales a izquierda de R tales que $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$. Veamos que esta sucesión no se estabiliza: Sean $n \in \mathbb{Z}_{>0}$ y $v \in V \setminus \{0\}$. Como R es denso en V, existe $f \in R$ tal que $f(u_j) = 0$ para todo $j \in \{1, \dots, n\}$ y $f(u_{n+1}) = v \neq 0$. Luego $I_1 \supsetneq I_2 \supsetneq \cdots \supsetneq I_n \supsetneq \cdots$, una contradicción pues R es artiniano a izquierda. □

Theorem 13.15 (Wedderburn). *Sea R un anillo artiniano a izquierda. Las siguientes afirmaciones son equivalentes:*

1) *R es simple.*
2) *R es primo.*
3) *R es primitivo.*
4) *$R \simeq M_n(D)$ para algún n y algún anillo de división D.*

Proof. La implicación $(1) \implies (2)$ es trivial.

Para demostrar que $(2) \implies (3)$ basta observar que como R es artiniano, R tiene un ideal a izquierda minimal. Por el lema 13.13, R es primitivo.

Veamos que $(3) \implies (4)$. Si R es primitivo, por el teorema de densidad de Jacbonson, existe un anillo de división D tal que R es isomorfo a un anillo S que es denso en un D-espacio vectorial V. Como R es artiniano a izquierda, el lema 13.14 implica que $R = \operatorname{End}_D(V) \simeq M_n(D)$ pues $\dim_D V < \infty$.

Por último, $(4) \implies (1)$ es trivial pues $M_n(D)$ es simple. □

Para completar nuestra presentación del teorema de Wedderburn, veremos que la descomposición es única. Necesitaremos dos lemas previos:

lem:wedderburn_unididad **Lemma 13.16.** *Sea D un anillo de división. Entonces*

$$D^{\mathrm{op}} \simeq \operatorname{End}_{M_n(D)}(D^n).$$

Proof. Sea

$$\phi\colon D^{\mathrm{op}} \to \operatorname{End}_{M_n(D)}(D^n), \qquad d \mapsto \phi(d)\colon D^n \to D^n,$$

donde $\phi(d)(x) = xd$. Es evidente que ϕ es lineal; es morfismo pues además

$$\phi(d_1 \cdot_{\mathrm{op}} d_2)(x) = \phi(d_2 d_1)(x) = x(d_2 d_1) = (x d_2) d_1 = \phi(d_1)\phi(d_2)(x).$$

Como ϕ es no nulo y D^{op} es es simple por ser de división, se concluye que ϕ es inyectivo. Veamos que ϕ es sobreyectivo: sean $f \in \operatorname{End}_{M_n(D)}(D^n)$ y

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} = f(e_1), \quad A = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix}.$$

Entonces

$$f\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = f(Ae_1) = Af(e_1) = \begin{pmatrix} a_1 d_1 \\ a_2 d_2 \\ \vdots \\ a_n d_1 \end{pmatrix} = \phi(d_1)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

□

lem:simple_izqminimal

Lemma 13.17. *Sea R un anillo simple con un ideal a izquierda L minimal. Entonces todo R-módulo simple es isomorfo a L.*

Proof. Sea M un módulo simple. Como LR es un ideal de R y el anillo R es simple, $LR = R$. Como

$$0 \neq RM = (LR)M = L(RM) \subseteq LM,$$

existe $m \in M$ tal que $Lm \neq 0$. Luego Lm es un submódulo no nulo del simple M y entonces $Lm = M$. El morfismo $\gamma \colon L \to M$, $l \mapsto lm$, es sobreyectivo e inyectiva (pues $\ker\gamma$ es un ideal a izquierda propiamente contenido en L). Luego $L \simeq M$. □

Theorem 13.18. *Si D y E son anillos de división tales que Si $M_n(D) \simeq M_m(E)$ entonces $n = m$ y $D \simeq E$.*

Proof. Como $M_n(D)$ es artiniano a izquierda, existe un ideal a izquierda L minimal. Como $D^n \simeq E^m \simeq L$ como $M_n(D)$-módulos (ver ejemplo 2.11), el lema 13.17 implica que

$$D^{\text{op}} \simeq \operatorname{End}_{M_n(D)}(D^n) \simeq \operatorname{End}_{M_n(D)}(L) \simeq \operatorname{End}_{M_m(E)}(L) \simeq \operatorname{End}_{M_m(E)}(E^m) \simeq E^{\text{op}}.$$

Luego $D \simeq E$ y entonces $n = m$ pues $\dim M_n(D) = \dim M_m(E)$. □

Lecture 9

§14. Kapanskly's problems

Let G be a group and K be a field. If $x \in G$ is such that $x^n = 1$, then, since

$$(1-x)(1+x+x^2+\cdots+x^{n-1}) = 0,$$

it follows that $K[G]$ has non-trivial zero divisors. What happens in the case where G is torsion-free?

example:k[Z] **Example 14.1.** Let $G = \langle x \rangle \simeq \mathbb{Z}$. We claim that $K[G]$ has no zero divisors. Let $\alpha, \beta \in K[G] \setminus \{0\}$ and write $\alpha = \sum_{i \leq n} a_i x^i$ with $a_n \neq 0$ and $\beta = \sum_{j \leq m} b_j x^j$ with $b_m \neq 0$. Since the coefficient of x^{n+m} of $\alpha\beta$ is non-zero, it follows that $\alpha\beta \neq 0$.

A similar problem concerns units of group algebras. A unit $u \in K[G]$ is said to be **trivial** if $u = \lambda g$ for some $\lambda \in K \setminus \{0\}$ and $g \in G$.

Exercise 14.2. Prove that units of $\mathbb{C}[C_2]$ are trivial.

Exercise 14.3. Prove that $\mathbb{C}[C_5]$ has non-trivial units.

We mention some intriguing problems, generally known as Kaplansky's problems.

prob:units **Open problem 14.1 (Units).** Let G be a torsion-free group. Is it true that all units of $K[G]$ are trivial?

A ring R is **reduced** if for all $r \in R$ such that $r^2 = 0$ one has $r = 0$.

prob:reducido **Open problem 14.2 (Are group algebras reduced?).** Let G be a torsion-free group. Is it true that $K[G]$ is reduced?

prob:dominio **Open problem 14.3 (Zero divisors).** Let G be a torsion-free group. Is it true that $K[G]$ is a domain?

We mentioned before the semisimplicity problem.

prob:J

Open problem 14.4 (Semisimplicity). Let G be a torsion-free group. It is true that $J(K[G])=0$ if G is non-trivial?

pro:idempotente

Open problem 14.5 (Idempotents). Let G be a torsion-free group and $\alpha\in K[G]$ be an idempotent. Is it true that $\alpha\in\{0,1\}$?

Exercise 14.4. Prove that if $K[G]$ has no zero-divisors and $\alpha\in K[G]$ is an idempotent, then $\alpha\in\{0,1\}$.

Exercise 14.5. Prove that $K[\mathbb{Z}/4]$ contains non-trivial zero divisors and every idemportent of $K[\mathbb{Z}/4]$ is trivial.

The problems mentinoed are all related. Our goal is the prove the following implications:

$$14.4 \Longleftarrow 14.1 \Longrightarrow 14.2 \Longleftrightarrow 14.3$$

We first prove that an affirmative solution to the Units Problem 14.1 yields a solution to Problem 14.2 about the reducibility of group algebras.

Theorem 14.6. *Let 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 $1-\alpha=\lambda g$. If $g\neq 1$, then

$$0=\alpha^2=(1-\lambda g)^2=1-2\lambda g+\lambda^2g^2,$$

a contradiction. Therefore $g=1$ and hence $\alpha=1-\lambda\in K$. Since K is a field, one concludes that $\alpha=0$. □

We now prove that an affirmative solution to the Units Problem 14.1 also yields a solution to the Jacobson Semisimplicity Problem 14.4.

Theorem 14.7. *Let 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 $1-\alpha=\lambda g$. Assume that $g\neq 1$. 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 $\alpha=0$. □

Exercise 14.8. Prove that if $G=\langle g\rangle\simeq\mathbb{Z}/2$, then $J(\mathbb{F}_2[G])=\{0,g-1\}\neq\{0\}$.

§15. Passman's theorem

Now we prove that an affirmative solution to the Units Problem (Open Problem 14.1) yields a solution to Open Problem 14.3 about zero divisors in group algebras. The proof is hard and requires some preliminaries. We first need to discuss a group theoretical tool known as the *transfer map*.

If H is a subgroup of G, a **transversal** of H in G is a complete set of coset representatives of G/H.

thm:transfer **Theorem 15.1.** *Let G be a group and H be a finite-index subgroup of G. The map*

$$\nu\colon G \to H/[H,H], \quad g \mapsto d(Rg,R),$$

does not depend on the transversal R of H in G and it is a group homomorphism.

To prove the theorem we first need a lemma.

lem:d **Lemma 15.2.** *Let G be a group and H be a subgroup of G of finite index. Let R and S be transversals of H in G and let $\alpha\colon H \to H/[H,H]$ be the canonical map. Then*

$$d(R,S) = \prod \alpha(rs^{-1}),$$

where the product is taken over all pairs $(r,s) \in R \times S$ such that $Hr = Hs$, is well-defined and satisfies the following properties:

1) $d(R,S)^{-1} = d(S,R)$.
2) $d(R,S)d(S,T) = d(R,T)$ *for all transversal T of H in G.*
3) $d(Rg,Sg) = d(R,S)$.
4) $d(Rg,R) = d(Sg,S)$.

Proof. The product that defines $d(R,S)$ is well-defined since $H/[H,H]$ is an abelian group. The first three claim are trivial. Let us prove 4). By 2),

$$d(Rg,Sg)d(Sg,S)d(S,R) = d(Rg,S)d(S,R) = d(Rg,R).$$

Since $H/[H,H]$ is abelian, 1) and 3) imply that

$$d(Rg,Sg)d(Sg,S)d(S,R) = d(R,S)d(S,R)d(Sg,S) = d(Sg,S). \qquad \square$$

We are know ready to prove the theorem:

Proof of Theorem 15.1. The lemma implies that the map does not depend on the transversal used. Moreover, ν is a group homomorphism, as

$$\nu(gh) = d(R(gh),R) = d(R(gh),Rh)d(Rh,R) = d(Rg,R)d(Rh,R) = \nu(g)\nu(h). \ \square$$

The theorem justifies the following definition:

Definition 15.3. Let G be a group and H be a finite-index subgroup of G. The **transfer map** of G in H is the group homomorphism

$$\nu\colon G \to H/[H,H], \quad g \mapsto d(Rg,R),$$

of Theorem 15.1, where R is some transversal of H in G.

Veamos cómo calcular el morfismo de transferencia. Si H es un subgrupo de G de índice n, fijemos un transversal $T = \{x_1,\dots,x_n\}$. Para $g \in G$,

$$\nu(g) = \prod \alpha(xy^{-1}),$$

donde el producto se hace sobre los pares $(x,y) \in (Tg,T)$ tales que $Hx = Hy$ y $\alpha\colon H \to H/[H,H]$ es el morfismo canónico. Si escribimos $x = x_i g$ para algún $i \in \{1,\dots,n\}$, entonces $Hx_i g = Hx_{\sigma(i)}$ para alguna permutación $\sigma \in \mathbb{S}_n$. Luego

$$\nu(g) = \prod_{i=1}^{n} \alpha(x_i g x_{\sigma(i)}^{-1}).$$

lem:transfer

Lemma 15.4. *Sean G un grupo y H un subgrupo de índice finito n y sea T un transversal de H en G. Para cada $g \in G$ existe $k \in$ y existen enteros positivos $n_1,\dots,n_k$ tales que $n_1+\cdots+n_k = n$ y elementos $t_1,\dots,t_k \in T$ tales que*

$$\nu(g) = \prod_{i=1}^{k} \alpha(t_i g^{n_i} t_i^{-1}),$$

donde $\alpha\colon H \to H/[H,H]$ es el morfismo canónico.

Proof. Sabemos que existe una permutación $\sigma \in \mathbb{S}_n$ tal que

$$\nu(g) = \prod_{i=1}^{n} t_i g t_{\sigma(i)}^{-1}.$$

Si escribimos a σ como producto de k ciclos disjuntos $\sigma = \alpha_1 \cdots \alpha_k$, donde cada α_j es un ciclo de longitud n_j, entonces para cada ciclo de la forma $(i_1 \cdots i_{n_j})$ reordenamos el producto de forma tal que

$$\alpha(x_{i_1} g x_{i_2}^{-1})\alpha(x_{i_2} g x_{i_3}^{-1}) \cdots \alpha(x_{i_{n_j}} g x_{i_1}^{-1}) = \alpha(x_{i_1} g^{n_1} x_{i_1}^{-1}).$$

Luego existen $t_1,\dots,t_k \in T$ tales que $\nu(g) = \prod_{j=1}^{k} t_i g^{n_i} t_i^{-1}$. ◻

El morfismo de transferencia nos permite demostrar el siguiente lema:

lem:center

Lemma 15.5. *Si G es un grupo tal que su centro $Z(G)$ tiene índice finito n, entonces $(gh)^n = g^n h^n$ para todo $g,h \in G$.*

Proof. Sea $g \in G$. Por el lema 15.4 sabemos que existen enteros positivos $n_1, \dots, n_k$ tales que $n_1 + \dots + n_k = n$ y elementos $t_1, \dots, t_k$ de un transversal de $Z(G)$ en G tales que

$$\nu(g) = \prod_{i=1}^{k} \alpha(t_i g^{n_1} t_i^{-1}),$$

donde $\alpha \colon G \to H/[H,H]$ es el morfismo canónico. Como $g^{n_i} \in Z(G)$ para todo $i \in \{1, \dots, k\}$ (pues $t_i g^{n_i} t_i^{-1} \in Z(G)$), se sigue que $\nu(g) = g^{n_1 + \dots + n_k} = g^n$. Como ν es un morfismo de grupos por el teorema 15.1, se concluye que

$$(gh)^n = \nu(gh) = \nu(g)\nu(h) = g^n h^n.$$

□

Dado un grupo G consideramos el subconjunto

$$\Delta(G) = \{g \in G : (G : C_G(g)) < \infty\}.$$

Exercise 15.6. Demuestre que $\Delta(\Delta(G)) = \Delta(G)$.

Lemma 15.7. *Si G es un grupo, entonces $\Delta(G)$ es un subgrupo característico de G.*

Proof. Primero veamos que $\Delta(G)$ es un subgrupo de G. Si $x, y \in \Delta(G)$ y $g \in G$, entonces $g(xy^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})^{-1}$. Además $1 \in \Delta(G)$. Veamos ahora que $\Delta(G)$ es característico en G. Si $f \in \mathrm{Aut}(G)$ y $x \in G$, entonces, como $f(gxg^{-1}) = f(g)f(x)f(g)^{-1}$, se concluye que $f(x) \in \Delta(G)$. □

Exercise 15.8. Demuestre que si $G = \langle r, s : s^2 = 1, srs = r^{-1} \rangle$ es el grupo diedral infinito, entonces $\Delta(G) = \langle r \rangle$.

Exercise 15.9. Sean H y K subgrupos de G de índice finito. Demuestre que

$$(G : H \cap K) \leq (G : H)(G : K).$$

lem:FCabeliano

Lemma 15.10. *Si G es un grupo sin torsión tal que $\Delta(G) = G$, entonces G es abeliano.*

Proof. Sean $x, y \in G$ y sea $S = \langle x, y \rangle$. El grupo $Z(S) = C_S(x) \cap C_S(y)$ tiene índice finito, digamos n, en S. Como por el lema 15.5 la función $S \to Z(S)$, $s \mapsto s^n$, es un morfismo de grupos, se tiene que

$$[x, y]^n = (xyx^{-1}y^{-1})^n = x^n y^n x^{-n} y^{-n} = 1$$

pues $x^n \in Z(S)$. Como G es libre de torsión, $[x, y] = 1$. □

lem:Neumann

Lemma 15.11 (Neumann). *Sean $H_1, \dots, H_m$ subgrupos de G. Supongamos que existen finitos elementos $a_{ij} \in G$, $1 \leq i \leq m$, $1 \leq j \leq n$, tales que*

$$G = \bigcup_{i=1}^{m}\bigcup_{j=1}^{n} H_i a_{ij}.$$

Entonces algún H_i tiene índice finito en G.

Proof. Procederemos por inducción en m. El caso $m = 1$ es trivial. Supongamos entonces que $m \geq 2$. Si $(G : H_1) = \infty$, existe $b \in G$ tal que

$$Hb \cap \left(\bigcup_{j=1}^{n} H_1 a_{1j}\right) = \emptyset.$$

Como entonces $H_1 b \subseteq \bigcup_{i=2}^{m}\bigcup_{j=1}^{n} H_i a_{ij}$, se concluye que

$$H_1 a_{1k} \subseteq \bigcup_{i=2}^{m}\bigcup_{j=1}^{n} H a_{ij} b^{-1} a_{1k}.$$

Luego G puede cubrirse con finitas coclases de $H_2, \dots, H_m$ y por hipótesis inductiva alguno de estos H_j tiene índice finito en G. □

Veremos ahora un operador de proyección del álgebra de grupo. Si G es un grupo y H es un subgrupo de G, se define

$$\pi_H : K[G] \to K[H], \quad \pi_H\left(\sum_{g\in G} \lambda_g g\right) = \sum_{g\in H} \lambda_g g.$$

Exercise 15.12. Sea G un grupo y sea H un subgrupo de G. Demuestre que si $\alpha \in K[G]$, entonces π_H es un morfismo de $(K[H], K[H])$-bimódulos con las multiplicaciones a izquierda y a derecha, es decir:

$$\pi_H(\beta\alpha\gamma) = \beta\pi_H(\alpha)\gamma$$

para todo $\beta, \gamma \in K[H]$.

lem:escritura

Lemma 15.13. *Sea X un transversal a izquierda de H en G. Todo $\alpha \in K[G]$ se escribe unívocamente como*

$$\alpha = \sum_{x\in X} x\alpha_x,$$

donde $\alpha_x = \pi_H(x^{-1}\alpha) \in K[H]$.

Proof. Sea $\alpha \in K[G]$. Como $\operatorname{supp}\alpha$ es finito, $\operatorname{supp}\alpha$ está contenido en finitas coclases de H, digamos $x_1H, \dots, x_nH$, donde los x_j son elementos de X. Escribimos $\alpha = \alpha_1 + \dots + \alpha_n$, donde $\alpha_i = \sum_{g\in x_i H} \lambda_g g$. Si $g \in x_i H$, entonces $x_i^{-1} g \in H$ y luego podemos escribir

$$\alpha = \sum_{i=1}^{n} x_i (x_i^{-1}\alpha_i) = \sum_{x\in X} x\alpha_x$$

con $\alpha_x \in K[H]$ para todo $x \in X$. Para la unicidad observemos que para cada $x \in X$ gracias al ejercicio anterior se tiene

$$\pi_H(x^{-1}\alpha) = \pi_H\left(\sum_{y\in X} x^{-1}y\alpha_y\right) = \sum_{y\in X} \pi_H(x^{-1}y)\alpha_y = \alpha_x$$

pues

$$\pi_H(x^{-1}y) = \begin{cases} 1 & \text{si } x = y, \\ 0 & \text{si } x \neq y. \end{cases}$$

□

lem:ideal_pi

Lemma 15.14. *Sea G un grupo y H un subgrupo de G. Si I es un ideal a izquierda no nulo de $K[G]$, entonces $\pi_H(I) \neq 0$.*

Proof. Sea X un transversal a izquierda de H en G y sea $\alpha \in I \setminus \{0\}$. Por el lema 15.13 podemos escribir $\alpha = \sum_{x\in X} x\alpha_x$ con $\alpha_x = \pi_H(x^{-1}\alpha) \in K[H]$ para todo $x \in X$. Como $\alpha \neq 0$, existe $y \in X$ tal que $0 \neq \alpha_y = \pi_H(y^{-1}\alpha) \in \pi_H(I)$ ($y^{-1}\alpha \in I$ pues I es un ideal a izquierda). □

Antes de avanzar, veamos una aplicación del operador de proyección:

Proposition 15.15. *Sean G un grupo, H un subgrupo de G y $\alpha \in K[H]$. Valen las siguientes afirmaciones:*

1) *α es inversible en $K[H]$ si y sólo si α es inversible en $K[G]$.*
2) *α es un divisor de cero en $K[H]$ si y sólo si α es un divisor de cero en $K[G]$.*

Proof. Si α es inversible en $K[G]$, existe $\beta \in K[G]$ tal que $\alpha\beta = \beta\alpha = 1$. Al aplicar π_H y usar que π_H es un morfismo de $(K[H], K[H])$-bimódulos,

$$\alpha\pi_H(\beta) = \pi_H(\alpha\beta) = \pi_H(1) = 1 = \pi_H(1) = \pi_H(\beta\alpha) = \pi_H(\beta)\alpha.$$

Si $\alpha\beta = 0$ para algún $\beta \in K[G] \setminus \{0\}$, sea $g \in G$ tal que $1 \in \operatorname{supp}(\beta g)$. Como $\alpha(\beta g) = 0$,

$$0 = \pi_H(0) = \pi_H(\alpha(\beta g)) = \alpha\pi_H(\beta g),$$

donde $\pi_H(\beta g) \in K[H] \setminus \{0\}$ pues $1 \in \operatorname{supp}(\beta g)$. □

lem:Passman

Lemma 15.16 (Passman). *Sea G un grupo y sean $\gamma_1, \gamma_2 \in K[G]$ con $\gamma_1 K[G]\gamma_2 = 0$. Entonces $\pi_{\Delta(G)}(\gamma_1)\pi_{\Delta(G)}(\gamma_2) = 0$.*

Proof. Basta ver que $\pi_{\Delta(G)}(\gamma_1)\gamma_2 = 0$ pues en este caso

$$0 = \pi_{\Delta(G)}(\pi_{\Delta(G)}(\gamma_1)\gamma_2) = \pi_\Delta(\gamma_1)\pi_{\Delta(G)}(\gamma_2).$$

Escribimos $\gamma_1 = \alpha_1 + \beta_1$, donde

$$\begin{aligned} \alpha_1 &= a_1u_1+\cdots+a_ru_r, && u_1,\dots,u_r\in\Delta(G),\\ \beta_1 &= b_1v_1+\cdots+b_sv_s, && v_1,\dots,v_s\notin\Delta(G),\\ \gamma_2 &= c_1w_1+\cdots+c_tw_t, && w_1,\dots,w_t\in G. \end{aligned}$$

El subgrupo $C=\bigcap_{i=1}^r C_G(u_i)$ tiene índice finito en G. Supongamos que

$$0\neq\pi_\Delta(\gamma_1)\gamma_2=\alpha_1\gamma_2$$

y sea $g\in\operatorname{supp}(\alpha_1\gamma_2)$. Si v_i es conjugado de algún gw_j^{-1} en G, sea $g_{ij}\in G$ tal que $g_{ij}^{-1}v_ig_{ij}=gw_j^{-1}$. Si v_i y gw_j^{-1} no son conjugados tomamos $g_{ij}=1$.

Para cada $x\in C$ se tiene $\alpha_1\gamma_2=(x^{-1}\alpha_1x)\gamma_2$. Como además

$$x^{-1}\gamma_1x\gamma_2\in x^{-1}\gamma_1K[G]\gamma_2=0,$$

tenemos

$$\begin{aligned}(a_1u_1+\cdots+a_ru_r)\gamma_2=\alpha_1\gamma_2=x^{-1}\alpha_1x\gamma_2&=-x^{-1}\beta_1x\gamma_2\\ &=-x^{-1}(b_1v_1+\cdots+b_sv_r)x(c_1w_1+\cdots+c_tw_t).\end{aligned}$$

Como $g\in\operatorname{supp}(\alpha_1\gamma_2)$, existen i,j tales que $g=x^{-1}v_ixw_j$. Luego v_i y gw_j^{-1} son conjugados y entonces $x^{-1}v_ix=gw_j^{-1}=g_{ij}^{-1}v_ig_{ij}$, es decir $x\in C_G(v_i)g_{ij}$. Esto demuestra que

$$C\subseteq\bigcup_{i,j}C_G(v_i)g_{ij}$$

y como C tiene índice finito en G, esto implica que G puede cubrirse con finitas coclases de los $C_G(v_i)$. Pero como $v_i\notin\Delta(G)$, cada uno de los $C_G(v_i)$ tiene índice infinito en G, una contradicción al lema de Neumann. □

Theorem 15.17. *Sea G un grupo sin torsión. Si $K[G]$ es reducido, entonces $K[G]$ es un dominio.*

Proof. Supongamos que $K[G]$ no es un dominio y sean $\gamma_1,\gamma_2\in K[G]\setminus\{0\}$ tales que $\gamma_2\gamma_1=0$. Si $\alpha\in K[G]$, entonces

$$(\gamma_1\alpha\gamma_2)^2=\gamma_1\alpha\gamma_2\gamma_1\alpha\gamma_2=0$$

y luego $\gamma_1\alpha\gamma_2=0$ pues $K[G]$ es reducido. En particular, $\gamma_1K[G]\gamma_2=0$. Sea I el ideal a izquierda de $K[G]$ generado por γ_2. Como $I\neq0$, $\pi_{\Delta(G)}(I)\neq0$ por el lema 15.14 y luego $\pi_{\Delta(G)}(\beta\gamma_2)\neq0$ para algún $\beta\in K[G]$. Similarmente se demuestra que $\pi_{\Delta(G)}(\gamma_1\alpha)\neq0$ para algún $\alpha\in K[G]$. Como

$$\gamma_1\alpha K[G]\beta\gamma_2\subseteq\gamma_1K[G]\gamma_2=0,$$

se tiene que $\pi_{\Delta(G)}(\gamma_1\alpha)\pi_{\Delta(G)}(\beta\gamma_2)=0$ por el lema de Passman. Luego $K[\Delta(G)]$ tiene divisores de cero, una contradicción pues $\Delta(G)$ es un grupo abeliano. □

§16. Grupos (bi)ordenables

En esta sección estudiaremos algunas propiedades del grupo G motivadas por el análisis que se hizo en el ejemplo 14.1.

Definition 16.1. Un grupo G se dice **biordenable** si existe un orden total $<$ en G tal que $x < y$ implica que $xz < yz$ y $zx < zy$ para todo $x, y, z \in G$.

Example 16.2. El grupo $\mathbb{R}_{>0}$ de números reales positivos es biordenable.

Exercise 16.3. Sea G un grupo biordenable y sean $x, x', y, y' \in G$. Demuestre que si $x < y$ y $x' < y'$, entonces $xx' < yy'$.

Exercise 16.4. Sea G un grupo biordenable y sean $g, h \in G$. Demuestre que si $g^n = h^n$ para algún $n > 0$ entonces $g = h$.

Definition 16.5. Sea G un grupo biordenable. El cono positivo es el conjunto $P(G) = \{x \in G : 1 < x\}$.

lemma:biordenableP1 **Lemma 16.6.** *Sea G un grupo biordenable con cono positivo P. Entonces*

1) *P es cerrado para la multiplicación.*
2) *$G = P \cup P^{-1} \cup \{1\}$ (unión disjunta).*
3) *$xPx^{-1} = P$ para todo $x \in G$.*

Proof. Si $x, y \in P$ y $z \in G$, entonces, como $1 < x$ y además $1 < y$, se tiene que $1 < xy$. Luego $1 = z1z^{-1} < zxz^{-1}$. Queda demostrar entonces la segunda afirmación: Si $g \in G$, entonces $g = 1$ o $g > 1$ o $g < 1$. Como $g < 1$ y si sólo si $1 < g^{-1}$. □

lem:biordenableP2 **Lemma 16.7.** *Sea G un grupo y sea P un subconjunto de G cerrado para la multiplicación y tal que $G = P \cup P^{-1} \cup \{1\}$ (unión disjunta) y $xPx^{-1} = P$ para todo $x \in G$. Si definimos $x < y$ si y sólo si $yx^{-1} \in P$, entonces G resulta biordenable con cono positivo P.*

Proof. Sean $x, y \in G$. Como $yx^{-1} \in G$ y sabemos que $G = P \cup P^{-1} \cup \{1\}$ (unión disjunta), se tiene exactamente alguna de las siguientes tres posibilidades: $yx^{-1} \in P$, $xy^{-1} = (yx^{-1})^{-1} \in P$ o bien $yx^{-1} = 1$. Luego $x < y$, $y < x$ o bien $x = y$. Si $x < y$ y $z \in G$, entonces $zx < zy$ pues $(zy)(zx)^{-1} = z(yx^{-1})z^{-1} \in P$ ya que $zPz^{-1} = P$. Además $xz < yz$ pues $(yz)(xz)^{-1} = yx^{-1} \in P$. Para demostrar que que P es el cono positivo de este biorden en G basta observar que $x1^{-1} = x \in P$ si y sólo si $1 < x$. □

pro:BOsintorsion **Proposition 16.8.** *Todo grupo biordenable es libre de torsión.*

Proof. Sea G un grupo biordenable y sea $g \in G \setminus \{1\}$. Si $g > 1$, entonces $1 < g < g^2 < \cdots$. Si $g < 1$, entonces $1 > g > g^2 > \cdots$. Luego $g^n \neq 1$ para todo $n \neq 0$. □

Example 16.9. El grupo $G = \langle x, y : yxy^{-1} = x^{-1} \rangle$ no es biordenable y es libre de torsión. Supongamos que G es biordenable y sea P su cono positivo. Si $x \in P$ entonces $yxy^{-1} = x^{-1} \in P$, una contradicción. Entonces $x^{-1} \in P$ y luego $x = y^{-1}x^{-1}y \in P$, una contradicción.

thm:BO **Theorem 16.10.** *Sea G un grupo biordenable. Entonces $K[G]$ es un dominio tal que solamente tiene unidades triviales. Más aún, si G es no trivial, $J(K[G]) = 0$.*

Proof. Sean $\alpha, \beta \in K[G]$ tales que

$$\alpha = \sum_{i=1}^{m} a_i g_i, \qquad g_1 < g_2 < \cdots < g_m, \qquad a_i \neq 0 \qquad \forall i \in \{1, \dots, m\},$$
$$\beta = \sum_{j=1}^{n} b_j h_j, \qquad h_1 < h_2 < \cdots < h_n, \qquad b_j \neq 0 \qquad \forall j \in \{1, \dots, n\}.$$

Entonces

$$g_1 h_1 \leq g_i h_j \leq g_m h_n$$

para todo i, j. Además $g_1 h_1 = g_i h_j$ si y sólo si $i = j = 1$. El coeficiente de $g_1 h_1$ en $\alpha\beta$ es $a_1 b_1 \neq 0$ y en particular $\alpha\beta \neq 0$. Si $\alpha\beta = \beta\alpha = 1$, entonces el coefciente de $g_m h_n$ en $\alpha\beta$ es $a_m b_n$ y luego $m = n = 1$ y por lo tanto $\alpha = a_1 g_1$ y $\beta = b_1 h_1$ con $a_1 b_1 = b_1 a_1 = 1$ en K y $g_1 h_1 = 1$ en G. □

thm:Levi **Theorem 16.11 (Levi).** *Sea A un grupo abeliano. Entonces A es biordenable si y sólo si A es libre de torsión.*

Proof. Si A es biordenable, entonces A no tiene torsión por la proposición 16.8. Supongamos entonces que A es un grupo abeliano sin torsión y veamos que es biordenable. Sea $\mathcal{S}$ la clase de subconjuntos P de A tales que $0 \in P$, P es cerrado para la suma de A y cumplen con la siguiente propiedad: si $x \in P$ y $-x \in P$, entonces $x = 0$. Claramente $\mathcal{S}$ es no vacía pues $\{0\} \in \mathcal{S}$. Si ordenamos parcialmente a $\mathcal{S}$ con la inclusión, vemos que el elemento $\bigcup_{i \in I} P_i$ es una cota superior para la cadena $P_1 \subseteq P_2 \subseteq \cdots$ de $\mathcal{S}$. Por el lema de Zorn, $\mathcal{S}$ tiene un elemento maximal $P \in \mathcal{S}$.

Claim. Si $x \in A$ es tal que $kx \in P$ para algún $k > 0$, entonces $x \in P$.

Para demostrar la afirmación sea $Q = \{x \in A : kx \in P \text{ para algún } k > 0\}$. Veamos que $Q \in \mathcal{S}$. Trivialmente $0 \in Q$. Además Q es cerrado por la adición: si $k_1 x_1 \in P$ y $k_2 x_2 \in P$ entonces $k_1 k_2 (x_1 + x_2) \in P$. Sea $x \in A$ tal que $x \in Q$ y $-x \in Q$. Entonces $kx \in P$ y $l(-x) \in P$ para algún $l > 0$. Como entonces $klx \in P$ y $kl(-x) \in P$, se concluye que $klx = 0$, una contradicción pues A no tiene torsión. Luego $x \in Q \subseteq P$.

Claim. Si $x \in A$ es tal que $x \notin P$ entonces $-x \in P$.

Supongamos que $-x \notin P$ y sea $P_1 = \{y + nx : y \in P, n \geq 0\}$. Vamos a ver que $P_1 \in \mathcal{S}$. Claramente $0 \in P_1$ y P_1 es cerrado para la suma. Si $P_1 \notin S$ existe

$$0 \neq y_1 + n_1 x = -(y_2 + n_2 x),$$

donde $y_1, y_2 \in P$ y $n_1, n_2 \geq 0$. Entonces $y_1 + y_2 = -(n_1 + n_2)x$. Si $n_1 = n_2 = 0$, entonces $y_1 = -y_2 \in P$ y luego $y_1 = y_2 = 0$ y se concluye que $y_1 + n_1 x = 0$, una contradicción. Si $n_1 + n_2 > 0$, entonces, como

$$(n_1+n_2)(-x) = y_1+y_2 \in P,$$

la primera afirmación que hicimos implica que $-x \in P$, una contradicción. Demostramos entonces que $P_1 \in \mathcal{S}$. Como $P \subseteq P_1$, la maximalidad de P implica que $x \in P = P_1$.

Gracias al lema 16.7 sabemos que el conjunto $P^* = P \setminus \{0\}$ que construimos es en realidad el cono positivo de un biorden en A. En efecto, P^* es cerrado para la suma pues si $x, y \in P^*$, entonces $x+y \in P$ y si $x+y=0$ entonces, como $x=-y \in P$, se concluye que $x=y=0$. Además $G = P^* \cup -P^* \cup \{0\}$ (unión disjunta) pues demostramos en la segunda afirmación que si $x \notin P^*$ entonces $-x \in P$. □

Corollary 16.12. *Sea A un grupo abeliano no trivial y sin torsión. Entonces $K[A]$ es un dominio tal que solamente tiene unidades triviales y $J(K[A]) = 0$.*

Proof. Es consecuencia del teorema de Levi y del teorema 16.10. □

Definition 16.13. Un grupo G se dice **ordenable a derecha** si existe un orden total $<$ en G tal que si $x<y$ entonces $xz<yz$ para todo $x,y,z \in G$.

Si G es un grupo ordenable a derecha, se define el cono positivo de G como el subconjunto $P(G) = \{x \in G : 1 < x\}$.

Exercise 16.14. Sea G un grupo ordenable a derecha con cono positivo P. Demuestre las siguientes afirmaciones:

1) P es cerrado por multiplicación.
2) $G = P \cup P^{-1} \cup \{1\}$ (unión disjunta).

Exercise 16.15. Sea G un grupo y sea P un subconjunto cerrado por multiplicación y tal que $G = P \cup P^{-1} \cup \{1\}$ (unión disjunta). Demuestre que si se define $x<y$ si y sólo si $yx^{-1} \in P$, entonces G es ordenable a derecha con cono positivo P.

Lemma 16.16. *Sea G un grupo y sea N un subgrupo normal de G. Si N y G/N son ordenables a derecha, entonces G también lo es.*

Proof. Como N y G/N son ordenables a derecha, existen los conos positivos $P(N)$ y $P(G/N)$. Sea $\pi\colon G \to G/N$ el morfismo canónico y sea

$$P(G) = \{x \in G : \pi(x) \in P(G/N) \text{ o bien } x \in N\}.$$

Dejamos como ejercicio demostrar que $P(G)$ es cerrado por la multiplicación y que $G = P(G) \cup P(G)^{-1} \cup \{1\}$ (unión disjunta). Luego G es ordenable a derecha. □

Para dar un criterio de ordenabilidad necesitamos un lema:

lemma:fg **Lemma 16.17.** *Sea G un grupo finitamente generado y sea H un subgrupo de índice finito. Entonces H es finitamente generado.*

Proof. Supongamos que G está generado por $\{g_1,\dots,g_m\}$ y supongamos que para cada i existe k tal que $g_i^{-1}=g_k$. Sea $t_1,\dots,t_n$ un conjunto de representantes de G/H. Para $i\in\{1,\dots,n\}$, $j\in\{1,\dots,m\}$, escribimos

$$t_i g_j = h(i,j)t_{k(i,j)}.$$

Vamos a demostrar que H está generado por los $h(i,j)$. Sea $x\in H$. Escribamos

$$\begin{aligned} x &= g_{i_1}\cdots g_{i_s}\\ &= (t_1 g_{i_1})g_{i_2}\cdots g_{i_s}\\ &= h(1,i_1)t_{k_1}g_{i_2}\cdots g_{i_s}\\ &= h(1,i_1)h(k_1,i_2)t_{k_2}g_{i_3}\cdots g_{i_s}\\ &= h(1,i_1)h(k_1,i_2)\cdots h(k_{s-1},g_{i_s})t_{k_s}, \end{aligned}$$

donde $k_1,\dots,k_{s-1}\in\{1,\dots,n\}$. Como $t_{k_s}\in H$, $t_{k_s}=t_1\in H$ y luego $x\in H$. $\square$

El siguiente teorema nos da un criterio de ordenabilidad a derecha:

Theorem 16.18. *Sea G un grupo libre de torsión y finitamente generado. Si A es un subgrupo normal abeliano tal que G/A es finito y cíclico, entonces G es ordenable a derecha.*

Proof. Primero observemos que si A es trivial, entonces G también es trivial. Supongamos entonces que $A\neq 1$. Como A tiene índice finito, es finitamente generado. Procederemos por inducción en la cantidad de generadores de A. Como G/A es cíclico, existe $x\in G$ tal que $G=\langle A,x\rangle$. Luego $[x,A]=\langle [x,a]:a\in A\rangle$ es un subgrupo normal de G tal que $A/C_A(x)\simeq [x,A]$ (pues $a\mapsto [x,a]$ es un morfismo de grupos $A\to A$ con imagen $[x,A]$ y núcleo $C_A(x)$). Si $\pi\colon G\to G/[x,A]$, entonces $G/[x,A]=\langle \pi(A),\pi(x)\rangle$ y luego $G/[x,A]$ es abeliano pues $[\pi(x),\pi(A)]=\pi[x,A]=1$. Además $G/[x,A]$ es finitamente generado pues G es finitamente generado. Como $(G:A)=n$ y G no tiene torsión, $1\neq x^n\in A$. Luego $x^n\in C_A(x)$ y entonces $1\leq \operatorname{rank} C_A(x)<\operatorname{rank} A$ (si $\operatorname{rank} C_A(x)=\operatorname{rank} A$, entonces $[x,A]$ sería un subgrupo de torsión de A, una contradicción pues $x\notin A$). Luego

$$\operatorname{rank}[x,A]=\operatorname{rank}(A/C_A(x))\leq \operatorname{rank} A-1$$

y entonces $\operatorname{rank}(A/[x,A])\geq 1$. Demostramos así que $A/[x,A]$ es infinito y luego $G/[x,A]$ es también infinito.

Como $G/[x,A]$ es un grupo abeliano finitamente generado e infinito, existe un un subgrupo normal H de G tal que $[x,A]\subseteq H$ y $G/H\simeq\mathbb{Z}$. El subgrupo $B=A\cap H$ es abeliano, normal en H y cumple que H/B es cíclico (pues puede identificarse con un subgrupo de G/A). Como $\operatorname{rank} B<\operatorname{rank} A$, la hipótesis inductiva implica que H es ordenable a derecha y luego G también es ordenable a derecha. $\square$

Exercise 16.19 (Malcev–Neumann). Sea G un grupo ordenable a derecha. Demuestre que $K[G]$ no tiene divisores de cero ni unidades no triviales.

En 1973 Formanek demostró que la conjetura de los divisores de cero es verdadera para grupos super resolubles sin torsión. En 1976 Brown e independientemente Farkas y Snider demostraron que la conjetura es verdadera para grupos policíclicos-por-finitos sin torsión.

§17. Grupos con la propiedad del producto único

Sea G un grupo y sean $A, B \subseteq G$ subconjuntos no vacíos. Diremos que un elemento $g \in G$ es un producto único en AB si $g = ab = a_1 b_1$ con $a, a_1 \in A$ y $b, b_1 \in B$ implica que $a = a_1$ y $b = b_1$.

Definition 17.1. Se dice que un grupo G tiene la **propiedad del producto único** si dados dos subconjuntos $A, B \subseteq G$ finitos y no vacíos existe al menos un producto único en AB.

Proposition 17.2. *Si un grupo G es ordenable a derecha, entonces G tiene la propiedad del producto único.*

Proof. Sean $A = \{a_1, \dots, a_n\} \subseteq G$ y $B \subseteq G$ ambos finitos y no vacíos. Supongamos que $a_1 < a_2 < \cdots < a_n$. Sea $c \in B$ tal que $a_1 c$ es el mínimo del conjunto $a_1 B = \{a_1 b : b \in B\}$. Veamos que $a_1 c$ admite una única representación de la forma $\alpha\beta$ con $\alpha \in A$ y $\beta \in B$. Si $a_1 c = ab$, entonces, como $ab = a_1 c \leq a_1 b$, se tiene que $a \leq a_1$ y luego $a = a_1$ y $b = c$. □

Exercise 17.3. Demuestre que un grupo que satisface la propiedad del producto único es libre de torsión.

Definition 17.4. Se dice que un grupo G tiene la **propiedad del doble producto único** si dados dos subconjuntos $A, B \subseteq G$ finitos y no vacíos tales que $|A| + |B| > 2$ existen al menos dos productos únicos en AB.

theorem:Strojnowski

Theorem 17.5 (Strojnowski). *Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

1) *G tiene la propiedad del doble producto único.*
2) *Para todo subconjunto $A \subseteq G$ finito y no vacío, existe al menos un producto único en $AA = \{a_1 a_2 : a_1, a_2 \in A\}$.*
3) *G tiene la propiedad del producto único.*

Proof. La implicación (1) $\implies$ (2) es trivial. Demostremos que vale (2) $\implies$ (3). Si G no tiene la propiedad del producto único, existen subconjuntos $A, B \subseteq G$ finitos y no vacíos tales que todo elemento de AB admite al menos dos representaciones. Sea $C = AB$. Todo $c \in C$ es de la forma $c = (a_1 b_1)(a_2 b_2)$ con $a_1, a_2 \in A$ y $b_1, b_2 \in B$. Como $a_2^{-1} b_1^{-1} \in AB$, existen $a_3 \in A \setminus \{a_2\}$ y $b_3 \in B \setminus \{b_1\}$ tales que $a_2^{-1} b_1^{-1} = a_3^{-1} b_3^{-1}$. Luego $b_1 a_2 = b_3 a_3$ y entonces

$$c = (a_1 b_1)(a_2 b_2) = (a_1 b_3)(a_3 b_2)$$

son dos representaciones distintas de c en AB. pues $a_2 \neq a_3$ y $b_1 \neq b_3$.

Demostremos ahora que (3) $\Longrightarrow$ (1). Si G tiene la propiedad del producto único pero no tiene la propiedad del doble producto único, existen subconjuntos $A, B \subseteq G$ finitos y no vacíos con $|A| + |B| > 2$ tales que en AB existe un único elemento ab con una única representación en AB. Sean $C = a^{-1}A$ y $D = Bb^{-1}$. Entonces $1 \in C \cap D$ y el elemento neutro 1 admite una única representación en CD (pues si $1 = cd$ con $c = a^{-1}a_1 \neq 1$ y $d = b_1 b^{-1} \neq 1$, entonces $ab = a_1 b_1$ con $a \neq a_1$ y $b \neq b_1$). Sean $E = D^{-1}C$ y $F = DC^{-1}$. Todo elemento de EF se escribe como $(d_1^{-1}c_1)(d_2 c_2^{-1})$. Si $c_1 \neq 1$ o $d_2 \neq 1$ entonces $c_1 d_2 = c_3 d_3$ para algún $c_3 \in C \setminus \{c_1\}$ y algún $d_3 \in D \setminus \{d_2\}$. Entonces $(d_1^{-1}c_1)(d_2 c_2^{-1}) = (d_1^{-1}c_3)(d_3 c_2^{-1})$ son dos representaciones distintas para $(d_1^{-1}c_1)(d_2 c_2^{-1})$. Si $c_2 \neq 1$ o $d_1 \neq 1$ entonces $c_2 d_1 = c_4 d_4$ para algún $d_4 \in D \setminus \{d_1\}$ y algún $c_4 \in C \setminus \{c_2\}$ y entonces, como $d_1^{-1}c_2^{-1} = d_4^{-1}c_4^{-1}$, $(d_1^{-1}1)(1c_2^{-1}) = (d_4^{-1}1)(1c_4^{-1})$. Como $|C| + |D| > 2$, C o D contienen algún $c \neq 1$, y entonces $(1 \cdot 1)(1 \cdot 1) = (1 \cdot c)(1 \cdot c^{-1})$. Demostramos entonces que todo elemento de EF tiene al menos dos representaciones. $\square$

Exercise 17.6. Demuestre que si G es un grupo que satisface la propiedad del producto único, entonces $K[G]$ tiene solamente unidades triviales.

En general es muy difícil verificar si un grupo posee la propiedad del producto único. Una propiedad similar es la de ser un grupo difuso. Si G es un grupo libre de torsión y $A \subseteq G$ es un subconjunto, diremos que A es antisimétrico si $A \cap A^{-1} \subseteq \{1\}$, donde $A^{-1} = \{a^{-1} : a \in A\}$. El conjunto de **elementos extremales** de A se define como $\Delta(A) = \{a \in A : Aa^{-1} \text{ es antisimétrico}\}$. Luego

$$a \in A \setminus \Delta(A) \Longleftrightarrow \text{existe } g \in G \setminus \{1\} \text{ tal que } ga \in A \text{ y } g^{-1}a \in A.$$

Definition 17.7. Un grupo G se dice **difuso** si para todo subconjunto $A \subseteq G$ tal que $2 \leq |A| < \infty$ se tiene $|\Delta(A)| \geq 2$.

Lemma 17.8. *Si G es ordenable a derecha, entonces G es difuso.*

Proof. Supongamos que $A = \{a_1, \dots, a_n\}$ y $a_1 < a_2 < \dots < a_n$. Vamos a demostrar que $\{a_1, a_n\} \subseteq \Delta(A)$. Si $a_1 \in A \setminus \Delta(A)$, existe $g \in G \setminus \{1\}$ tal que $ga_1 \in A$ y $g^{-1}a_1 \in A$. Esto implica que $a_1 \leq ga_1$ y $a_1 \leq g^{-1}a_1$, de donde se concluye que $1 \leq g$ y $1 \leq g^{-1}$, una contradicción. De la misma forma se demuestra que $a_n \in \Delta(A)$. $\square$

lemma:difuso=>2up

Lemma 17.9. *Si G es difuso, entonces G tiene la propiedad del doble producto único.*

Proof. Supongamos que G no tiene la propiedad del doble producto único. Existen entonces subconjuntos finitos $A, B \subseteq G$ con $|A| + |B| > 2$ tales que $C = AB$ tiene a lo sumo un producto único. Luego $|C| \geq 2$. Como G es difuso, $|\Delta(C)| \geq 2$. Si $c \in \Delta(C)$, entonces c tiene una única expresión como $c = ab$ con $a \in A$ y $b \in B$ (de lo contrario, si $c = a_0 b_0 = a_1 b_1$ con $a_0 \neq a_1$ y $b_0 \neq b_1$. Si $g = a_0 a_1^{-1}$, entonces

$g \neq 1$, $gc = a_0a_1^{-1}a_1b_1 = a_0b_1 \in C$ y además $g^{-1}c = a_1a_0^{-1}a_0b_0 = a_1b_0 \in C$. Luego $c \notin \Delta(c)$, una contradicción. □

Open problem 17.1. ¿Existe un grupo que tenga la propiedad del producto único y no sea difuso?

§18. Connel's theorem

When $K[G]$ is prime? Connel's theorem gives a full answer to this natural question in the case where K is of characteristic zero.

If S is a finite subset of a group G, then we define $\widehat{S} = \sum_{x\in S} x$.

lemma:sumN **Lemma 18.1.** *Let N be a finite normal subgroup of G. Then $\widehat{N} = \sum_{x\in N} x$ is central in $K[G]$ and $\widehat{N}(\widehat{N} - |N|1) = 0$.*

Proof. Assume that $N = \{n_1, \dots, n_k\}$. Let $g \in G$. Since $N \to N$, $n \mapsto gng^{-1}$, is bijective,

$$g\widehat{N}g^{-1} = g(n_1 + \cdots + n_k)g^{-1} = gn_1g^{-1} + \cdots + gn_kg^{-1} = \widehat{N}.$$

Since $nN = N$ if $n \in N$, it follows that $n\widehat{N} = \widehat{N}$. Thus $\widehat{N}\widehat{N} = \sum_{j=1}^{k} n_j\widehat{N} = |N|\widehat{N}$. □

Before proving Connel's theorem we need to prove two group theoretical results. The first one goes to Dietzman:

theorem:Dietzmann **Theorem 18.2 (Dietzmann).** *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.*

Proof. Let $S = \langle X\rangle$. Since $x^{-1} = x^{n-1}$, every element of S can be written as a finite product of elements of X. Fix $x \in X$. We claim that if $x \in X$ appears $k \geq 1$ times in the word s, then we can write s as a product of m elements of X, where the first k elements are equal to x. Suppose that

$$s = x_1x_2\cdots x_{t-1}xx_{t+1}\cdots x_m,$$

where $x_j \neq x$ for all $j \in \{1, \dots, t-1\}$. Then

$$s = x(x^{-1}x_1x)(x^{-1}x_2x)\cdots(x^{-1}x_{t-1}x)x_{t+1}\cdots x_m$$

is a product of m elements of X since X is closed under conjugation and the first element is x. The same argument implies that s can be written as

$$s = x^k y_{k+1}\cdots y_m,$$

where each y_j belongs to $X \setminus \{x\}$.

Let $s \in S$ and write s as a product of m elements of X, where m is minimal. We need to show that $m \leq (n-1)|X|$. If $m > (n-1)|X|$, then at least $x \in X$ appear n times in the representation of s. Without loss of generality, we write

$$s = x^n x_{n+1} \cdots x_m = x_{n+1} \cdots x_m,$$

a contradiction to the minimality of m. □

The second result goes back to Schur:

thm:Schur **Theorem 18.3 (Schur).** *Let G be a group. If $Z(G)$ has finite index in G, then $[G,G]$ is finite.*

Proof. Let $n = (G : Z(G))$ and X be the set of commutators of G. We claim that X is finite, in fact $|X| \leq n^2$. The map

$$\varphi\colon X \to G/Z(G) \times G/Z(G), \quad [x,y] \mapsto (xZ(G), yZ(G)),$$

is injective: if $(xZ(G), yZ(G)) = (uZ(G), vZ(G))$, then $u^{-1}x \in Z(G)$, $v^{-1}y \in Z(G)$. Thus

$$[u,v] = uvu^{-1}v^{-1} = uv(u^{-1}x)x^{-1}v^{-1} = xvx^{-1}(v^{-1}y)y^{-1} = xyx^{-1}y^{-1} = [x,y].$$

Moreover, X is closed under conjugation, as

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

for all $g, x, y \in G$. Since $G \to Z(G)$, $g \mapsto g^n$ is a group homomorphism, Lemma 15.5 implies that $[x,y]^n = [x^n, y^n] = 1$ for all $[x,y] \in X$. The theorem follows from applying Dietzmann's theorem. □

Si G es un grupo, consideramos el subconjunto

$$\Delta^+(G) = \{x \in \Delta(G) : x \text{ tiene orden finito}\}.$$

lem:DcharG **Lemma 18.4.** *Si G es un grupo, entonces $\Delta^+(G)$ es un subgrupo característico de G.*

Proof. Claramente $1 \in \Delta^+(G)$. Sean $x, y \in \Delta^+(G)$ y sea H el subgrupo de G generado por el conjunto C formado por los finitos conjugados de x e y. Si $|x| = n$ y $|y| = m$, entonces $c^{nm} = 1$ para todo $c \in C$. Como C es finito y cerrado por conjugación, el teorema de Dietzmann implica que H es finito. Luego $H \subseteq \Delta^+(G)$ y en particular $xy^{-1} \in \Delta^+(G)$. Es evidente que $\Delta^+(G)$ es un subgrupo característico pues para todo $f \in \mathrm{Aut}(G)$ se tiene que $f(x) \in \Delta^+(G)$ si $x \in \Delta^+(G)$. □

La segunda aplicación del teorema de Dietzmann es el siguiente resultado:

lem:Connel **Lemma 18.5.** *Sea G un grupo y sea $x \in \Delta^+(G)$. Existe entonces un subgrupo finito H normal en G tal que $x \in H$.*

Dejamos la demostración como ejercicio ya que el muy similar a lo que hicimos en la demostración del lema 18.4.

thm:Connel **Theorem 18.6 (Connell).** *Supongamos que el cuerpo K es de característica cero. Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

1) *$K[G]$ es primo.*
2) *$Z(K[G])$ es primo.*
3) *G no tiene subgrupos finitos normales no triviales.*
4) *$\Delta^+(G) = 1$.*

Proof. Demostremos que (1) $\implies$ (2). Como $Z(K[G])$ es un anillo conmutativo, probar que es primo es equivalente a probar que no existen divisores de cero no triviales. Sean $\alpha, \beta \in Z(K[G])$ tales que $\alpha\beta = 0$. Sean $A = \alpha K[G]$ y $B = \beta K[G]$. Como α y β son centrales, A y B son ideales de $K[G]$. Como $AB = 0$, entonces $A = \{0\}$ o $B = \{0\}$ pues $K[G]$ es primo. Luego $\alpha = 0$ o $\beta = 0$.

Demostremos ahora que (2) $\implies$ (3). Sea N un subgrupo normal finito. Por el lema 18.1, $\widehat{N} = \sum_{x \in N} x$ es central en $K[G]$ y $\widehat{N}(\widehat{N} - |N|1) = 0$. Como $\widehat{N} \neq 0$ (pues K tiene característica cero) y $Z(K[G])$ es un dominio, $\widehat{N} = |N|1$, es decir: $N = \{1\}$.

Demostremos que (3) $\implies$ (4). Sea $x \in \Delta^+(G)$. Por el lema 18.5 sabemos que existe un subgrupo finito H normal en G que contiene a x. Como por hipótesis H es trivial, se concluye que $x = 1$.

Finalmente demostramos que (4) $\implies$ (1). Sean A y B ideales de $K[G]$ tales que $AB = 0$. Supongamos que $B \neq 0$ y sea $\beta \in B \setminus \{0\}$. Si $\alpha \in A$, entonces, como $\alpha K[G]\beta \subseteq \alpha B \subseteq AB = 0$, el lema 15.16 de Passman implica que $\pi_{\Delta(G)}(\alpha)\pi_{\Delta(G)}(\beta) = 0$. Como por hipótesis $\Delta^+(G)$ es trivial, sabemos que $\Delta(G)$ es libre de torsión y luego $\Delta(G)$ es abeliano por el lema 15.10. Esto nos dice que $K[\Delta(G)]$ no tiene divisores de cero y luego $\alpha = 0$. Demostramos entonces que $B \neq 0$ implica que $A = 0$. □

Theorem 18.7 (Connel). *Sea K un cuerpo de característica cero y sea G un grupo. Entonces $K[G]$ es artiniano a izquierda si y sólo si G es finito.*

Proof. Si G es finito, $K[G]$ es un álgebra de dimensión finita y luego es artiniano a izquierda. Supongamos entonces que $K[G]$ es artiniano a izquierda.

Primero observemos que si $K[G]$ es un álgebra prima, entonces por el teorema de Wedderburn $K[G]$ es simple y luego G es el grupo trivial (pues si G no es trivial, $K[G]$ no es simple ya que el ideal de aumentación es un ideal no nulo de $K[G]$).

Como $K[G]$ es artiniano a izquierda, es noetheriano a izquierda por Hopkins–Levitzky y entonces, $K[G]$ admite una serie de composición por el teorema 5.10. Para demostrar el teorema procederemos por inducción en la longitud de la serie de composición de $K[G]$. Si la longitud es uno, $\{0\}$ es el único ideal de $K[G]$ y luego $K[G]$ es prima y el resultado está demostrado. Si suponemos que el resultado vale para longitud n y además $K[G]$ no es prima, entonces, por el teorema de Connel, G posee un subgrupo normal H finito y no trivial. Al considerar el morfismo canónico $K[G] \to K[G/H]$ vemos que $K[G/H]$ es artiniano a izquierda y tiene longitud $< n$. Por hipótesis inductiva, G/H es un grupo finito y luego, como H también es finito, G es finito. □

Lecture 10

§19. Frobenius's theorem

thm:Frobenius

Theorem 19.1 (Frobenius). *Every finite-dimensioanal real division algebra is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.*

We present an elementaly proof. We shall need some lemmas.

lem:trick_frobenius1

Lemma 19.2. *Let D be a real division algebra such that $\dim D = n$. If $x \in D$, then there exists $\lambda \in \mathbb{R}$ such that $x^2 + \lambda x \in \mathbb{R}$.*

Proof. Since $\dim D = n$, the set $\{1, x, x^2, \dots, x^n\}$ is linearly dependent. So there exists a non-zero polynomial $f(X) \in \mathbb{R}[X]$ of degree $\leq n$ such that $f(x) = 0$. Without loss of generality we may assume that the leading coefficient of $f(X)$ is one. Then we can write $f(X)$ as a product of polynomials of degree ≤ 2, say

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_r)(X^2 + \lambda_1 X + \mu_1) \cdots (X^2 + \lambda_s X + \mu_s).$$

Since D is a division algebra and $f(x) = 0$, some factor of $f(X)$ is zero. If $x - \lambda_j \neq 0$ for all j, then x is a root of some $X^2 + \lambda_k X + \mu_k$. In any case, there exists $\lambda \in \mathbb{R}$ such that $x^2 + \lambda x \in \mathbb{R}$. □

lem:trick_frobenius2

Lemma 19.3. *Let D be a real division algebra of dimension n. Then*

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

is a subspace of D such that $D = \mathbb{R} \oplus V$.

Proof. Let $x \in D \setminus V$ be such that $x^2 \in \mathbb{R}$. Since $x^2 > 0$, it follows that $x^2 = \alpha^2$ for some $\alpha \in \mathbb{R}$. Thus $x = \pm\alpha \in \mathbb{R}$, as D is a division algebra and $(x - \alpha)(x + \alpha) = x^2 - \alpha^2 = 0$.

We claim that V is a subspace of D. Note that $0 \in V$ and that if $x \in V$, then $\lambda x \in V$ for all $\lambda \in \mathbb{R}$. Let $x, y \in V$. If $\{x, y\}$ is linearly dependent, then $x + y \in V$. If not, we claim that $\{1, x, y\}$ is linearly independent. If there exist $\alpha, \beta, \gamma \in \mathbb{R}$ such that $\alpha x + \beta y + \gamma = 0$, then

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

This implies that $2\beta\gamma y \in \mathbb{R}$ and thus $\beta\gamma = 0$. Hence $\alpha = \beta = \gamma = 0$. The previous lemma implies that there exist $\lambda, \mu \in \mathbb{R}$ such that

$$(x+y)^2 + \lambda(x+y) \in \mathbb{R}, \quad (x-y)^2 + \mu(x-y) \in \mathbb{R}.$$

Since

$$(x+y)^2 + (x-y)^2 = 2x^2 + 2y^2 \in \mathbb{R},$$

it follows that $(\lambda+\mu)x + (\lambda-\mu)y \in \mathbb{R}$. Since $\{1, x, y\}$ is linearly independent, $\lambda = \mu = 0$. Thus $(x+y)^2 \in \mathbb{R}$. If $x + y \notin V$, then, the first paragraph of the proof implies that $x + y \in \mathbb{R}$, a constradiction.

Clearly, $\mathbb{R} \cap V = 0$. If $x \in D \setminus \mathbb{R}$, then the previous lemma implies that $x^2 + \lambda x \in \mathbb{R}$ for some $\lambda \in \mathbb{R}$. We claim that $x + \lambda/2 \in V$. If not, since

$$(x + \lambda/2)^2 = x^2 + \lambda x + (\lambda/2)^2 \in \mathbb{R},$$

it follows that $x + \lambda/2 \in \mathbb{R}$ and thus $x \in \mathbb{R}$. Hence $x = -\lambda/2 + (x + \lambda/2) \in \mathbb{R} \oplus V$. □

lem:trick_frobenius3 **Lemma 19.4.** *Let D be a real algebra of (real) dimension n. If $n > 2$, then there exist $i, j, k \in D$ such that $\{1, i, j, k\}$ is linearly independent and*

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i. \tag{10.1}$$ eq:H

Proof. Let $V = \{x \in D : x^2 \in \mathbb{R}, x^2 \leq 0\}$ be the subspace of Lemma 19.3. For $x, y \in V$ let $x \circ y = xy + yx = (x+y)^2 - x^2 - y^2 \in \mathbb{R}$. If $x \neq 0$, then $x \circ x = 2x^2 \neq 0$. Since $\dim V = n - 1$, there exist $y, z \in V$ such that $\{y, z\}$ is linearly independent. Let

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

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

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

it follows that $xy = -yx$. Let

$$i = \frac{1}{\sqrt{-x^2}} x, \quad j = \frac{1}{\sqrt{-y^2}} y, \quad k = ij.$$

A direct calculation shows that the formulas of (10.1) hold. For example,

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

Now we are finally ready to prove the theorem:

Proof of 19.1. 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 19.3 is non-zero and thus there exists $i \in D$ such that $i^2 = -1$. Hence $D \simeq \mathbb{C}$. Lemma 19.4 implies that $n \neq 3$. If $n = 4$, then $D \simeq \mathbb{H}$. Suppose that $n > 4$. By Lemma 19.4 there exist $i, j, k \in D$ such that $\{1, i, j, k\}$ is linearly independent and that the formulas of (10.1) hold. Let

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

By Lemma 19.3, $\dim V = n - 1$. Thus there exists $x \in V \setminus \langle i, j, k \rangle$. Let

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

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

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

a contradiction. □

§20. Wedderburn's little theorem

Vamos a dar una demostración completamente elemental de un famoso teorema de Wedderburn. Antes necesitamos repasar algunos conceptos básicos sobre polinomios ciclotómicos.

Definition 20.1. El n-polinomio ciclotómico se define como

$$\Phi_n(X) = \prod (X - \zeta), \tag{10.2}$$ eq:ciclotomico

donde el producto se hace sobre todas las n-raíces primitivas de la unidad.

Example 20.2. Veamos algunos ejemplos:

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

Lemma 20.3. *Sea $n \in \mathbb{Z}_{>0}$. Entonces*

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

Proof. Escribimos

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

□

Lemma 20.4. *Sea $n \in \mathbb{Z}_{>0}$. Entonces $\Phi_n(X) \in \mathbb{Z}[X]$.*

Proof. Procederemos por inducción en n. El caso $n = 1$ es trivial pues $\Phi_1(X) = X - 1$. Supongamos entonces $\Phi_d(X) \in \mathbb{Z}[X]$ para todo $d < n$. Entonces

$$\prod_{d|n, d \neq n} \Phi_d(X) \in \mathbb{Z}[X]$$

y es un polinomio mónico. Luego $\Phi_n(X)/\prod_{d|n,d<n} \Phi_d(X) \in \mathbb{Z}[X]$. □

Theorem 20.5 (Wedderburn). *Todo anillo de división finito es un cuerpo.*

Proof. Sea $K = Z(D)$. Entonces K es un cuerpo finito, digamos $|K| = q$. Sea $n = \dim_K D$. Vamos a demostrar que $n = 1$. Supongamos que $n > 1$. La ecuación de clases para el grupo $D^\times = D \setminus \{0\}$ implica que

$$q^n - 1 = q - 1 + \sum_{j=1}^{m} \frac{q^n - 1}{q^{d_j} - 1}, \tag{10.3}$$

eq:clases

donde $1 < \frac{q^n-1}{q^{d_j}-1} \in \mathbb{Z}$ para todo $j \in \{1, \dots, m\}$. Como $d^{d_j} - 1$ divide a $q^n - 1$, cada d_j divide a n. En particular, la fórmula (10.2) implica que podemos escribir

$$X^n - 1 = \Phi_n(X)(X^{d_j} - 1)h(X) \tag{10.4}$$

eq:trick_ciclotomico

para algún polinomio $h(X) \in \mathbb{Z}[X]$. Al evaluar (10.4) en $X = q$ obtenemos que $\Phi_n(q)$ divide a $q^n - 1$ y que $\Phi_n(q)$ divide a $\frac{q^n-1}{q^{d_j}-1}$. Entonces, por (10.3), $\Phi_n(q)$ divide a $q - 1$. Luego

$$q - 1 \geq |\Phi_n(q)| = \prod |q - \zeta| > q - 1$$

pues cada $|q - \zeta| > q - 1$ (basta dibujar q y ζ en el plano complejo), una contradicción. □

Veamos como corolario una aplicación al último teorema de Fermat en anillos finitos. Demostraremos el siguiente resultado:

Theorem 20.6. *Sea R un anillo unitario finito. Entonces para todo $n \geq 1$ existen $x, y, z \in R \setminus \{0\}$ tales que $x^n + y^n = z^n$ si y sólo si R no es un anillo de división.*

Proof. Supongamos primero que R es de división. Por el teorema de Wedderburn, R es entonces un cuerpo finito, digamos $|R| = q$. Como entonces $x^{q-1} = 1$ para todo $x \in R \setminus \{0\}$, se concluye que la ecuación $x^{q-1} + y^{q-1} = z^{q-1}$ no tiene solución.

Supongamos ahora que R no es de división. Como entonces, en particular, R no es un cuerpo, $|R| > 2$ y luego $x + y = z$ tiene solución en $R \setminus \{0\}$ (tomar por ejemplo $x = 1$, $y = z - 1$ y $z \notin \{0, 1\}$). Como R es finito, R es artiniano a izquierda y entonces el radical de Jacobson $J(R)$ es nilpotente. Si $J(R) \neq 0$, existe entonces $a \in R \setminus \{0\}$ tal que $a^2 = 0$ y luego $a^n = 0$ para todo $n \geq 2$. En este caso, la ecuación $x^n + y^n = z^n$ tiene solución en $R \setminus \{0\}$ si $n \geq 2$ (tomar por ejemplo $x = a$, $y = z = 1$). Si $J(R) = 0$, entonces, R es semisimple y luego, por el teorema de Wedderburn,

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

donde los D_i son cuerpos finitos (por ser anillos de división finitos). Como R no es un cuerpo, hay dos posibilidades: o bien $n_i > 1$ para algún $i \in \{1, \dots, k\}$, o bien $k \geq 2$ y $n_i = 1$ para todo $i \in \{1, \dots, k\}$. En el primer caso, como $M_{n_i}(D_i)$ tiene elementos no nulos cuyo cuadrado es cero, R también los tiene, y luego, tal como se hizo antes, vemos que $x^n + y^n = z^n$ tiene solución. En el segundo caso, $x = (1, 0, 0, \dots, 0)$, $y = (0, 1, 0, \dots, 0)$ y $z = (1, 1, 0, \dots, 0)$ es una solución de $x^n + y^n = z^n$. $\square$

Lecture 11
Some hints

Lecture 1

Lecture 2

Lecture 3

Lecture 4

Lecture 5

Consider the proper non-zero ideal

$$I(G) = \left\{ \sum_{g \in G} \lambda_g g \in K[G] : \sum_{g \in G} \lambda_g = 0 \right\}.$$

2.69 Apply Zorn's lemma to the set of left ideals L such that $I \subseteq L \subsetneq R$ partially ordered by inclusion. A maximal element of S is a maximal left ideal of R that is left regular and that contains I.

Lecture 6

Lecture 7

Lecture 8

Lecture 9

Lecture 10

Lecture 9

Lecture 10

Lecture 11

Lecture 12

Lecture 13

Lecture 12
Some solutions

Lecture 1

Lecture 2

Lecture 3

2.24 Since R is unitary, there exists a maximal left ideal I and, moreover, R is regular. By Proposition 2.17, R/I is a simple R-module. Since $\mathrm{Ann}_R(R/I)$ is an ideal of R and R is simple, either $\mathrm{Ann}_R(R/I) \in \{0\}$ or $\mathrm{Ann}_R(R/I) = R$. Moreover, since $1 \notin \mathrm{Ann}(R/I)$, it follows that $\mathrm{Ann}_R(R/I) = \{0\}$.

2.25 If R is a field, then R is primitive because it is a unitary simple ring, see Exercise 2.24. If R is a primitive commutative ring, Proposition 2.17 implies that there exists a maximal regular ideal I such that R/I is a faithful simple R-module. Since $I \subseteq \mathrm{Ann}_R(R/I) = \{0\}$ and I is regular, there exists $e \in R$ such that $r = re = er$. Therefore R is a unitary commutative ring. Since $I = \{0\}$ is a maximal ideal, R is a field.

Lecture 4

2.31 Let R be a ring with identity and M be a maximal ideal of R. Then R/M is a simple unitary ring by Exercise **??**. Then R/M is primitive by Exercise 2.24. By Lemma 2.28, M is primitive.

Lecture 5

Lecture 6

Lecture 7

Lecture 8

Lecture 9

Lecture 10

10.1 Since a is algebraic,

$$a^n(1+\lambda_1 a+\cdots+\lambda_m a^m)=0$$

for some minimal $n \geq 0$ and scalars $\lambda_1,\ldots,\lambda_m$. If $n>0$, then

$$b=(1+\lambda_1 a+\cdots+\lambda_m a^m)a^{n-1}\neq 0$$

is such that $ab=ba=0$. If $n=0$, then

$$c=-\lambda_1-\lambda_2 a-\cdots-\lambda_m a^{m-1}\neq 0$$

is such that $ac=ca=1$.

Lecture 9

Lecture 10

Lecture 11

Lecture 12

Lecture 13

References

1. S. A. Amitsur. Nil radicals. Historical notes and some new results. In *Rings, modules and radicals (Proc. Internat. Colloq., Keszthely, 1971)*, pages 47–65. Colloq. Math. Soc. János Bolyai, Vol. 6, 1973.
2. M. Brešar. *Introduction to noncommutative algebra*. Universitext. Springer, Cham, 2014.
3. I. N. Herstein. A counterexample in Noetherian rings. *Proc. Nat. Acad. Sci. U.S.A.*, 54:1036–1037, 1965.
4. 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.
5. N. Jacobson. *Structure of rings*. American Mathematical Society Colloquium Publications, Vol. 37. American Mathematical Society, Providence, R.I., revised edition, 1964.
6. G. Köthe. Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist. *Math. Z.*, 32(1):161–186, 1930.
7. J. Krempa. Logical connections between some open problems concerning nil rings. *Fund. Math.*, 76(2):121–130, 1972.
8. P. P. Nielsen. Simplifying Smoktunowicz's extraordinary example. *Comm. Algebra*, 41(11):4339–4350, 2013.
9. D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.
10. A. Smoktunowicz. Polynomial rings over nil rings need not be nil. *J. Algebra*, 233(2):427–436, 2000.
11. A. Smoktunowicz. On some results related to Köthe's conjecture. *Serdica Math. J.*, 27(2):159–170, 2001.
12. A. Smoktunowicz. Some results in noncommutative ring theory. In *International Congress of Mathematicians. Vol. II*, pages 259–269. Eur. Math. Soc., Zürich, 2006.

Index