Leandro Vendramin

Associative algebras

Notes

Thursday 30th September, 2021

Contents

1 1

2 5

3 11

4 19

5 27

6 41

7 49

8 57

Some hints 63

Some solutions 65

References 67

Index 69

Lecture 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 $n \in \mathbb{N}$. 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 $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$, is a ring homomorphism that is not an algebra homomorphism over $\mathbb{C}$.

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

Exercise 1.11. Let A be an algebra and G be a finite group. If $f\colon G \to \mathscr{U}(A)$ 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 $\{1, a, a^2, \ldots, a^n\}$ has $n+1$ elements, it is a linearly dependent set. Thus there exists a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$. □

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. □

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

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 $S_i \cap (N \oplus T) \subseteq S_i$. Since the module S_i is simple, it follows that $S_i \cap (N \oplus T) = \{0\}$. Thus $N \cap (S_i \oplus T) = \{0\}$, a contradiction to the maximality of $\dim T$.

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

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

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

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

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

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

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

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

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

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

is also semisimple. □

Lecture 2

Definition 2.1. An algebra A is **semisimple** if every finitely-generated A-module is semisimple.

Proposition 2.2. *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. 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 2.3. *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 2.4. 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 2.5. *Let D be a division algebra and V be a finitey-generated module over D. Then V is a simple module over $\mathrm{End}_D(V)$ and there exits $n \in \mathbb{Z}_{>0}$ such that $\mathrm{End}_D(V) \simeq nV$ is semisimple.*

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

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

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

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

it follows that the map is an isomorphism. Thus

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

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 $f \in \mathrm{End}_D(V)$ such that $f\cdot v = f(v) = w$. Thus $w \in (v)$ and therefore $V = (v)$. □

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

Theorem 2.6. *Let A be a finite-dimensional algebra and let $S_1,\dots,S_k$ be the simple modules over A. If*

$$M \simeq n_1S_1 \oplus \cdots \oplus n_kS_k,$$

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 $\mathrm{Hom}_A(S_i,S_j) = \{0\}$ whenever $i \neq j$. For each $j \in \{1,\dots,k\}$,

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

Since M and S_j are finite-dimensional vector spaces, $\mathrm{Hom}_A(M,S_j)$ and $\mathrm{Hom}_A(S_j,S_j)$ are finite-dimensional vector spaces. Moreover, since $\mathrm{id} \in \mathrm{Hom}_A(S_j,S_j)$, it follows that $\dim \mathrm{Hom}_A(S_j,S_j) \geq 1$. 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 2.7.** *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 bijection $\mathrm{End}_A(A) \to A^{\mathrm{op}}$ 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 2.8.** *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 $i, j \in \{1, \ldots, n\}$, $a = (a_{ij})$ 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 2.9.** *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:

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

The reader should prove that the map is an injective algebra homomorphism

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

It is surjective: if $\psi \in \mathrm{End}(nS)$ and $i, j \in \{1, \ldots, n\}$ one defines ψ_{ij} by

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

Theorem 2.10 (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 $n_1, \ldots, n_k \in \mathbb{N}$ and some division algebras $D_1, \ldots, D_k$.

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

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

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

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

Since $\mathrm{End}_A(A) \simeq A^{\mathrm{op}}$, 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 2.11 (Mollien). *If A is a finite-dimensional complex semisimple algebra, then*

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

for some $n_1, \ldots, n_k \in \mathbb{N}$.

Proof. By Wedderburn's theorem,

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

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 isomorhpism. In particular,

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

Exercise 2.12. Let A and B be algebras. Prove that the ideals of $A \times B$ are of the form $I \times J$, where I is an ideal of A and J is an ideal of B.

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

Proposition 2.14. *Let A be a finite-dimensional simple algebra. There exists a non-zero left ideal I of minimal dimension. This ideal is a simple A-module and every simple A-module is isomorphic to I.*

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

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

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

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

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

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

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

Proposition 2.15. *Let A be a finite-dimensional algebra. If A is simple, then A is semisimple.*

Proof. Let S be the sum of the simple submodules appearing in the regular representation of A. We claim that S is an ideal of A. We 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 representaion of A is semisimple (because it is a sum of simple submodules). Therefore A is semisimple. □

Theorem 2.16 (Wedderburn). *Let A be a finite-dimensional algebra. If A is simple, then $A \simeq M_n(D)$ for some $n \in \mathbb{N}$ 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 $n_1, \ldots, n_k$ and some division algebras $D_1, \ldots, D_k$. 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 $n \in \mathbb{N}$ and some division algebra D. □

Lecture 3

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 3.1. $2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$ 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 3.2. If I and J are both ideals of R, then the sum $I+J = \{x+y : x \in I, y \in J\}$ and the intersection $I \cap J$ are both ideals of R. The product IJ, defined as the additive subgroup of R generated by $\{xy : x \in I, y \in J\}$, is also an ideal of R.

Example 3.3. If R is a ring, the set $Ra = \{xa : x \in R\}$ is a left ideal of R. Similarly, the set $aR = \{ax : x \in R\}$ is a right ideal of R. The set RaR, which is defined as the additive subgroup of R generated by $\{xay : x,y \in R\}$, is a ideal of R.

Example 3.4. 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 3.5. 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 3.6. 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

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

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

Exercise 3.7. 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 $R \times M \to M$, $(r, m) \mapsto rm$, such that

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

for all $r, s \in R$, $m, n \in M$. If R has an identity 1 and $1m = m$ holds for all $m \in M$, the module M is said to be **unitary**. If M is a unitary module, then $M = RM \neq \{0\}$.

Definition 3.8. A module M is said to be **simple** if $RM \neq \{0\}$ and the only submodules of M are 0 and M. If M is a simple module, then $M \neq \{0\}$.

lemma:simple **Lemma 3.9.** *Let M be a non-zero module. Then M is simple if and only if $M = Rm$ for all $0 \neq m \in M$.*

Proof. Assume that M is simple. Let $m \neq 0$. Since Rm is a submodule of the simple module M, either $Rm = \{0\}$ or $Rm = M$. Let $N = \{n \in M : Rn = \{0\}\}$. Since N is a submodule of M and $RM \neq \{0\}$, $N = \{0\}$. Therefore $Rm = M$, as $m \neq 0$. Now assume that $M = Rm$ 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 $M = Rx \subseteq L$. □

Example 3.10. 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-módulo with $fv = f(v)$, $f \in R$. $v \in V$.

exa:I_k **Example 3.11.** 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 3.12. 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 3.13. Let D be a division ring and let $R = M_n(D)$. Then $L = RE_{11}$ is a minimal left ideal.

Example 3.14. 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 3.15. 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 3.16. 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 3.17. *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 $M = Rm$ for some $m \neq 0$ by Lemma 3.9. The map $\phi : R \to M$, $r \mapsto rm$, is an epimorphism 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 simpllicity 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 $m = em$. If $r \in R$, then $r - re \in I$ since $\phi(r - re) = \phi(r) - \phi(re) = rm - r(em) = 0$.

Supongamos ahora que L es maximal y regular. Por el teorema de la correspondencia, R/L no tiene submódulos propios no nulos. Veamos entonces que $R(R/L) \neq 0$. Si $R(R/L) = 0$ y $r \in R$, entonces, como L es regular, $r - re \in L$ y luego $r \in L$ pues

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

una contradicción a la maximalidad de L. □

We will now discuss primitive rings.

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

$$\mathrm{Ann}_R(N) = \{r \in R : rn = 0 \ \forall n \in N\}.$$

Example 3.18. $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/n) = n\mathbb{Z}$.

Exercise 3.19. 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 3.20. A module M is said to be **faithful** if $\mathrm{Ann}_R(M) = \{0\}$.

Example 3.21. If K is a field, then K^n is a faithful unitary $M_n(K)$-module.

Example 3.22. If V is vector space over a field K, then V is faithful unitary $\mathrm{End}_K(V)$-module.

Definition 3.23. 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.

proposition:simple=>prim

Proposition 3.24. *If R is a simple unitary ring, then R is primitive.*

Proof. Since R is unitary, there exists a maximal left ideal I and, moreover, R is regular. By Proposition 3.17, 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 $\mathrm{Ann}_R(R/I) = \{0\}$. □

osition:prim+conm=cuerpo

Proposition 3.25. *If R is a commutative ring, then R is primitive if and only if R is a field.*

Proof. If R is a field, then R is primitive because it is a unitary simple ring, see Proposition 3.24. If R is a primitive commutative ring, Proposition 3.17 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. □

Example 3.26. The ring $\mathbb{Z}$ is not primitive.

Definition 3.27. 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 3.28. *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 $(r+P)m = rm$, $r \in R$, $m \in M$. 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 $(r+P)M = 0$, 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 $rm = (r+P)m$, $r \in R$, $m \in M$, turns M into an R-module. It follows that M is simple and that $P = \mathrm{Ann}_R(M)$. □

Example 3.29. Let $R_1, \ldots, R_n$ be primitive ring 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 3.30. *Let R be a ring. Si P es un ideal primitivo, existe un ideal a izquierda L maximal tal que $P = \{x \in R : xR \subseteq L\}$. Recíprocamente, si L es un ideal a izquierda maximal y regular, entonces $\{x \in R : xR \subseteq L\}$ es un ideal primitivo.*

Proof. Assume that $P = \mathrm{Ann}_R(M)$ for some simple R-module M. By Proposition 3.17, there exists a regular maximal left ideal L such that $M \simeq R/L$. Then $P = \mathrm{Ann}_R(R/L) = \{x \in R : xR \subseteq L\}$.

Conversely, let L a regular maximal left ideal.By Proposition 3.17, R/L is a simple R-module simple. Then

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

if a primitive ideal. □

Proposition 3.31. *Maximal ideals of unitary rings are primitive.*

Proof. Let R be a ring with identity and M be a maximal ideal of R. Then R/M is a simple unitary ring by Proposition 3.17. Then R/M is primitive by Proposition 3.24. By lema 3.28, M is primitive. □

Exercise 3.32. Prove that every primitive ideal of a commutative ring is maximal.

Exercise 3.33. Prove that $M_n(R)$ is primitive if and only if R is primitive.

Let us discuss the Jacobson radical and radical rings.

Definition 3.34. 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 $n \in \mathbb{N}$, I^n is the additive subgroup of R generated by the set $\{y_1 \dots y_n : y_j \in I\}$.

Definition 3.35. An ideal I of R is **nilpotent** if $I^n = \{0\}$ for some $n \in \mathbb{N}$.

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

Definition 3.36. An element x of a ring is said to be **nil** (or nilpotent) if $x^n = 0$ for some $n \in \mathbb{N}$.

Definition 3.37. 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 3.38. 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 $k \in \mathbb{N}$ 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 3.39.** *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. □

Definition 3.40. 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 3.41.** 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 3.42. 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 3.43. 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 3.44. 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 3.45.** *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

$$x = 0 \circ x = (s \circ r) \circ x = s \circ (r \circ x) = s \circ 0 = s.$$ □

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 3.46. *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 $x \notin \mathrm{Ann}_R(R/M)$.*

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

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

Let $\mathscr{S}$ 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 $\mathscr{S}$, 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 $\mathscr{S}$ admits a maximal element M. Thus M is a maximal left ideal such that $x \notin M$. Moreover, M is regular since $r + r(-x) \in T \subseteq M$ for all $r \in R$. Therefore R/M is a simple R-module by Proposition 3.17. 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 3.47. *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 3.46 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 3.45. □

The theorem immediately implies the following corollary.

Corollary 3.48. *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 3.49.** *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 3.17,

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

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

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

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

Example 3.50. Each maximal ideals of $\mathbb{Z}$ is of the form $p\mathbb{Z} = \{pm : m \in \mathbb{Z}\}$ for some prime number p. Thus $J(\mathbb{Z}) = \cap_p p\mathbb{Z} = \{0\}$.

Lecture 4

We now review some basic results useful to compute radicals.

Proposition 4.1. *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 4.2. *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 4.3. *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 4.2. □

Definition 4.4. A ring R is said to be **radical** if $J(R) = R$.

Example 4.5. If R is a ring, then $J(R)$ is a radical ring, by Proposition 4.3.

Example 4.6. The Jacobson radical of $\mathbb{Z}/8$ is $\{0,2,4,6\}$.

There are several characterizations of radical rings.

theorem:anillo_radical

Theorem 4.7. *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 3.47.

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 3.17.

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. □

Example 4.8. 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 4.9. 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 4.10. Prove that a nil ring is a radical ring.

Exercise 4.11. 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:Jnilpotente

Theorem 4.12. *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 $(J^m)_{m\in\mathbb{N}}$ of left ideals stabilizes. There exists $k \in \mathbb{N}$ such that $J^k = J^l$ for all $l \geq k$. We claim that $J^k = \{0\}$. If $J^k \neq \{0\}$ let $\mathscr{S}$ 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 $\mathscr{S}$ is non-empty. Since R is left artinian, $\mathscr{S}$ 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 $J^k x \in \mathscr{S}$, 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 4.13. *Let R be a left artinian ring. Each nil left ideal is nilpotent and $J(R)$ is the unique maximal nilpotent ideal of R.*

Proof. Let L be a nil left ideal of R. By Proposition 3.39, L is contained in $J(R)$. Thus L is nilpotent, as $J(R)$ is nilpotent by Theorem 4.12. □

Theorem 4.14. *Let R be a ring and $n \in \mathbb{N}$. 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 $m_1, \ldots, m_n \in M$. Then

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

In particular, $x_{ij} \in \operatorname{Ann}_R(M)$ for all $i, j \in \{1, \ldots, n\}$. 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 $i \in \{1, \ldots, n\}$. In conclusion,

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

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

Exercise 4.15. Let R be a unitary ring. Then

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

Exercise 4.16. 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) $1 + \sum_{i=1}^{n} r_i x s_i$ is invertible for all $n \in \mathbb{N}$ and all $r_i, s_i \in R$.
6) x belongs to every left maximal ideal maximal.

The following exercises are optional. They somewhat show a recent new application of radical rings to solutions of the celebrated Yang–Baxter equation.

Exercise 4.17. A pair (X, r) is a **solution** to the Yang–Baxter equation if X is a set and $r \colon X \times X \to X \times X$ is a bijective map such that

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

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

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

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

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

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

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

Prove the following statements:

2) $\lambda\colon (R,\circ)\to \mathrm{Aut}(R,+)$, $x\mapsto\lambda_x$, is wis a group homomorphism.
3) $\mu\colon (R,\circ)\to \mathrm{Aut}(R,+)$, $y\mapsto\mu_y$, 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 4.18. If D is a division ring and $R=D[X_1,\dots,X_n]$, then $J(R)=\{0\}$.

Example 4.19. 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.

Theorem 4.20. *Let A be a K-algebra and I be a subset of A. Then I is a left regular maximal ideal ideal of the algebra A if and only if I is a left regular maximal ideal of the ring A.*

Proof. Sea I un ideal a izquierda maximal y regular del anillo A. Queremos demostrar que $\lambda I\subseteq I$ para todo $\lambda\in K$. Si suponemos que $\lambda I\not\subseteq I$ para algún λ, entonces $I+\lambda I$ es un ideal a izquierda del anillo A que contiene a I pues

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

Como I es maximal, $I+\lambda I=A$. Por la regularidad de I, existe $e\in R$ tal que $a-ae\in I$ para todo $a\in A$. Si escribimos $e=x+\lambda y$ para $x,y\in I$, entonces

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

Como $e^2-e\in I$ y $e^2\in I$, se concluye que $e\in I$. Luego $A=I$ pues $a-ae\in I$ para todo $a\in A$, una contradicción.

Recíprocamente, si I es un ideal a izquierda maximal y regular del álgebra A, entonces I es ideal a izquierda regular del anillo A. Falta ver entonces que I es maximal. Por el ejercicio **??** sabemos que existe un ideal a izquierda maximal L del anillo A que contiene a I. Como L es regular, la implicación demostrada nos dice que L es un ideal a izquierda maximal y regular del anillo A. Luego $L = I$ por la maximalidad de I. □

Corollary 4.21. *Sea A un álgebra. El radical de Jacobson del anillo A coincide con el radical de Jacobson del álgebra A.*

Proof. Es consecuencia del teorema anterior y de que el radical de Jacobson es la intersección de los ideales a izquierda maximales y regulares. □

lemma:algebraico=nil

Lemma 4.22. *Sea A un álgebra unitaria y sea $x \in J(A)$. Entonces x es algebraico si y sólo si x es nil.*

Proof. Demostremos la implicación no trivial. Como x es algebraico, existen $a_0, \dots, a_n \in K$ no todos cero tales que

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

Sea r el menor entero tal que $a_r \neq 0$. Podemos escribir entonces

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

donde $b_1, \dots, b_m \in K$. Como $1 + b_1 x + \cdots + b_m x^m$ es una unidad por el corolario **??**, entonces $x^r = 0$. □

Como aplicación tenemos el siguiente resultado:

thm:algebraica=>Jnil

Theorem 4.23. *Si A es un álgebra algebraica, $J(A)$ es el mayor ideal nil de A.*

Proof. Por el lema 4.22, $J(A)$ es un ideal nil. Por la propoisición 3.39, $J(A)$ es el mayor ideal nil de A. □

thm:Amitsur

Theorem 4.24 (Amitsur). *Si A es una K-álgebra unitaria tal que $\dim_K A < |K|$ (como cardinales), entonces $J(A)$ es el mayor ideal nil de A.*

Proof. Si K es un cuerpo finito, entonces A es un álgebra de dimensión finita. Como entonces A es algebraica, $J(A)$ es un ideal nil por el teorema 4.23.

Supongamos entonces que K es infinito. Sea $a \in J(A)$. El corolario **??** implica que todo elemento de la forma $1 - \lambda^{-1} a$, $\lambda \in K \setminus \{0\}$, es inversible. Entonces

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

es inversible para todo $\lambda \in K \setminus \{0\}$. Sea $S = \{(a - \lambda)^{-1} : \lambda \in K \setminus \{0\}\}$. Como

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

entonces $|S| = |K \setminus \{0\}| = |K| > \dim_K A$. Como entonces S es linealmente dependiente, existen escalares no nulos $\beta_1, \ldots, \beta_n \in K$ y elementos distintos $\lambda_1, \ldots, \lambda_n \in K$ tales que

$$\sum_{i=1}^{n} \beta_i (a - \lambda_i)^{-1} = 0. \tag{4.1}$$

eq:Amitsur

Si multiplicamos (4.1) por $\prod_{i=1}^{n}(a - \lambda_i)$, obtenemos

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

Afirmamos que a es algebraico sobre K. En efecto,

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

es no nulo pues $f(\lambda_1) = \beta_1(\lambda_1 - \lambda_2) \cdots (\lambda_1 - \lambda_n) \neq 0$ y cumple que $f(a) = 0$. Como $a \in J(A)$ es algebraico, a es nil por el lema 4.22. □

Amitsur's theorem implies the following result.

Corollary 4.25. *Sea K un cuerpo no numerable y A una K-álgebra con base numerable. Entonces $J(A)$ es el mayor ideal nil de A.*

The following problem is maybe the most important open problem in noncommutative ring theory.

prob:Koethe

Open problem 4.26 (Köthe). Let R be a ring. Is the sum of two arbitrary nil left ideals of R is nil?

Open problem 4.26 is the well-known Köthe's conjecture. The conjecture was first formulated in 1930, see [2]. It is known to be true in several cases. In full generality, the problem is still open. In [3] 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 [5] 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 [4]. See [6, 7] for more information on Köthe's conjecture and related topics.

Lecture 5

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

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

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

Exercise 5.4. 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 5.5. 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 5.6. 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.

Veamos otros ejemplo un poco más difíciles. La idea a utilizar es la siguiente: Si A es una K-álgebra y $\rho\colon G \to U(A)$ es un morfismo de grupos, donde $U(A)$ es el grupo de unidades de A, entonces la función $K[G] \to A$, $\sum_{g\in G} \lambda_g g \mapsto \sum_{g\in G} \lambda_g \rho(g)$, es un morfismo de álgebras.

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

Exercise 5.8. 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) $\mathbb{Q}[G] \simeq \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q})$.

Theorem 5.9 (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. Supongamos que $G = \{g_1, \ldots, g_n\}$ con $g_1 = 1$. Sea $\rho\colon K[G] \to K$ dada por $\alpha \mapsto \text{traza}(L_\alpha)$, donde $L_\alpha(\beta) = \alpha\beta$. Tenemos $\rho(g_1) = n$ y $\rho(g_i) = 0$ para todo $i \in \{2, \ldots, n\}$ pues, como $L_{g_i}(g_j) = g_i g_j \neq g_j$, la matriz de L_{g_i} en la base $\{g_1, \ldots, g_n\}$ tiene ceros en la diagonal.

Supongamos que $J = J(K[G])$ es no nulo y sea $\alpha = \sum_{i=1}^n \lambda_i g_i \in J \setminus \{0\}$. Sin pérdida de generalidad podemos suponer que $\lambda_1 \neq 0$ (pues si $\lambda_1 = 0$ hay algún $\lambda_i \neq 0$ y alcanza con tomar $g_i^{-1}\alpha \in J$). Entonces

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

Como G es un grupo finito, $K[G]$ es un álgebra de dimensión finita y luego $K[G]$ es artiniana a izquierda. Como el radical de Jacobson J es un ideal nilpotente, en particular α es un elemento nil. Luego L_α es nilpotente y entonces $0 = \rho(\alpha) = n\lambda_1$. Esto implica que la característica del cuerpo K divide a n.

Recíprocamente, supongamos que la característica de K es un número primo que divide a n y sea $\alpha = \sum_{i=1}^n g_i$. Como $\alpha g_j = g_j \alpha = \alpha$ para todo $j \in \{1, \ldots, n\}$, el conjunto $I = K[G]\alpha$ es un ideal de $K[G]$. Como además

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

se concluye que I es un ideal no nulo y nilpotente. Luego $J(K[G]) \neq 0$ pues por la proposición 3.39 sabemos que $I \subseteq J(K[G])$. □

cor:GfinitoNOnil

Corollary 5.10. *Sea G un grupo finito. Entonces $K[G]$ no contiene ideales a izquierda nil no nulos.*

Proof. Es consecuencia inmediata del teorema de Maschke ya que $J(K[G])$ contiene a todo ideal a izquierda nil. □

Herstein's theorem

El objetivo de esta sección responderemos la siguiente pregunta: ¿Cuándo un álgebra de grupo es un álgebra algebraica? Una respuesta parcial está dada por el teorema de Herstein.

Definition 5.11. Un grupo G se dice **localmente finito** si todo subgrupo de G finitamente generado es finito.

Si G es un grupo localmente finito, entonces todo $g \in G$ tiene orden finito (pues el subgrupo $\langle g \rangle$ es finito por ser finitamente generado).

Example 5.12. Todo grupo finito es obviamente localmente finito.

Example 5.13. El grupo $\mathbb{Z}$ no es localmente finito pues es libre de torsión.

Example 5.14. Sea p un primo. El **grupo de Prüfer**

$$\mathbb{Z}(p^\infty) = \{z \in \mathbb{Z} : z^{p^n} = 1 \text{ para algún } n \in \mathbb{N}\}$$

de todas las raíces p-ésimas de uno es localmente finito.

Example 5.15. Sean X un conjunto infinito y $\mathbb{S}_X$ el conjunto de biyecciones $X \to X$ que mueven únicamente una cantidad finita de elementos de X. Entonces $\mathbb{S}_X$ es localmente finito.

Antes de demostrar el teorema de Herstein vamos a dar una familia de ejemplos de grupos localmente finitos. Para eso necesitamos un lema:

lem:solvable_torsion=>lf

Lemma 5.16. *Sea G un grupo y sea N un subgrupo normal de G. Si N y G/N son localmente finitos, entonces G es localmente finito.*

Proof. Sea $\pi\colon G \to G/N$ el morfismo canónico. Sea $\{g_1, \ldots, g_n\}$ un subconjunto finito de G. Como G/N es localmente finito, el subgrupo Q de G/N generado por $\pi(g_1), \ldots, \pi(g_n)$ es finito, digamos

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

Para cada $i, j \in \{1, \ldots, n\}$ sabemos que existen $u_{ij} \in N$ y $k \in \{1, \ldots, m\}$ tales que $g_i g_j = u_{ij} g_k$. Sea U el subgrupo de G generado por los u_{ij}. Como N es localmente finito, U es un subgrupo finito. Como además cada elemento $g_i g_j g_l$ puede escribirse como

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

para algún $u \in U$ y algún $t \in \{1, \ldots, m\}$, se concluye que el subgrupo H de G generado por $\{g_1, \ldots, g_n\}$ es finito pues $|H| \leq m|U|$. □

Veamos una aplicación a los grupos resolubles. Recordemos que un grupo G se dice **resoluble** si existe una sucesión de subgrupos

$$1 = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = G \tag{5.1}$$

eq:resoluble

donde cada G_i es normal en G_{i+1} y cada cociente G_i/G_{i-1} es abeliano.

Proposition 5.17. *Si G es un grupo resoluble y de torsión, entonces G es localmente finito.*

Proof. Procederemos por inducción en la longitud n de la sucesión de resolubilidad (5.1). Si $n = 1$ entonces G es finito por ser abeliano y de torsión. Supongamos que el resultado vale para grupos resolubles de longitud $n-1$ y sea G un grupo resoluble tal que (5.1). Por hipótesis inductiva, el subgrupo normal G_{n-1} de G es localmente finito. Entonces, como G/G_{n-1} es localmente finito por ser abeliano y de torsión, el resultado se obtiene del lema 5.16. □

Theorem 5.18 (Herstein). *Si G es un grupo localmente finito, entonces $K[G]$ es algebraica. Recíprocamente, si $K[G]$ es algebraica y K es de característica cero, entonces G es localmente finito.*

Proof. Supongamos que G es localmente finito y sea $\alpha \in K[G]$. El subgrupo $H = \langle \operatorname{supp} \alpha \rangle$ es finitamente generado y luego finito. Como $\alpha \in K[H]$ y $\dim_K K[H] < \infty$, el conjunto $\{1, \alpha, \alpha^2, \ldots\}$ es linealmente dependiente. Luego α es algebraico sobre K.

Sea $\{x_1, \ldots, x_m\}$ un subconjunto finito de G. Si agregamos los inversos, podemos suponer que $\{x_1, \ldots, x_m\}$ genera al subgrupo $H = \langle x_1, \ldots, x_m \rangle$ como semigrupo. Si $\alpha = x_1 + \cdots + x_m \in K[G]$, entonces, como α es algebraico sobre K,

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

para algún $n \geq 0$ y escalares $a_0, \ldots, x_n \in K$. Sea $w = x_{i_1} \cdots x_{i_{n+1}} \in H$ una palabra de longitud $n+1$. Observemos que existen enteros positivos $c_{i_1 \cdots i_m}$ tales que

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

Como K es de característica cero, se concluye que $w \in \operatorname{supp}(\alpha^{n+1})$. Pero como además $\alpha^{n+1} = \sum_{j=0}^{n} a_j \alpha^j$, entonces $w \in \operatorname{supp}(\alpha^j)$ para algún $j \in \{0,\dots,n\}$. Demostramos entonces que toda palabra en las x_j de longitud $n+1$ puede escribirse como una palabra en las x_j de longitud a lo sumo n. Luego H es finito y entonces G es localmente finito. □

Formanek's theorem

Veremos un resultado de Formanek que puede entenderse como una generalización del teorema de Herstein.

Exercise 5.19. Sea A un álgebra algebraica y sea $a \in A$. Demuestre las siguientes afirmaciones:

1) a es un divisor de cero a izquierda si y sólo si a es un divisor de cero a derecha.
2) a es inversible a izquierda si y sólo si a es inversible a derecha.
3) a es inversible si y sólo si a no es un divisor de cero.

exa:norma **Exercise 5.20.** Si $\alpha = \sum_{g\in G} \alpha_g g \in \mathbb{C}[G]$ se define $|\alpha| = \sum_{g\in G} |\alpha_g| \in \mathbb{R}$. Demuestre que valen las siguientes propiedades:

1) $|\alpha+\beta| \le |\alpha| + |\beta|$, y
2) $|\alpha\beta| \le |\alpha||\beta|$

para todo $\alpha, \beta \in \mathbb{C}[G]$.

thm:FormanekQ **Theorem 5.21 (Formanek, primera versión).** *Sea G un grupo y supongamos que todo elemento de $\mathbb{Q}[G]$ es inversible o un divisor de cero. Entonces G es localmente finito.*

Proof. Sea $\{x_1,\dots,x_n\}$ un subconjunto finito de G. Si agregamos los inversos, podemos suponer que $\{x_1,\dots,x_n\}$ genera al subgrupo $H = \langle x_1,\dots,x_n\rangle$ como semigrupo. Sea

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

Veamos que $1-\alpha \in \mathbb{Q}[G]$ es inversible. Si no, entonces es un divisor de cero. Si existe $\delta \in \mathbb{Q}[G]$ tal que $\delta(1-\alpha) = 0$, entonces $\delta = \delta\alpha$ y luego, como

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

se concluye que $\delta = 0$. Similarmente se demuestra que $(1-\alpha)\delta = 0$ implica que $\delta = 0$.

Sea $\beta = (1-\alpha)^{-1} \in \mathbb{Q}[G]$. Para cada k definimos

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

Entonces

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

y luego $\gamma_k = -\alpha^{k+1}\beta$. Como

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

se concluye que $\lim_{k\to\infty}|\gamma_k| = 0$.

Para terminar veamos que $H \subseteq \operatorname{supp}\beta$. Si $H \not\subseteq \operatorname{supp}\beta$, sea $h \in H \setminus \operatorname{supp}\beta$. Supongamos que $h = x_{i_1}\cdots x_{i_m}$ es una palabra de longitud m en los x_j. Sea c_j el coeficiente de h en α^j. Entonces $c_0+\cdots+c_k$ es el coeficiente de h en γ_k, pero

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

para todo $k \geq m$ pues cada c_j es no negativo, una contradicción pues demostramos que $|\gamma_k| \to 0$ si $k \to \infty$. □

A continuación explicaremos por qué el teorema de Formanek se considera una generalización del teorema de Herstein. En el teorema 5.21 nos concentramos en álgebras de grupo sobre los números racionales. ¿Cómo podemos extender este resultado a álgebras de grupo sobre cuerpos de característica cero? Para extender el cuerpo de base sobre el que se trabaja necesitamos definir el producto tensorial de espacios vectoriales y el producto tensorial de álgebras.

Definition 5.22. El **producto tensorial** de los K-espacios vectoriales U y V es el espacio vectorial cociente $K[U\times V]/T$, donde $K[U\times V]$ es el espacio vectorial con base $\{(u,v) : u \in U, v \in V\}$ y T es el subespacio generado por los elementos de la forma

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

para $\lambda,\mu \in K$, $u,u' \in U$ y $v,v' \in V$.

El producto tensorial de U y V será denotado por $U \otimes_K V$ o por $U \otimes V$ si la referencia al cuerpo K puede omitirse. Dados $u \in U$ y $v \in V$ escribiremos $u \otimes v$ para denotar a la coclase $(u,v)+T$.

Theorem 5.23. *Sean U y V espacios vectoriales. Existe entonces una función bilineal $U\times V \to U\otimes V$, $(u,v)\mapsto u\otimes v$, tal que todo elemento de $U\otimes V$ es una suma finita de la forma*

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

para $u_1,\ldots,u_N \in U$ y $v_1,\ldots,v_N \in V$. Más aún, dado un espacio vectorial W y una función bilineal $\beta : U\times V \to W$, existe una función lineal $\overline{\beta} : U\otimes V \to W$ tal que $\overline{\beta}(u\otimes v) = \beta(u,v)$ para todo $u \in U$ y $v \in V$.

Proof. Por la definición del producto tensorial, la función

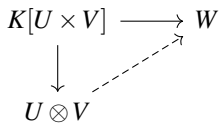
$$U \times V \to U \otimes V, \quad (u,v) \mapsto u \otimes v,$$

es bilineal. También de la definición se deduce inmediatamente que todo elemento de $U \otimes V$ es una combinación lineal finita de elementos de la forma $u \otimes v$, donde $u \in U$ y $v \in V$. Como $\lambda(u \otimes v) = (\lambda u) \otimes v$ para todo $\lambda \in K$, la primera afirmación queda demostrada.

Como $U \times V$ es base de $K[U \times V]$, existe una transformación lineal

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

Como β es bilineal por hipótesis, $T \subseteq \ker\gamma$. Existe entonces una transformación lineal $\overline{\beta}\colon U \otimes V \to W$ tal que



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

xca:tensorial_unicidad

Exercise 5.24. Demuestre que las propiedades mencionadas en el teorema anterior caracterizan el producto tensorial salvo isomorfismo.

Veamos algunas propiedades del producto tensorial de espacios vectoriales.

Lemma 5.25. *Sean $\varphi\colon U \to U'$ y $\psi\colon V \to V'$ transformaciones lineales. Existe entonces una única transformación lineal $\varphi \otimes \psi\colon U \otimes V \to U' \otimes V'$ tal que*

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

para todo $u \in U$ y $v \in V$.

Proof. Como la función $U \times V \to U \otimes V$, $(u,v) \mapsto \varphi(u) \otimes \psi(v)$, es bilineal, existe una transformación lineal $U \otimes V \to U \otimes V$, $u \otimes v \to \varphi(u) \otimes \psi(v)$. Luego la función

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

está bien definida. □

Exercise 5.26. Demuestre las siguientes afirmaciones:

1) $(\varphi \otimes \psi)(\varphi' \otimes \psi') = (\varphi\varphi') \otimes (\psi\psi')$.
2) Si φ y ψ son isomorfismos, entonces $\varphi \otimes \psi$ es un isomorfismo.
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) Si $U \simeq U'$ y $V \simeq V'$, entonces $U \otimes V \simeq U' \otimes V'$.

Lemma 5.27. *Si U y V son espacios vectoriales, entonces $U \otimes V \simeq V \otimes U$.*

Proof. Como la función $U \times V \to V \otimes U$, $(u,v) \mapsto v \otimes u$, existe una transformación lineal $U \otimes V \to V \otimes U$, $u \otimes v \mapsto v \otimes u$. Similarmente se demuestra que existe una transformación lineal $V \otimes U \to U \otimes V$, $v \otimes u \mapsto u \otimes v$. Luego $U \otimes V \simeq V \otimes U$. □

xca:UxVxW **Exercise 5.28.** Demuestre que $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$.

xca:UxK **Exercise 5.29.** Demuestre que $U \otimes K \simeq K \simeq K \otimes U$.

lem:U_LI **Lemma 5.30.** *Sea $\{u_1, \ldots, u_n\} \subseteq U$ un conjunto linealmente independiente y sean $v_1, \ldots, v_n \in V$ tales que $\sum_{i=1}^n u_i \otimes v_i = 0$. Entonces $v_i = 0$ para todo $i \in \{1, \ldots, n\}$.*

Proof. Sea $i \in \{1, \ldots, n\}$ y sea $f_i \colon U \to K$, $f_i(u_j) = \delta_{ij}$. Como la función $U \times V \to V$, $(u,v) \mapsto f_i(u)v$, es bilineal, existe una función $\alpha_i \colon U \otimes V \to V$ lineal tal que $\alpha_i(u \otimes v) = f_i(u)v$. Luego

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

□

xca:uxv=0 **Exercise 5.31.** Demuestre que si $u \otimes v = 0$ y $v \neq 0$, entonces $u = 0$.

Theorem 5.32. *Si $\{u_i : i \in I\}$ es una base de U y $\{v_j : j \in J\}$ es una base de V, entonces $\{u_i \otimes v_j : i \in I, j \in J\}$ es una base de $U \otimes V$.*

Proof. Los $u_i \otimes v_j$ forman un conjunto de generadores pues si $u = \sum_i \lambda_i u_i$ y $v = \sum_j \mu_j v_j$, entonces $u \otimes v = \sum_{i,j} \lambda_i \mu_j u_i \otimes v_j$. Veamos ahora que los $u_i \otimes v_j$ son linealmente independientes. Para eso, queremos ver que cualquier subconjunto finito de los $u_i \otimes v_j$ es linealmente independiente. Si $\sum_k \sum_l \lambda_{kl} u_{i_k} \otimes v_{j_l} = 0$, entonces $0 = \sum_k u_{i_k} \otimes \left(\sum_l \lambda_{kl} v_{j_l} \right)$ y luego, como los u_{i_k} son linealmente indepentientes, el lema 5.30 implica que $\sum_l \lambda_{kl} v_{j_l} = 0$. Luego $\lambda_{kl} = 0$ para todo k, l pues los v_{j_l} son linealmente independientes. □

El teorema anterior implica inmediatamente que si U y V son espacios vectoriales de dimensión finita entonces

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

Corollary 5.33. *Si $\{u_i : i \in I\}$ es base de U, entonces todo elemento de $U \otimes V$ se escribe unívocamente como una suma finita $\sum_i u_i \otimes v_i$.*

Proof. Sabemos que todo elemento de $U \otimes V$ es una suma finita $\sum_i x_i \otimes y_i$, donde $x_i \in U$ y $y_i \in V$. Si escribimos $x_i = \sum_j \lambda_{ij} u_j$, entonces

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

□

El siguiente lema nos permite definir el **producto tensorial de álgebras**.

Lemma 5.34. *Si A y B son álgebras, entonces $A \otimes B$ es un álgebra con el producto*

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

Proof. Para $x \in A$, $y \in B$ consideramos $R_x \otimes R_y \in \mathrm{End}_K(A \otimes B)$. Como la función $A \times B \to \mathrm{End}_K(A \otimes B)$, $(x,y) \mapsto R_x \otimes R_y$, es bilineal, existe una función lineal $\varphi \colon A \otimes B \to \mathrm{End}_K(A \otimes B)$, $\varphi(x \otimes y) = R_x \otimes R_y$. Para $u, v \in A \otimes B$ definimos

$$uv = \varphi(v)(u).$$

Esta operación es bilineal pues por ejemplo

$$u(v+w) = \varphi(v+w)(u) = (\varphi(v) + \varphi(w))(u) = \varphi(v)(u) + \varphi(w)(u) = uv + uw.$$

Además $(a \otimes b)(x \otimes y) = \varphi(x \otimes y)(a \otimes b) = (R_x \otimes R_y)(a \otimes b) = ax \otimes by$. Un cálculo sencillo muestra que este producto es asociativo. □

Exercise 5.35. Demuestre que para álgebras valen las siguientes afirmaciones:

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) Si $A \otimes A'$ y $B \otimes B'$ entonces $A \otimes B \simeq A' \otimes B'$.

Veamos algunos ejemplos:

Proposition 5.36. *Si G y H son grupos, entonces $K[G] \otimes K[H] \simeq K[G \times H]$.*

Proof. Sabemos que $\{g \otimes h : g \in G, h \in H\}$ es una base de $K[G] \otimes K[H]$ y que $G \times H$ es una base de $K[G \times H]$. Tenemos entonces un isomorfismo lineal

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

que además es multiplicativo. Luego $K[G] \otimes K[H] \simeq K[G \times H]$ como álgebras. □

Proposition 5.37. *Si A es un álgebra, entonces $A \otimes K[X] \simeq A[X]$.*

Proof. Todo elemento de $A \otimes K[X]$ se escribe unívocamente como una suma finita de la forma $\sum a_i \otimes X^i$. Un cálculo sencillo muestra que $A \otimes K[X] \mapsto A[X]$, $\sum a_i \otimes X^i \mapsto \sum a_i X^i$, es un isomorfismo de álgebras. □

Exercise 5.38. Demuestre que si A es un álgebra, $A \otimes M_n(K) \simeq M_n(A)$. En particular, $M_n(K) \otimes M_m(K) \simeq M_{nm}(K)$.

Estos últimos dos ejemplos son casos particulares de una construcción importante que involucra productos tensoriales y se conoce como **extensión de escalares**.

Theorem 5.39. *Sea A un álgebra sobre K y sea E una extensión de K. Entonces $A^E = E \otimes_K A$ es un álgebra sobre E con respecto a la multiplicación por escalares dada por*

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

para $\lambda, \mu \in E$ y $a \in A$.

Proof. Sea $\lambda \in E$. Como la función $E \times A \to E \otimes_K A$, $(\mu, a) \mapsto (\lambda\mu) \otimes a$, es K-bilineal, existe una transformación lineal $E \otimes_K A \to E \otimes_K A$, $\mu \otimes a \mapsto (\lambda\mu) \otimes a$. Queda bien definida entonces la multiplicación por escalares y además

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

para $\lambda \in E$ y $u, v \in E \otimes_K A$. Un cálculo directo muestra que además

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

valen para todo $u, v \in E \otimes_K A$ y $\lambda, \mu \in E$. □

Exercise 5.40. Demuestre que valen las siguientes afirmaciones:

1) $1 \otimes A$ es una subálgebra de A^E isomorfa a A.
2) Si $\{a_i : i \in I\}$ es base de A, entonces $\{1 \otimes a_i : i \in I\}$ es base de A^E.

Exercise 5.41. Demuestre que si G es un grupo y K es un subcuerpo de E, entonces $E \otimes_K K[G] \simeq E[G]$.

Estamos en condiciones de demostrar el teorema de Formanek:

Theorem 5.42 (Formanek). *Sea K un cuerpo de característica cero y sea G un grupo. Si todo elemento de $K[G]$ es inversible o un divisor de cero, entonces G es localmente finito.*

Proof. Como K es de característica cero, $\mathbb{Q} \subseteq K$ y $K[G] \simeq K \otimes_{\mathbb{Q}} \mathbb{Q}[G]$. Todo $\beta \in K \otimes_{\mathbb{Q}} \mathbb{Q}[Q]$ se escribe unívocamente como

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

donde $\{1, k_1, k_2, \ldots,\}$ es una base de K como $\mathbb{Q}$-espacio vectorial. Sea $\alpha \in \mathbb{Q}[G]$ y sea $\beta \in K[G]$ tal que $\alpha\beta = 1$. Como entonces

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

la unicidad de la escritura nos dice que $\alpha\beta_0 = 1$. De la misma forma, si $\alpha\beta = 0$, entonces $\alpha\beta_j = 0$ para todo j. Luego, como todo $\alpha \in \mathbb{Q}[G]$ es inversible o un divisor de cero, el resultado se obtiene al usar el teorema 5.21 de Formanek para $\mathbb{Q}$. □

Lecture 5

Rickart's theorem

En esta sección vamos a demostrar que para cualquier grupo G el radical de Jacobson de $\mathbb{C}[G]$ es cero. Demostraremos también que el radical de Jacobson de $\mathbb{R}[G]$ es cero.

Definition 5.43. Sea R un anillo. Una **involución** del anillo R es un morfismo aditivo $R \to R$, $x \mapsto x^*$, tal que $x^{**} = x$ y $(xy)^* = y^*x^*$ para todo $x, y \in R$.

De la definición se deduce inmediatamente que si R es unitario, entonces $1^* = 1$.

Example 5.44. La conjugación $z \mapsto \overline{z}$ es una involución de $\mathbb{C}$.

Example 5.45. La trasposición $X \mapsto X^T$ es una involución del anillo $M_n(K)$.

Example 5.46. Sea G un grupo. Entonces $\left(\sum_{g\in G} \alpha_g g\right)^* = \sum_{g\in G} \overline{\alpha_g} g^{-1}$ es una involución de $\mathbb{C}[G]$.

Dado un grupo G, se define la **traza** de un elemento $\alpha = \sum_{g\in G} \alpha_g g \in K[G]$ como $\operatorname{traza}(\alpha) = \alpha_1$. Es fácil ver que $\operatorname{traza}\colon K[G] \to K$, $\alpha \mapsto \operatorname{traza}(\alpha)$ es una función K-lineal tal que $\operatorname{traza}(\alpha\beta) = \operatorname{traza}(\beta\alpha)$.

Exercise 5.47. Sea G un grupo finito y K un cuerpo tal que su característica no divide al orden de G. Demuestre las siguientes afirmaciones:

1) Si $\alpha \in K[G]$ es nilpotente, entonces $\operatorname{traza}(\alpha) = 0$.
2) Si $\alpha \in K[G]$ es idempotente, entonces $\operatorname{traza}(\alpha) = \dim K[G]\alpha/|G|$.

Exercise 5.48. Demuestre que $\langle \alpha, \beta \rangle = \operatorname{traza}(\alpha\beta^*)$, $\alpha, \beta \in \mathbb{C}[G]$, define un producto interno en $\mathbb{C}[G]$.

lem:algebraico

Lemma 5.49. *Sea G un grupo. Si $J(\mathbb{C}[G]) \neq 0$, entonces existe $\alpha \in J(\mathbb{C}[G])$ tal que $\operatorname{traza}(\alpha^{2^m}) \in \mathbb{R}_{\geq 1}$ para todo $m \geq 1$.*

Proof. Sea $\alpha = \sum_{g\in G} \alpha_g g \in \mathbb{C}[G]$. Entonces

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

Al usar esta fórmula para algún α tal que $\alpha^* = \alpha$ y usar inducción se obtiene que $\operatorname{traza}(\alpha^{2^m}) \geq |\operatorname{traza}(\alpha)|^{2^m}$ para todo $m \geq 1$.

Sea $\beta = \sum_{g\in G} \beta_g g \in J(\mathbb{C}[G])$ tal que $\beta \neq 0$. Como $\operatorname{traza}(\beta^*\beta) = \sum_{g\in G} |\beta_g|^2 \neq 0$ y $J(\mathbb{C}[G])$ es un ideal,

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

Este elemento α cumple que $\alpha^* = \alpha$ y $\operatorname{traza}(\alpha) = 1$. Luego $\operatorname{traza}(\alpha^{2^m}) \geq 1$ para todo $m \geq 1$. □

El ejercicio 5.20 implica que $\mathbb{C}[G]$ con $\operatorname{dist}(\alpha,\beta) = |\alpha - \beta|$ es un espacio métrico. En este espacio métrico, la función $\mathbb{C}[G] \to \mathbb{C}$, $\alpha \mapsto \operatorname{traza}(\alpha)$, es una función continua.

lem:phi_diferenciable

Lemma 5.50. *Sea $\alpha \in J(\mathbb{C}[G])$. La función*

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

es continua, diferenciable y $\varphi(z) = \sum_{n\geq 0} \alpha^n z^n \in \mathbb{C}[G]$ si $|z|$ es suficientemente pequeño.

Proof. Sean $y, z \in \mathbb{C}$. Como $\varphi(y)$ y $\varphi(z)$ conmutan,

$$\begin{aligned} \varphi(y) - \varphi(z) &= ((1 - z\alpha) - (1 - y\alpha))\,(1 - y\alpha)^{-1}(1 - z\alpha)^{-1} \\ &= (y - z)\alpha\varphi(y)\varphi(z). \end{aligned} \tag{5.2}$$

eq:Rickart

Entonces $|\varphi(y)| \leq |\varphi(z)| + |y - z||\alpha\varphi(y)||\varphi(z)|$ y luego

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

Fijado z podemos elegir y suficientemente cerca de z de forma tal que se cumpla que $1 - |y - z||\alpha\varphi(z)| \geq 1/2$. Luego $|\varphi(y)| \leq 2|\varphi(z)|$. De la igualdad (5.2) se obtiene entonces $|\varphi(y) - \varphi(z)| \leq 2|y - z||\alpha||\varphi(z)|^2$ y luego φ es una función continua. Por la expresión (5.2),

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

para todo $z \in \mathbb{C}$.

Si z es tal que $|z||\alpha| = |z\alpha| < 1$, entonces

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

y luego

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

Como $\varphi(z)$ está acotada cerca de $z = 0$, se concluye que $\left|\varphi(z) - \sum_{n=0}^{N} z^n\alpha^n\right| \to 0$ si $N \to \infty$. □

Estamos en condiciones de demostrar el teorema de Rickart:

Theorem 5.51 (Rickart). *Si G es un grupo, entonces $J(\mathbb{C}[G]) = 0$.*

Proof. Sea $\alpha \in J(\mathbb{C}[G])$ y sea $\varphi(z) = (1 - \alpha z)^{-1}$. Sea $f\colon \mathbb{C} \to \mathbb{C}$ dada por $f(z) = \operatorname{traza}\varphi(z) = \operatorname{traza}\left((1 - z\alpha)^{-1}\right)$. Por el lema 5.50, $f(z)$ es una función entera tal que $f'(z) = \operatorname{traza}(\alpha\varphi(z)^2)$ y

$$f(z) = \sum_{n=0}^{\infty} z^n \operatorname{traza}(\alpha^n) \tag{5.3}$$ eq:Taylor

si $|z|$ es suficientemente pequeño. En particular, la igualdad (5.3) es la expansión en serie de Taylor para $f(z)$ en el origen. Esto implica que esta serie tiene radio de convergencia infinito y converge a $f(z)$ para todo $z \in \mathbb{C}$. En particular,

$$\lim_{n\to\infty} \operatorname{traza}(\alpha^n) = 0. \tag{5.4}$$ eq:limite

Por otro lado, si $\alpha \neq 0$ el lema 5.49 implica que $\operatorname{traza}(\alpha^{2^m}) \geq 1$ para todo $m \geq 0$, lo que contradice el límite calculado en (5.4). Luego $\alpha = 0$. □

Para demostrar un corolario necesitamos dos lemas:

lem:Nakayama **Lemma 5.52 (Nakayama).** *Sea R un anillo unitario y sea M un R-módulo finitamente generado. Si $J(R)M = M$, entonces $M = 0$.*

Proof. Supongamos que M está generado por los elementos $x_1, \ldots, x_n$. Como $x_n \in M = J(R)M$, existen $r_1, \ldots, r_n \in J(R)$ tales que $x_n = r_1x_1 + \cdots + r_nx_n$, es decir $(1 - r_n)x_n = \sum_{j=1}^{n-1} r_jx_j$. Como $1 - r_n$ es inversible, existe $s \in R$ tal que $s(1 - r_n) = 1$. Luego $x_n = \sum_{j=1}^{n-1} sr_jx_j$ y entonces M está generado por $x_1, \ldots, x_{n-1}$. Al repetir este procedimiento una cierta cantidad finita de veces, se obtiene que $M = 0$. □

lem:Rickart **Lemma 5.53.** *Sea $\iota : R \to S$ un morfismo de anillos unitarios. Si*

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

donde cada x_j cumple que $x_jy = yx_j$ para todo $y \in \iota(R)$, entonces $\iota(J(R)) \subseteq J(S)$.

Proof. Veamos que $J = \iota(J(R))$ actúa trivialmente en cada S-módulo simple M. Si M es un S-módulo simple, escribimos $M = Sm$ para algún $m \neq 0$. Es claro que M es un R-módulo con $r \cdot m = \iota(r)m$. Como

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

M es finitamente generado como $\iota(R)$-módulo. Además $J(R) \cdot M = JM = \iota(J)M$ es un S-submódulo de M pues

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

Como $M \neq 0$, el lema de Nakayama implica que $J(R) \cdot M \subsetneq M$. Luego, como M es un S-módulo simple, se concluye que $J(R)M = 0$. □

Corollary 5.54. *Si G es un grupo, entonces $J(\mathbb{R}[G]) = 0$.*

Proof. Sea $\iota : \mathbb{R}[G] \to \mathbb{C}[G]$ la inclusión canónica. Como

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

el lema 5.53 y el teorema de Rickart implican que $\iota(J(\mathbb{R}[G])) \subseteq J(\mathbb{C}[G]) = 0$. Luego $J(\mathbb{R}[G]) = 0$ pues ι es inyectiva. □

Lecture 6

Definition 6.1. Sea R un anillo. Un R-módulo N se dice **artiniano** si para toda sucesión $N_1 \supseteq N_2 \supseteq \cdots$ de submódulos de N existe $n \in \mathbb{N}$ tal que $N_n = N_{n+k}$ para todo $k \in \mathbb{N}$.

Definition 6.2. Sea R un anillo. Un R-módulo N se dice **noetheriano** si para toda sucesión $N_1 \subseteq N_2 \subseteq \cdots$ de submódulos de N existe $n \in \mathbb{N}$ tal que $N_n = N_{n+k}$ para todo $k \in \mathbb{N}$.

Sea X un conjunto y sea $\mathscr{S}$ un conjunto de subconjuntos de X. Diremos que $A \in \mathscr{S}$ es un **elemento minimal** en $\mathscr{S}$ si no existe $Y \in \mathscr{S}$ tal que $Y \subsetneq A$. Similarmente, que $B \in \mathscr{S}$ es un **elemento maximal** en $\mathscr{S}$ si no existe $Z \in \mathscr{S}$ tal que $B \subsetneq Z$.

lem:modulo_artiniano

Lemma 6.3. *Un módulo N es artiniano si y sólo si todo conjunto no vacío de submódulos de N tiene un elemento minimal.*

Proof. Supongamos que N es artiniano y que . Sea $\mathscr{S}$ el conjunto (no vacío) de submódulos de N. Supongamos que $\mathscr{S}$ no tiene elemento minimal y sea $N_1 \in \mathscr{S}$. Como N_1 no es minimal, existe $N_2 \in \mathscr{S}$ tal que $N_1 \supsetneq N_2$. Supongamos que tenemos elegidos k submódulos $N_1 \supsetneq N_2 \supseteq \cdots \supsetneq N_k$. Como N_k no es minimal, existe N_{k+1} tal que $N_k \supsetneq N_{k+1}$. De esta forma tenemos una sucesión de submódulos $N_1 \supsetneq N_2 \supsetneq \cdots$ que no se estabiliza, una contradicción.

Recíprocamente, si $N_1 \supseteq N_2 \supseteq \cdots$ es una sucesión de submódulos, entonces el conjunto $\mathscr{S} = \{N_j : j \geq 1\}$ tiene un elemento minimal N_n. Luego $N_n = N_{n+k}$ para todo $k \in \mathbb{N}$. □

lem:noetheriano1

Lemma 6.4. *Un módulo N es noetheriano si y sólo si todo conjunto no vacío de submódulos de N tiene un elemento maximal.*

Proof. Es similar a la prueba del lema 6.3. □

lem:noetheriano2

Lemma 6.5. *Un módulo N es noetheriano si y sólo si todo submódulo de N es finitamente generado.*

Proof. Supongamos que N es noetheriano. Sea P un submódulo de N y sea $\mathscr{S}$ el conjunto de submódulos de P finitamente generados. Como $0 \in \mathscr{S}$, el conjunto $\mathscr{S}$ es no vacío. Por el lema 6.4, existe $B \in \mathscr{S}$ elemento maximal. Sea $\{b_1, \ldots, b_m\}$ un conjunto finito de generadores de B. Si $p \in P$ entonces, por maximalidad, B está contenido en el submódulo de P generado por $\{p, b_1, \ldots, b_m\}$. Como este submódulo está en $\mathscr{S}$, se concluye que $p \in B$.

Sea $N_1 \subseteq N_2 \subseteq \cdots$ una subcesión de submódulos de N. Como $M = \cup_{j \geq 1} N_j$ es un submódulo de N, es finitamente generado. Sea $\{x_1, \ldots, x_m\}$ un conjunto de generadores de M. Como cada x_j está en algún N_k, existe $n \in \mathbb{N}$ tal que $M \subseteq N_n$. En particular, $N_n = N_{n+k}$ para todo $k \geq 1$. □

ercise:noetheriano:exact

Exercise 6.6. Sea

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

una sucesión exacta de R-módulos. Demuestre que B es noetheriano (resp. artiniano) si y sólo si A y C son noetherianos (resp. artinianos).

Definition 6.7. Un anillo R se dice **noetheriano a izquierda** si el módulo ${}_R R$ es noetheriano.

Análogamente se definen anillos noetherianos a derecha.

Definition 6.8. Un anillo R se dice **artiniano a izquierda** si el módulo ${}_R R$ es artiniano.

Análogamente se definen anillos artinianos a derecha.

Example 6.9. Del lema 6.5 se obtiene inmediatamente que $\mathbb{Z}$ es noetheriano. Sin embargo, $\mathbb{Z}$ no es noetheriano pues $2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq \cdots$ es una sucesión de ideales que no se estabiliza.

def:serie_de_composicion

Definition 6.10. Una **serie de composición** para un módulo M es una sucesión

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

de submódulos de M tal que cada M_i/M_{i-1} es no nulo y no tiene submódulos propios. En este caso, n es la longitud de M y M se dice de **longitud finita**.

La definición 6.10 tiene sentido también en anillos no unitarios, y por eso pedimos que cada cociente M_i/M_{i-1} no tenga submódulos propios (esto garantiza la simplicidad en el caso de anillos unitarios).

thm:serie_de_composicion

Theorem 6.11. *Un módulo no nulo admite una serie de composición si y sólo si es artiniano y noetheriano.*

Proof. Sea M un módulo no nulo y sea $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ una serie de composición para M. Demostraremos por inducción que cada M_i es artiniano y

noetheriano. El caso $i = 0$ es trivial. Supongamos entonces que M_i es artinoano y noetheriano. Como M_i/M_{i+1} no tiene submódulos propios y la sucesión

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

es exacta, se concluye que M_{i+1} es artiniano y noetheriano.

Supongamos ahora que M es un módulo noetheriano y artiniano. Sea $M_0 = 0$ y sea M_1 minimal entre los submódulos de M (existe M_1 gracias al lema 6.3 pues M es artiniano). Si $M_1 \neq M$, sea M_2 minimal entre los submódulos de M tales que $M_1 \subsetneq M_2$. Al continuar de esta forma obtenemos una sucesión

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

de submódulos de M, donde cada M_{i+1}/M_i es no nulo y no admite submódulos propios. Como M es noetheriano, la sucesión se estabiliza y luego $M_n = M$ para algún n. □

Definition 6.12. Diremos que las series de composición

$$V = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_k = 0, \quad V = W_0 \supseteq W_1 \supseteq \cdots \supseteq W_l = 0,$$

son **equivalentes** si $k = l$ y además existe una permutación $\sigma \in \mathbb{S}_n$ tal que para todo $i \in \{1, \ldots, k\}$ se tiene $V_i/V_{i-1} \simeq W_{\sigma(i)}/W_{\sigma(i)-1}$.

thm:JordanHolder

Theorem 6.13 (Jordan–Hölder). *Sea V un módulo y sean*

$$V = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_k = 0, \quad V = W_0 \supseteq W_1 \supseteq \cdots \supseteq W_l = 0,$$

dos series de composición para V. Entonces las series son equivalentes.

Proof. Procederemos por inducción en k. El caso $k = 1$ es trivial pues en este caso V no tiene submódulos propios y luego $V \supseteq 0$ es la única serie de composición. Supongamos entonces que el resultado vale para módulos con series de composición de longitud $< k$. Si $V_1 = W_1$ entonces V_1 tiene dos series de composición de longitudes $k-1$ y $l-1$. Por hipótesis inductiva, $k = l$ y el teorema queda demostrado. Supongamos entonces que $V_1 \neq W_1$. Como V_1 y W_1 son submódulos de V, la suma $V_1 + W_1$ es un submódulo de V. Además, como V/V_1 no tiene submódulos propios no nulos, $V_1 + W_1 = V$. Sea $U = V_1 \cap W_1$. Entonces

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

Como V_1 tiene una serie de composición, V_1 es artiniano y noetheriano por el teorema 6.11. Entonces también U es artiniano y noetheriano, y luego tiene una serie de composición por el teorema 6.11, digamos

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

Tenemos entonces que $V_1 \supseteq \cdots \supseteq V_k = 0$ y $V_1 \supseteq U \supseteq U_1 \supseteq \cdots \supseteq U_r = 0$ son series de composición para V_1. Por hipótesis inductiva, $k-1 = r+1$ y las series de composición son equivalentes. Similarmente,

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

son series de composición para W_1 y entonces $l-1 = r+1$ y las series son equivalentes. Luego $l = k$ y el teorema queda demostrado. □

Definition 6.14. Si M es un módulo que admite una serie de composición, digamos $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$, se define la **longitud** de M como el entero $c(M) = n$.

Exercise 6.15. Si N y Q son módulos de longitud finita y

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

es una sucesión exacta de módulos, entonces $c(M) = c(N) + C(Q)$.

Exercise 6.16. Sean A y B submódulos de M de longitud finita. Demuestre que entonces $c(A+B) + c(A \cap B) = c(A) + C(B)$.

Lemma 6.17. *Sea R un anillo unitario y M un módulo unitario semisimple. Son equivalentes:*

1) *M es noetheriano.*
2) *M es artiniano.*
3) *M es suma directa de finitos simples.*

Proof. Veamos ahora que $(3) \iff (1)$ y que $(3) \iff (2)$. Como cada submódulo simple es artiniano y noetheriano, M resulta artiniano y noetheriano. Recíprocamente, si M es artiniano, I debe ser finito pues de lo contrario podríamos elegir elementos $i_1, i_2, i_3, \ldots$ de I tales que la sucesión

$$\bigoplus_{i \in I} M_i \supsetneq \bigoplus_{i \in I \setminus \{i_1\}} M_i \supsetneq \bigoplus_{i \in I \setminus \{i_1, i_2\}} M_i \supsetneq \cdots$$

nunca se estabiliza. Análogamente, si M es noetheriano, podríamos elegir elementos $i_1, i_2, i_3, \cdots \in I$ tales que la sucesión

$$M_{i_1} \subsetneq M_{i_1} \oplus M_{i_2} \subsetneq \cdots$$

nunca se estabiliza. □

Veremos ahora la relación existente entre la semisimplicidad y el radical de Jacobson. Primero necesitamos un lema:

lem:Jartiniano

Lemma 6.18. *Sea R un anillo unitario y artiniano a izquierda. Entonces existen finitos ideales maximales $I_1, \ldots, I_n$ de R tales que $J(R) = I_1 \cap \cdots \cap I_n$.*

Proof. Como R es unitario, $J(R)$ es la intersección de ideales maximales de R. Como R es artiniano a izquierda, el lema 6.3 nos dice que el conjunto de ideales formados por la intersección de finitos ideales maximales $I_1, \ldots, I_k$ de R posee un elemento minimal, digamos $J = \bigcap_{i=1}^{k} I_i$. Veamos que $J = J(R)$. Si no, sea $x \in J(R) \setminus J$. Existe entonces un ideal maximal M tal que $x \notin M$. Pero entonces $J \cap M \subsetneq J$, una contradicción a la minimalidad de J. □

thm:SSartin=J

Theorem 6.19. *Si R es un anillo unitario, entonces R es semisimple si y sólo si R es artiniano a izquierda y $J(R) = 0$.*

Proof. Supongamos primero que R es semisimple. Por el teorema de Wedderburn, existen enteros positivos $n_1, \ldots, n_k$ y anillos de división $D_1, \ldots, D_k$ tales que

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

En particular, R es artiniano a izquierda y $J(R) = \prod_{i=1}^{k} J(M_{n_i}(D_i)) = 0$ pues cada $M_{n_i}(D_i)$ es simple.

Recíprocamente, por el lema anterior sabemos que $0 = J(R) = I_1 \cap \cdots \cap I_k$ para finitos ideales maximales $I_1, \ldots, I_k$. Como cada cociente R/I_i es simple, $\prod_{i=1}^{k} R/M_i$ es semisimple. Como $I_1 \cap \cdots \cap I_k = 0$, el morfismo $R \to \prod_{i=1}^{k} R/M_i$ es inyectivo y luego R es también semisimple. □

Como consecuencia tenemos el siguiente resultado:

Proposition 6.20. *Sea G un grupo. Entonces $\mathbb{C}[G]$ es artiniana a izquierda si y sólo si G es finito.*

Proof. Si G es finito sabemos que $\mathbb{C}[G]$ es artiniano a izquierda por ser de dimensión finita. Recíprocamente, si G es infinito, sabemos que $J(\mathbb{C}[G]) = 0$ (por el teorema de Rickart) y que $\mathbb{C}[G]$ no es semisimple (por la proposición **??**). Luego $\mathbb{C}[G]$ no es artiniana a izquierda por el teorema 6.19. □

Concluimos la sección con el siguiente teorema:

thm:Hopkins-Levitski

Theorem 6.21 (Hopkins–Levitszki). *Si R es un anillo unitario artiniano a izquierda, entonces R es noetheriano a izquierda.*

Proof. Sea $J = J(R)$. Como R es artiniano a izquierda, J es un ideal nilpotente por el teorema 4.12, digamos $J^n = 0$. Consideremos la sucesión

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

Cada J^i/J^{i+1} es un R-módulo anulado por J. Luego cada J^i/J^{i+1} es un (R/J)-módulo. Como R/J es artiniano (pues R lo es) y $J(R) = 0$, R/J es semisimple. Luego cada J^i/J^{i+1} es semisimple y entonces es noetheriano a izquierda. Inductivamente se demuestra entonces que cada J^i es noetheriano a izquierda y luego R también lo es. □

Definition 6.22. Un anillo R se dice **semiprimitivo** (o semisimple Jacobson) si $J(R) = 0$.

Example 6.23. Si R es primitivo entonces es semiprimitivo. En efecto, como R es primitivo, $\{0\}$ es un ideal primitivo y luego, como $J(R)$ es la intersección de los ideales primitivos de R, se concluye que $J(R) = 0$.

Example 6.24. Si $R = \prod_{i\in I} R_i$ es producto directo de anillos semiprimitivos, entonces R es semiprimitivo pues

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

Example 6.25. $\mathbb{Z}$ es semiprimitivo pues $J(\mathbb{Z}) = \cap_p \mathbb{Z}/p = \{0\}$.

Example 6.26. Sea $R = C[a,b]$ el anillo de funciones $f\colon [a,b] \to \mathbb{R}$ continuas. Como R es un anillo unitario, $J(R)$ es la intersección de los ideales maximales de R. Todo ideal maximal de R es de la forma

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

para algún $c \in [a,b]$. En efecto, es fácil ver que cada U_c es un ideal; U_c es maximal pues $C[a,b]/U_c \simeq \mathbb{R}$. Luego $J(R) = \cap_{a\le c\le b} U_c = 0$.

thm:semiprimitivo **Theorem 6.27.** *Si R es un anillo, entonces $R/J(R)$ es semiprimitivo.*

Proof. Si R es un anillo radical, el resultado es trivial. Supongamos entonces que $J(R) \neq R$ y sea M un módulo simple. Entonces M es un $R/J(R)$-módulo simple con

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

Si $x + J(R) \in J(R/J(R))$ entonces $xM = (x + J(R))M = 0$. Luego $x \in J(R)$ pues x anula a cualquier módulo simple de R. □

Definition 6.28. Sea $\{R_i : i \in I\}$ una familia de anillos. Un subanillo R de $\prod_{i\in I} R_i$ se dice un **producto subdirecto** de los R_j si cada $\pi_j\colon R \to R_j$ es sobreyectiva.

El siguiente teorema justifica que indistintamente llamemos anillos semiprimitivos a los anillos semisimples Jacobson:

thm:subdirecto **Theorem 6.29.** *Sea R un anillo no nulo. Entonces R semiprimitivo si y sólo si R es isomorfo a un producto subdirecto de anillos primitivos.*

Proof. Supongamos que R es semiprimitivo y sea $\{P_i : i \in I\}$ la familia de ideales primitivos de R. Cada R/P_j es primitivo y $\{0\} = J(R) = \cap_{i\in I} P_i$. Para cada j, sean $\lambda_j\colon R \to R/P_j$ y $\pi_j\colon \prod_{i\in I} R/P_i \to R/P_j$ los morfismos canónicos. La función

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

es un morfismo inyectivo de anillos tal que $\pi_j\phi(R) = R/P_j$ para todo j.

Supongamos ahora que R es isomorfo a un producto subrirecto de anillos R_j primitivos y sea $\varphi\colon R \to \prod_{i\in I} R_i$ un morfismo inyectivo tal que $\pi_j(\varphi(R)) = R_j$ para todo j. Para cada j sea $P_j = \ker \pi_j\varphi$. Como $R/P_j \simeq R_j$, cada P_j es un ideal primitivo. Si $x \in \cap_{i\in I} P_i$ entonces $\varphi(x) = 0$ y luego $x = 0$. Luego $J(R) \subseteq \cap_{i\in I} P_i = 0$. □

Example 6.30. El anillo $\mathbb{Z}$ es isomorfo a un producto subdirecto de los cuerpos $\mathbb{Z}/p$ con p primo.

Example 6.31. El anillo $C[a,b]$ es isomorfo a un producto subdirecto de los cuerpos $C[a,b]/U_c \simeq \mathbb{R}$.

Definition 6.32. Un anillo R se dice **semiprimo** si para todo $a \in R$ tal que $aRa = 0$ se tiene que $a = 0$.

Lemma 6.33. *Sea R un anillo. Son equivalentes:*

1) *R es semiprimo.*
2) *Si I es un ideal a izquierda tal que $I^2 = 0$ entonces $I = 0$.*
3) *Si I es un ideal tal que $I^2 = 0$ entonces $I = 0$.*
4) *R no tiene ideales nilpotentes no nulos.*

Proof. Veamos que $(1) \implies (2)$. Si $I^2 = 0$ y $x \in I$, entonces $xRx \subseteq I^2 = 0$ y luego $x = 0$. Las implicaciones $(2) \implies (3)$ y $(4) \implies (3)$ son triviales. Veamos que $(3) \implies (4)$. Si I es un ideal nilpotente no nulo, sea $n \in \mathbb{N}$ minimal tal que $I^n = 0$. Como $(I^{n-1})^2 = 0$, $I^{n-1} = 0$, una contradicción. Por último veamos que $(3) \implies (1)$. Sea $a \in R$ tal que $aRa = 0$. Entonces $I = RaR$ es un ideal de R tal que $I^2 = 0$. Por hipótesis, $RaR = I = 0$. Luego Ra y aR son ideales tales que $(Ra)R = R(aR) = 0$. Esto implica que $\mathbb{Z}a$ es un ideal de R tal que $(\mathbb{Z}a)R = 0$ y luego $a = 0$. □

Example 6.34. Un anillo conmutativo es semiprimo si y sólo si no tiene elementos nilpotentes no nulos.

Proposition 6.35. *El anillo $\mathbb{C}[G]$ es semiprimo.*

Proof. Como $J(\mathbb{C}[G]) = 0$ por el teorema de Rickart y además el radical de Jacboson contiene a todo ideal nil por la proposición 3.39, se deduce que $\mathbb{C}[G]$ no tiene ideales nil no triviales. Tampoco tiene entonces ideales nilpotentes no triviales y luego $\mathbb{C}[G]$ es semiprimo. □

Exercise 6.36. Demuestre que $Z(\mathbb{C}[G])$ es semiprimo.

Example 6.37. Sea D un anillo de división. Entonces $D[X]$ es semiprimo.

Example 6.38. Sea D un anillo de división. Entonces $D[[X]]$ es semiprimo y no es semiprimitivo.

Lecture 7

Definition 7.1. Sean D un anillo de división y V un espacio vectorial sobre D. Un subanillo $R \subseteq \mathrm{End}_D(V)$ se dice **denso** en V si para cada $n \in \mathbb{N}$, cada $\{u_1, \ldots, u_n\} \subseteq V$ linealmente independiente de V y cada conjunto $\{v_1, \ldots, v_n\} \subseteq V$ (no necesariamente linealmente independiente) existe $f \in R$ tal que $f(u_j) = v_j$ para todo $j \in \{1, \ldots, n\}$.

lem:unico_denso

Lemma 7.2. *Sea D un anillo de división V un D-espacio vectorial de dimensión finita. Entonces $\mathrm{End}_D(V)$ es el único anillo denso en V.*

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

lem:ideal_denso

Lemma 7.3. *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 $\{u_1, \ldots, u_n\} \subseteq V$ un conjunto linealmente independiente y sea $\{v_1, \ldots, v_n\} \subseteq V$. Como R es denso en V, existen $g_1, \ldots, g_n \in R$ tales que $g_i(u_i) = u$ y $g_i(u_j) = 0$ si $i \neq j$. Existen además $f_1, \ldots, f_n \in R$ 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 $j \in \{1, \ldots, n\}$. □

thm:densidad

Theorem 7.4 (densidad de Jacobson). *Un anillo R es primitivo si y sólo si es isomorfo a un anillo denso en un espacio vectorial sobre un anillo de división.*

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 $f \in \mathrm{Ann}_R(V)$ 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, $D = \mathrm{End}_R(V)$ 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 $\gamma_r \in \mathrm{End}_D(V)$ y que la función $R \to \mathrm{End}_D(V)$, $r \mapsto \gamma_r$, 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 $u_1, \ldots, u_n \in V$ vectores linealmente independientes y sean $v_1, \ldots, v_n \in V$ vectores arbitrarios. Si fijamos $i \in \{1, \ldots, n\}$, 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 $i \in \{1, \dots, n\}$. □

Corollary 7.5. *Si R es un anillo primitivo, entonces existe un anillo de división D tal que $R \simeq \mathrm{End}_D(V)$ para algún D-espacio vectorial V de dimensión finita, o bien para todo $m \in \mathbb{N}$ existe un subanillo R_m de R y un morfismo de anillos sobreyectivo $R_m \to \mathrm{End}_D(V_m)$ 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 7.4 podemos suponer que existe un anillo de división D tal que R es denso en un D-espacio vectorial V. Sea $\gamma\colon R \to \mathrm{End}_D(V)$, $r \mapsto \gamma_r$, 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 7.2. Supongamos entonces que V es de dimensión infinita y sea $\{u_1, u_2, \dots\}$ un conjunto linealmente independiente. Para cada $m \in \mathbb{N}$ 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 7.6. 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 7.7. 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 7.8. Un anillo conmutativo es primo si y sólo si es un dominio pues $ab = 0$ si y sólo si $aRb = 0$.

Example 7.9. Un ideal no nulo de un anillo primo es un anillo primo.

Lemma 7.10. *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 7.11. 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 7.12. 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 7.13. *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 7.14. *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 $R \subseteq \mathrm{End}_D(V)$, V es un R-módulo con $f \cdot v = f(v)$, donde $f \in R$ y $v \in V$. Para cada $n \in \mathbb{N}$ sea

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

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 $n \in \mathbb{N}$ 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 7.15 (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 $n \in \mathbb{N}$ 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 7.13, 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 7.14 implica que $R = \mathrm{End}_D(V) \simeq M_n(D)$ 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 7.16. *Sea D un anillo de división. Entonces*

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

Proof. Sea

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

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

$$\phi(d_1 \cdot_{\mathrm{op}} d_2)(x) = \phi(d_2 d_1)(x) = x(d_2 d_1) = (xd_2)d_1 = \phi(d_1)\phi(d_2)(x).$$

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 $f \in \mathrm{End}_{M_n(D)}(D^n)$ 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 7.17. *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 7.18. *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 3.11), el lema 7.17 implica que

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

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

Una pregunta surge naturalmente: ¿Cuándo el anillo de grupo $K[G]$ es primo? Obtendremos una respuesta completa en el caso en que K sea un cuerpo de característica cero.

Si S es un subconjunto finito de un grupo G se define $\widehat{S} = \sum_{x \in S} x$.

lemma:sumN

Lemma 7.19. *Sea N un subgrupo normal finito de G. Entonces $\widehat{N}$ es central en $K[G]$ y además $\widehat{N}(\widehat{N} - |N|1) = 0$.*

Proof. Supongamos que $N = \{n_1, \ldots, n_k\}$ y sea $g \in G$. Como la función $N \to N$, $n \mapsto gng^{-1}$, es una biyección,

$$g\widehat{N}g^{-1} = g(n_1 + \cdots + n_k)g^{-1} = gn_1g^{-1} + \cdots + gn_kg^{-1} = \widehat{N}.$$

Como $nN = N$ si $n \in N$, se tiene que $n\widehat{N} = \widehat{N}$. Luego $\widehat{N}\widehat{N} = \sum_{j=1}^{k} n_j\widehat{N} = |N|\widehat{N}$. □

Necesitamos el siguiente teorema:

theorem:Dietzmann

Theorem 7.20 (Dietzmann). *Sea G un grupo y sea $X \subseteq G$ un subconjunto finito de G cerrado por conjugación. Si existe $n \in \mathbb{N}$ tal que $x^n = 1$ para todo $x \in X$, entonces $\langle X \rangle$ es un subgrupo finito de G.*

Proof. Sea $S = \langle X \rangle$. Como $x^{-1} = x^{n-1}$, todo elemento de S puede escribirse como producto (finito) de elementos de X.

Fijemos $x \in X$. Vamos a demostrar que si $x \in X$ aparece $k \geq 1$ veces en la representación de una palabra s, podemos escribir a s como producto de m elementos de X donde los primeros k son iguales a x. Supongamos que

$$s = x_1x_2 \cdots x_{t-1}xx_{t+1} \cdots x_m,$$

donde cada $x_j \neq x$ para todo $j \in \{1, \ldots, t-1\}$. Entonces

$$s = x(x^{-1}x_1x)(x^{-1}x_2x) \cdots (x^{-1}x_{t-1}x)x_{t+1} \cdots x_m$$

es producto de m elementos de X pues X es cerrado por conjugación, y el primer elemento es nuestro x. Este mismo argumento implica que s puede escribirse como

$$s = x^k y_{k+1} \cdots y_m,$$

donde los y_j son elementos de $X \setminus \{x\}$.

Sea ahora $s \in S$ y escribamos a s como producto de m elementos de X, donde m es el mínimo posible. Para ver que S es finito basta ver que $m \leq (n-1)|X|$.

Si suponemos que $m > (n-1)|X|$, al menos un $x \in X$ aparecería n veces en la representación de s. Sin pérdida de generalidad, podríamos escribir

$$s = x^n x_{n+1} \cdots x_m = x_{n+1} \cdots x_m,$$

una contradicción a la minimalidad de m. □

Antes de seguir hacia nuestro objetivo demostraremos un teorema de Schur:

thm:Schur **Theorem 7.21 (Schur).** *Si $Z(G)$ tiene índice finito en G entonces $[G,G]$ es finito.*

Proof. Supongamos que $(G : Z(G)) = n$. Sea X el conjunto de conmutadores de G. El conjunto X es finito pues como la función

$$\varphi \colon X \to G/Z(G) \times G/Z(G), \quad [x,y] \mapsto (xZ(G), yZ(G)),$$

es inyectiva, se tiene que $|X| \leq n^2$. Para ver que φ es inyectiva supongamos que $(xZ(G), yZ(G)) = (uZ(G), vZ(G))$. Entonces $u^{-1}x \in Z(G)$, $v^{-1}y \in Z(G)$ y luego

$$[u,v] = uvu^{-1}v^{-1} = uv(u^{-1}x)x^{-1}v^{-1} = xvx^{-1}(v^{-1}y)y^{-1} = xyx^{-1}y^{-1} = [x,y].$$

Además X es cerrado por conjugación pues

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

para todo $g,x,y \in G$. Como $g \mapsto g^n$ es un morfismo de grupos $G \to Z(G)$, lema **??** implica que $[x,y]^n = [x^n, y^n] = 1$ para todo $[x,y] \in X$. Luego el teorema queda demostrado al aplicar el teorema 7.20 de Dietzmann. □

Si G es un grupo, consideramos el subconjunto

$$\Delta^+(G) = \{x \in \Delta(G) : x \text{ tiene orden finito}\}.$$

lem:DcharG **Lemma 7.22.** *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 7.23.** *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 7.22.

thm:Connel

Theorem 7.24 (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 7.19, $\widehat{N} = \sum_{x \in N} x$ 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 7.23 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 **??** 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 **??**. 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 7.25 (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 6.11. 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 8

Vamos a demostrar un teorema de Frobenius que afirma que salvo isomorfismo las únicas álgebras reales de dimensión finita que son álgebras de división son los reales, los complejos y los cuaterniones. Daremos una demostración completamente elemental.

lem:trick_frobenius1

Lemma 8.1. *Sea D un álgebra de división real de dimensión n. Si $x \in D$, entonces existe $\lambda \in \mathbb{R}$ tal que $x^2 + \lambda x \in \mathbb{R}$.*

Proof. Como $\dim D = n$, el conjunto $\{1, x, x^2, \ldots, x^n\}$ es linealmente dependiente. Entonces existe un polinomio no nulo $f \in \mathbb{R}[X]$ de grado $\leq n$ tal que $f(x) = 0$. Sin perder generaliadad podemos suponer que el coeficiente principal de f es uno y escribir entonces a f como producto de factores de grado ≤ 2:

$$f = (X - \alpha_1) \cdots (X - \alpha_r)(X^2 + \lambda_1 X + \mu_1) \cdots (X^2 + \lambda_s X + \mu_s).$$

Como D es de división y $f(x) = 0$, algún factor de f es cero. Entonces x es raíz de algún $X - \alpha_j$ o de algún $X^2 + \lambda_k X + \mu_k$. En cualquier caso, existe $\lambda \in \mathbb{R}$ tal que $x^2 + \lambda x \in \mathbb{R}$. □

lem:trick_frobenius2

Lemma 8.2. *Sea D un álgebra de división real de dimensión n. Entonces*

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

es un subespacio de D tal que $D = \mathbb{R} \oplus V$.

Proof. Sea $x \in D \setminus V$ tal que $x^2 \in \mathbb{R}$. Entonces, como $x^2 > 0$, podemos escribir $x^2 = \alpha^2$ para algún $\alpha \in \mathbb{R}$. Luego $x = \pm\alpha \in \mathbb{R}$ pues D es de división y $(x - \alpha)(x + \alpha) = x^2 - \alpha^2 = 0$.

Veamos que V es un subespacio de D. Primero observemos que $0 \in V$ y que si $x \in V$ entonces $\lambda x \in V$ para todo $\lambda \in \mathbb{R}$. Sean $x, y \in V$. Si $\{x, y\}$ es linealmente dependiente, entonces $x + y \in V$. Supongamos entonces que x e y son linealmente independientes. Probemos entonces que $\{1, x, y\}$ es linealmente independiente: si existen $\alpha, \beta, \gamma \in \mathbb{R}$ tales que $\alpha x + \beta y + \gamma = 0$, entonces

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

Esto implica que $2\beta\gamma y \in \mathbb{R}$ y luego $\beta\gamma = 0$. Luego $\alpha = \beta = \gamma = 0$. Por el lema 8.1, existen $\lambda, \mu \in \mathbb{R}$ tales que

$$(x+y)^2 + \lambda(x+y) \in \mathbb{R}, \quad (x-y)^2 + \mu(x-y) \in \mathbb{R}.$$

Como además

$$(x+y)^2 + (x-y)^2 = 2x^2 + 2y^2 \in \mathbb{R},$$

entonces $(\lambda+\mu)x + (\lambda-\mu)y \in \mathbb{R}$. Como $\{1, x, y\}$ es linealmente independiente, $\lambda = \mu = 0$. Luego $(x+y)^2 \in \mathbb{R}$. Si $x+y \notin V$, entonces, por lo que observamos al principio de la demostración, tendríamos que $x+y \in \mathbb{R}$, una contradicción.

Claramente $\mathbb{R} \cap V = 0$. Si $x \in D \setminus \mathbb{R}$ entonces, por el lema 8.1, $x^2 + \lambda x \in \mathbb{R}$ para algún $\lambda \in \mathbb{R}$. Afirmamos que $x + \lambda/2 \in V$. De lo contrario, como

$$(x + \lambda/2)^2 = x^2 + \lambda x + (\lambda/2)^2 \in \mathbb{R},$$

tendríamos $x + \lambda/2 \in \mathbb{R}$ y luego $x \in \mathbb{R}$. Luego $x = -\lambda/2 + (x + \lambda/2) \in \mathbb{R} \oplus V$. □

lem:trick_frobenius3

Lemma 8.3. *Sea D una $\mathbb{R}$-álgebra de división real de dimensión n. Si $n > 2$, entonces existen $i, j, k \in D$ tales que $\{1, i, j, k\}$ es linealmente independiente y*

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i. \tag{8.1}$$

eq:H

Proof. Sea $V = \{x \in D : x^2 \in \mathbb{R}, x^2 \leq 0\}$ el subespacio del lema 8.2. Para $x, y \in V$ definimos $x \circ y = xy + yx = (x+y)^2 - x^2 - y^2 \in \mathbb{R}$. Además si $x \neq 0$ entonces $x \circ x = 2x^2 \neq 0$. Como $\dim V = n-1$, existen $y, z \in V$ tales que $\{y, z\}$ es linealmente independiente. Sea

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

Como $\{y, z\}$ es linealmente independiente, $x \neq 0$. Además, como

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

se tiene que $xy = -yx$. Sean

$$i = \frac{1}{\sqrt{-x^2}} x, \quad j = \frac{1}{\sqrt{-y^2}} y, \quad k = ij.$$

Un cálculo directo demuestra que valen las fórmulas (8.1). Por ejemplo:

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

□

thm:Frobenius

Theorem 8.4 (Frobenius). *Toda álgebra real de división y dimensión finita es isomorfa a* $\mathbb{R}$*,* $\mathbb{C}$ *o* $\mathbb{H}$*.*

Proof. Sea D un álgebra real de división y sea $n = \dim D$. Si $n = 1$, entonces $D \simeq \mathbb{R}$. Si $n = 2$, el subespacio V del lema 8.2 es no nulo y entonces existe $i \in D$ tal que $i^2 = -1$. Luego $D \simeq \mathbb{C}$. El lema 8.3 demuestra que $n \neq 3$. Si $n = 4$ entonces $D \simeq \mathbb{H}$. Supongamos entonces que $n > 4$. El lema 8.3 garantiza la existencia de elementos $i, j, k \in D$ tales que $\{1, i, j, k\}$ es linealmente independiente y valen las fórmulas (8.1). Sea

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

Por el lema 8.2 sabemos que $\dim V = n - 1$. Entonces existe $x \in V \setminus \langle i, j, k\rangle$. Sea

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

Un cálculo directo muestra que $i \circ e = j \circ e = k \circ e = 0$. Pero entonces

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

una contradicción. □

Vamos a dar una demostración completamente elemental de un famoso teorema de Wedderburn. Antes necesitamos repasar algunos conceptos básicos sobre polinomios ciclotómicos.

Definition 8.5. El n-polinomio ciclotómico se define como

$$\Phi_n(X) = \prod (X - \zeta), \tag{8.2}$$

eq:ciclotomico

donde el producto se hace sobre todas las n-raíces primitivas de la unidad.

Example 8.6. 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 8.7. *Sea* $n \in \mathbb{N}$*. Entonces*

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

Proof. Escribimos

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

□

Lemma 8.8. *Sea $n \in \mathbb{N}$. 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 8.9 (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

$$q^n - 1 = q - 1 + \sum_{j=1}^{m} \frac{q^n - 1}{q^{d_j} - 1}, \tag{8.3}$$

eq:clases

donde $1 < \frac{q^n-1}{q^{d_j}-1} \in \mathbb{Z}$ para todo $j \in \{1, \ldots, m\}$. Como $d^{d_j} - 1$ divide a $q^n - 1$, cada d_j divide a n. En particular, la fórmula (8.2) implica que podemos escribir

$$X^n - 1 = \Phi_n(X)(X^{d_j} - 1)h(X) \tag{8.4}$$

eq:trick_ciclotomico

para algún polinomio $h(X) \in \mathbb{Z}[X]$. Al evaluar (8.4) 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 (8.3), $\Phi_n(q)$ divide a $q - 1$. Luego

$$q - 1 \ge |\Phi_n(q)| = \prod |q - \zeta| > q - 1$$

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 8.10. *Sea R un anillo unitario finito. Entonces para todo $n \ge 1$ 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 $i \in \{1,\ldots,k\}$, o bien $k \geq 2$ y $n_i = 1$ para todo $i \in \{1,\ldots,k\}$. 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, $x = (1,0,0,\ldots,0)$, $y = (0,1,0,\ldots,0)$ y $z = (1,1,0,\ldots,0)$ es una solución de $x^n + y^n = z^n$. □

Lecture 9
Some hints

Lecture 1

Lecture 2

Lecture 3

Lecture 4

Lecture 5

?? Consider the proper non-zero ideal

$$I(G) = \left\{ \sum_{g \in G} \lambda_g g \in K[G] : \sum_{g \in G} \lambda_g = 0 \right\}.$$

Lecture 6

Lecture 7

Lecture 8

Lecture 9

Lecture 10

Lecture 9

Lecture 10

Lecture 11

Lecture 12

Lecture 13

Lecture 10

Some solutions

Lecture 1

Lecture 2

Lecture 3

Lecture 4

Lecture 5

Lecture 6

Lecture 7

Lecture 8

Lecture 9

Lecture 10

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. G. Köthe. Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist. *Math. Z.*, 32(1):161–186, 1930.
3. J. Krempa. Logical connections between some open problems concerning nil rings. *Fund. Math.*, 76(2):121–130, 1972.
4. P. P. Nielsen. Simplifying Smoktunowicz's extraordinary example. *Comm. Algebra*, 41(11):4339–4350, 2013.
5. A. Smoktunowicz. Polynomial rings over nil rings need not be nil. *J. Algebra*, 233(2):427–436, 2000.
6. A. Smoktunowicz. On some results related to Köthe's conjecture. *Serdica Math. J.*, 27(2):159–170, 2001.
7. A. Smoktunowicz. Some results in noncommutative ring theory. In *International Congress of Mathematicians. Vol. II*, pages 259–269. Eur. Math. Soc., Zürich, 2006.

Index

Algebra, 1
  algebraic, 2
  commutative, 1
  dimension, 1
  ideal, 2
  simple, 9
Algebraic element, 2
Anillo
  artiniano a derecha, 42
  artiniano a izquierda, 42
  con involución, 37
  denso de operadores lineales, 49
  noetheriano a derecha, 42
  noetheriano a izquierda, 42
  primo, 51
  semiprimitivo, 46
  semisimple Jacobson, 46

Extensión de escalares, 35

Frobenius
  teorema de, 59

Grupo
  de Prüfer, 29
  localmente finito, 29
  resoluble, 30

Homomorphism
  of algebras, 2

Ideal
  primitive, 14
Involución
  de un anillo, 37

Jacobson
  densidad de, 49

Lema
  de Nakayama, 39
Lemma
  Zorn, 17

Maximal
  elemento, 41
Minimal
  elemento, 41
Módulo
  artiniano, 41
  de longitud finita, 42
  longitud, 44
  noetheriano, 41
  serie de composición de un, 42

Polinomio ciclotómico, 59
Producto subdirecto de anillos, 46
Producto tensorial
  de espacios vectoriales, 32
  de transformaciones lineales, 33
  de álgebras, 35
  propiedad universal, 32

Ring
  local, 23
  nil, 20
  primitive, 14
  radical, 19

Serie de composición, 43

Teorema
  de Connel, 56
  de densidad de Jacobson, 49

de Dietzmann, 54
de Formanek, 31, 36
de Frobenius, 59
de Herstein, 30
de Jordan–Hölder, 43
de Rickart, 38
de Schur, 55
de Wedderburn, 52, 60