Leandro Vendramin

Associative algebras

Notes

Wednesday 22nd September, 2021

Contents

Chapter 1
Semisimple algebras

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.

Two basic exercises about group algebras.

Exercise 1.9. Let G be a non-trivial finite group. Then $\mathbb{C}[G]$ has zero divisors.

Exercise 1.10. Let A be an algebra and G be a finite group. If $f\colon G \to \mathscr{U}(R)$ is a group homomorphism, then there exists an algebra homomorphism $\varphi\colon K[G] \to A$ such that $\varphi|_G = f$.

Definition 1.11. 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 $\mathbb{C}$.

Definition 1.12. An **ideal** of an algebra is an ideal of the underlying ring that is also a subspace.

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 left ideal of the algebra A. Indeed, if L is a left ideal of A and $\lambda \in K$ and $x \in L$, then

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

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

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 an algebra homomorphism.

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

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

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

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

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

Definition 1.15. A **module** M over an algebra A is a module over the ring A that is also a vector space.

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.

In this chapter we will work with finitely generated modules.

Example 1.16. An algebra A is a module over A with left multiplication, that is $a \cdot b = ab$, $a, b \in A$. This module is the (left) **regular representation** of A and it will be denoted by ${}_A A$.

Definition 1.17. 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 1.18. 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 1.19 (Schur). *Let A be an algebra. If S and T are simple modules and $f \colon S \to T$ is a non-zero module homomorphism, then f is an isomorphism.*

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

Proposition 1.20. *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 homomorphism. In particular, $A/\ker\varphi \simeq S$ and hence $\dim S = \dim(A/\ker\varphi) \leq \dim A$. $\square$

pro:semisimple

Proposition 1.21. *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 non-zero 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 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.

Veamos ahora que $(2) \implies (1)$. Sea J un subconjunto de $\{1, \dots, k\}$ maximal tal que la suma de los S_j con $j \in J$ es directa. Sea $N = \oplus_{j \in J} S_j$. Veamos que $M = N$. Para cada $i \in \{1, \dots, k\}$, se tiene que $S_i \cap N = \{0\}$ o bien que $S_i \cap N = S_i$, pues S_i es simple. Si $S_i \cap N = S_i$ para todo $i \in \{1, \dots, k\}$, entonces $S_i \subseteq N$ para todo $i \in \{1, \dots, k\}$. Si, en cambio, existe $i \in \{1, \dots, k\}$ tal que $S_i \cap N = \{0\}$, entonces N y S_i estarán en suma directa, una contradicción a la maximalidad del conjunto J.

Demostremos por último que $(3) \implies (1)$. Procederemos por inducción en $\dim M$. Si $\dim M = 1$ el resultado es trivial. Si $\dim M \geq 1$, sea S un submódulo no nulo de M de dimensión minimal. En particular, S es simple. Por hipótesis sabemos que existe un submódulo T de M tal que $M = S \oplus T$. Veamos que T verifica la hipótesis. Si X es un submódulo de T, entonces, como en particular T es un submódulo de M, existe un submódulo Y de M tal que $M = X \oplus Y$. Luego

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

pues $X \subseteq T$. Como $\dim T < \dim M$ y además $T \cap Y$ es un submódulo de T, la hipótesis inductiva implica que T es suma directa de módulos simples. Luego M también es suma directa de submódulos simples. $\square$

Proposition 1.22. *Si M es un A-módulo semisimple y N es un submódulo, entonces N y M/N son semisimples.*

Proof. Supongamos que $M = S_1 + \cdots + S_k$, donde los S_i son submódulos simples. Si $\pi \colon M \to M/N$ es el morfismo canónico, el lema de Schur nos dice que cada restricción $\pi|_{S_i}$ es cero o un isomorfismo. Luego

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

es también una suma finita de módulos simples. Como además existe un submódulo T tal que $M = N \oplus T$, se tiene que $N \simeq M/T$ es también semisimple. $\square$

Definition 1.23. Un álgebra A se dirá **semisimple** si todo A-módulo finitamente generado es semisimple.

Proposition 1.24. *Sea A un álgebra de dimensión finita. Entonces A es semisimple si y sólo si la representación regular de A es semisimple.*

Proof. Demostremos la implicación no trivial. Sea M un A-módulo finitamente generado, digamos $M = (m_1, \dots, m_k)$. La función

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

es un epimorfismo de A-módulos. Como A es semisimple, $\oplus_{i=1}^{k} A$ es semisimple. Luego M es semisimple por ser isomorfo al cociente de un semisimple. □

Theorem 1.25. *Sea A un álgebra semisimple de dimensión finita. Si ${}_A A = \oplus_{i=1}^{k} S_i$, donde los S_i son submódulos simples y S es un A-módulo simple, entonces $S \simeq S_i$ para algún $i \in \{1,\dots,k\}$.*

Proof. Sea $s \in S \setminus \{0\}$. La función $\varphi\colon A \to S$, $a \mapsto a \cdot s$, es un morfismo de A-módulos sobreyectivo. Como $\varphi \neq 0$, existe $i \in \{1,\dots,k\}$ tal que alguna restricción $\varphi|_{S_i}\colon S_i \to S$ es no nula. Por el lema de Schur, $\varphi|_{S_i}$ es un isomorfismo. □

Como aplicación inmediata tenemos que un álgebra semisimple A de dimensión finita admite, salvo isomorfismo, únicamente finitos módulos simples. Cuando digamos que $S_1,\dots,S_k$ son los simples de A estaremos refiriéndonos a que los S_i son representantes de las clases de isomorfismo de todos los A-módulos simples, es decir que todo simple es isomorfo a alguno de los S_i y además $S_i \not\simeq S_j$ si $i \neq j$.

Si A y B son álgebras, M es un A-módulo y N es un B-módulo, entonces $A \times B$ actúa en $M \oplus N$ por

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

Todo módulo M finitamente generado sobre un anillo de división es libre, es decir posee que una base. Tal como pasa en espacios vectoriales, vale además que todo conjunto linealmente independiente de M puede extenderse a una base.

Recordemos que si V es un A-módulo, $\operatorname{End}_A(V)$ se define como el conjunto de morfismos de módulos $V \to V$. En realidad, $\operatorname{End}_A(V)$ es un álgebra con las operaciones: $(f+g)(v) = f(v)+g(v)$, $(af)(v) = af(v)$ y $(fg)(v) = f(g(v))$ para todo $f,g \in \operatorname{End}_A(V)$, $a \in A$ y $v \in V$.

Lemma 1.26. *Sea D un álgebra de división y sea V un D-módulo finitamente generado. Entonces V es un $\operatorname{End}_D(V)$-módulo simple y además existe $n \in \mathbb{N}$ tal que $\operatorname{End}_D(V) \simeq nV$ es semisimple.*

Proof. Sea $\{v_1,\dots,v_n\}$ una base de V. La función

$$\operatorname{End}_D(V) \to \underbrace{V \oplus \cdots \oplus V}_{n\text{-veces}}, \quad f \mapsto (f(v_1),\dots,f(v_n)),$$

es un isomorfismo de $\operatorname{End}_D(V)$-módulos. Luego

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

Falta ver que V es simple. Para eso alcanza con demostrar que $V = (v)$ para todo $v \in V \setminus \{0\}$. Sea $v \in V \setminus \{0\}$. Si $w \in V \setminus \{0\}$, existen $w_2,\dots,w_n$ tal que

$\{w, w_2, \dots, w_n\}$ es una base de V. Existe $f \in \mathrm{End}_D(V)$ tal que $f \cdot v = f(v) = w$. En consecuencia, $w \in (v)$ y entonces $V = (v)$. □

En lenguaje matricial, el lema anterior nos dice que si D es un álgebra de división, entonces D^n es un $M_n(D)$-módulo simple y que $M_n(D) \simeq nD^n$ como $M_n(D)$-módulos.

Theorem 1.27. *Sea A un álgebra de dimensión finita y sean $S_1, \dots, S_k$ los representantes de las clases de isomorfismo de los A-módulos simples. Si*

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

entonces los n_j quedan únivocamente determinados.

Proof. Como los S_j son módulos simples no isomorfos, el lema de Schur nos dice que si $i \neq j$ entones $\mathrm{Hom}_A(S_i, S_j) = \{0\}$. Para cada $j \in \{1, \dots, k\}$ tenemos entonces que

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

Como M y los S_j son espacios vectoriales de dimensión finita, $\mathrm{Hom}_A(M, S_j)$ y $\mathrm{Hom}_A(S_j, S_j)$ son también espacios vectoriales de dimensión finita. Además $\dim \mathrm{Hom}_A(S_j, S_j) \geq 1$ pues $\mathrm{id} \in \mathrm{Hom}_A(S_j, S_j)$. Luego los n_j quedan unívocamente determinados, pues

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

Si A es un álgebra, definimos el **álgebra opuesta** A^{op} como el espacio vectorial A con el producto $(a, b) \mapsto ba = a \cdot_{\mathrm{op}} b$.

lem:A^op

Lemma 1.28. *Si A es un álgebra, $A^{\mathrm{op}} \simeq \mathrm{End}_A(A)$ como álgebras.*

Proof. Primero observemos que $\mathrm{End}_A(A) = \{\rho_a : a \in A\}$, donde $\rho_a \colon A \to A$ está dado por $x \mapsto xa$. En efecto, si $f \in \mathrm{End}_A(A)$ entonces $f(1) = a \in A$. Además $f(b) = f(b1) = bf(1) = ba$ y luego $f = \rho_a$. Tenemos entonces una biyección $\mathrm{End}_A(A) \to A^{\mathrm{op}}$ que es morfismo de álgebras pues

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

lem:Mn_op

Lemma 1.29. *Si A es un álgebra y $n \in \mathbb{N}$, entonces $M_n(A)^{\mathrm{op}} \simeq M_n(A^{\mathrm{op}})$ como álgebras.*

Proof. Sea $\psi \colon M_n(A)^{\mathrm{op}} \to M_n(A^{\mathrm{op}})$ dada por $X \mapsto X^T$, donde X^T es la traspuesta de X. Como ψ es una transformación lineal biyectiva, basta ver que ψ es morfismo. Si $i, j \in \{1, \dots, n\}$, $a = (a_{ij})$ y $b = (b_{ij})$ entonces

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

lem:simple

Lemma 1.30. *Si S es un módulo simple y $n \in \mathbb{N}$, entonces*

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

como álgebras.

Proof. Sea (φ_{ij}) una matriz con entradas en $\mathrm{End}_A(S)$. Vamos a definir una función $nS \to nS$ de la siguiente forma:

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

Dejamos como ejercicio demostrar que esta aplicación define un morfismo inyectivo de álgebras

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

Este morfismo es sobreyectivo pues si $\psi \in \mathrm{End}(nS)$ y para cada $i, j \in \{1, \dots, n\}$ es posible definir a los ψ_{ij} mediante las ecuaciones

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

Theorem 1.31 (Artin–Wedderburn). *Sea A un álgebra semisimple y de dimensión finita, digamos con k clases de isomorfismos de A-módulos simples. Entonces*

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

para ciertos $n_1, \dots, n_k \in \mathbb{N}$ y ciertas álgebras de división $D_1, \dots, D_k$.

Proof. Al agrupar los finitos submódulos simples de la representación regular de A podemos escribir

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

donde los S_i son submódulos simples tales que $S_i \not\simeq S_j$ si $i \neq j$. Dejamos como ejercicio verificar que, gracias al lema de Schur, tenemos

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

donde cada $D_i = \mathrm{End}_A(S_i)$ es un álgebra de división. Tenemos entonces que

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

Como $\mathrm{End}_A(A) \simeq A^{\mathrm{op}}$, entonces

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

Como además cada D_i es un álgebra de división, cada D_i^{op} también lo es. □

Utilizaremos el teorema de Wedderburn en el caso de los números complejos.

Corollary 1.32 (Mollien). *Si A es un álgebra compleja de dimensión finita semisimple, entonces*

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

para ciertos $n_1, \dots, n_k \in \mathbb{N}$.

Proof. Vimos en la demostración del teorema de Wedderburn que

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

donde $S_1, \dots, S_k$ son representantes de las clases de isomorfismos de los A-módulos simples y cada $\mathrm{End}_A(S_i)$ es un álgebra de división. Veamos que

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

para todo $i \in \{1, \dots, k\}$. En efecto, si $f \in \mathrm{End}_A(S_i)$, entonces f tiene un autovalor $\lambda \in \mathbb{C}$. Como entonces $f - \lambda\,\mathrm{id}$ no es un isomorfismo, el lema de Schur implica que $f - \lambda\,\mathrm{id} = 0$, es decir $f = \lambda\,\mathrm{id}$. Luego $\mathrm{End}_A(S_i) \to \mathbb{C}$, $\varphi \mapsto \lambda$, es un isomorfismo de álgebras. En particular,

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

Exercise 1.33. Sean A y B álgebras. Demuestre que los ideales de $A \times B$ son de la forma $I \times J$, donde I es un ideal de A y J es un ideal de B.

Definition 1.34. Un álgebra A se dice **simple** si sus únicos ideales son $\{0\}$ y A.

Proposition 1.35. *Sea A un álgebra simple de dimensión finita. Entonces existe un ideal a izquierda no nulo I de dimensión minimal. Este ideal es un A-módulo simple y todo A-módulo simple es isomorfo a I.*

Proof. Como A es de dimensión finita y A es un ideal a izquierda de A, existe un ideal a izquierda no nulo I de dimensión minimal. La minimalidad de $\dim I$ implica que I es simple como A-módulo.

Sea M un A-módulo simple. En particular, $M \neq \{0\}$. Como

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

es un ideal de A y además $1 \in A \setminus \mathrm{Ann}(M)$, la simplicidad de A implica que $\mathrm{Ann}(M) = \{0\}$ y luego $I \cdot M \neq \{0\}$ (pues $I \cdot m \neq 0$ para todo $m \in M$ implica que $I \subseteq \mathrm{Ann}(M)$ e I es no nulo, una contradicción). Sea $m \in M$ tal que $I \cdot m \neq \{0\}$. La función

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

es un morfismo de módulos. Como $I \cdot m \neq \{0\}$, el morfismo φ es no nulo. Como I y M son A-módulos simples, el lema de Schur implica que φ es un isomorfismo. □

Si D es un álgebra de división, el álgebra de matrices $M_n(D)$ es un álgebra simple. La proposición anterior nos dice en particular que $M_n(D)$ tiene una única clase de isomorfismos de $M_n(D)$-módulos simples. Como sabemos, estos módulos son isomorfos a D^n.

Proposition 1.36. *Sea A un álgebra de dimensión finita. Si A es simple, entonces A es semisimple.*

Proof. Sea S la suma de los submódulos simples de la representación regular de A. Afirmamos que S es un ideal de A. Sabemos que S es un ideal a izquierda, pues los submódulos de la representación regular de A son exactamente los ideales a izquierda de A. Para ver que $Sa \subseteq S$ para todo $a \in A$, debemos demostrar que $Ta \subseteq S$ para todo submódulo simple T de A. Si $T \subseteq A$ es un submódulo simple y $a \in A$, sea $f \colon T \to Ta$, $t \mapsto ta$. Como f es un morfismo de A-módulos y T es simple, $\ker f = \{0\}$ o bien $\ker T = T$. Si $\ker T = T$, entonces $f(T) = Ta = \{0\} \subseteq S$. Si $\ker f = \{0\}$, entonces $T \simeq f(T) = Ta$ y luego Ta es simple y entonces $Ta \subseteq S$.

Como S es un ideal de A y A es un álgebra simple, entonces $S = \{0\}$ o bien $S = A$. Como $S \neq \{0\}$, pues existe un ideal a izquierda no nulo I de A tal que $I \neq \{0\}$ de dimensión minimal, se concluye que $S = A$, es decir la representación regular de A es semisimple (por ser suma de submódulos simples) y luego el álgebra A es semisimple. □

Theorem 1.37 (Wedderburn). *Sea A un álgebra de dimensión finita. Si A es simple, entonces $A \simeq M_n(D)$ para algún $n \in \mathbb{N}$ y alguna álgebra de división D.*

Proof. Como A es simple, entonces A es semisimple. El teorema de Artin–Wedderburn implica que $A \simeq \prod_{i=1}^{k} M_{n_i}(D_i)$ para ciertos $n_1, \dots, n_k$ y ciertas álgebras de división $D_1, \dots, D_k$. Además A tiene k clases de isomorfismos de módulos simples. Como A es simple, A tiene solamente una clase de isomorfismos de módulos simples. Luego $k = 1$ y entonce $A \simeq M_n(D)$ para algún $n \in \mathbb{N}$ y alguna álgebra de división D. □

Let A be an algebra over K. If I is a left ideal of the ring A, then I is a subspace (over K), as $\lambda a = \lambda(1_A a) = (\lambda 1_A)a$ for all $\lambda \in K$ and $a \in A$.

An important example of a module is given by the left representation. The algebra A is a module over A with the left multiplication.

Chapter 2
The Jacobson radical

radical

We will consider rings possibly without identity. Thus a **ring** is an abelian group R with an associative multiplication $(x,y) \mapsto xy$ such that $(x+y)z = xz+yz$ and $x(y+z) = xy+xz$ for all $x,y,z \in R$. If there is an element $1 \in R$ such that $x1 = 1x = x$ for all $x \in R$, we say that R is a ring (or a unitary ring). A **subring** S of R is an additive subgroup of R closed under multiplication.

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

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

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

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

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

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 $1 \in R^2$.

Example 2.5. 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

$$E_{ij}AE_{kl} = a_{jk}E_{il} \tag{2.1}$$

eq:trick

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

Exercise 2.6. 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 $M=RM\neq\{0\}$.

The 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 2.7. *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 $M=Rx\subseteq L$. $\square$

Example 2.8. 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 2.9. 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.

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

Example 2.10. Let D be a division ring and let $R=M_n(D)$. Then $L=RE_{11}$ is a minimal left ideal.

Example 2.11. 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.

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

proposition:R/I

Proposition 2.12. *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 2.7. The map $\phi\colon R \to M$, $r \mapsto rm$, 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 2.13. $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/n) = n\mathbb{Z}$.

The following exercise is standard.

Exercise 2.14. 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.

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

Example 2.15. If K is a field, then K^n is a faithful unitary $M_n(K)$-module.

Example 2.16. If V is vector space over a field K, then V is faithful unitary $\mathrm{End}_K(V)$-module.

A ring R is said to be **primitive** if there exists a faithful simple R-módulo. 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 2.17. *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 2.12, 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 2.18. *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 2.17. If R is a primitive commutative ring, Proposition 2.12 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 2.19. The ring $\mathbb{Z}$ is not primitive.

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

lemma:primitivo

Lemma 2.20. *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 2.21. Let $R_1, \dots, R_n$ 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 2.22. *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 2.12, 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 2.12, 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 2.23. *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 2.12. Then R/M is primitive by Proposition 2.17. By lema 2.20, M is primitive. □

Exercise 2.24. Prove that every primitive ideal of a commutative ring is maximal.

Exercise 2.25. Prove that $M_n(R)$ is primitive if and only if R is primitive.

Let us discuss the Jacobson radical and radical rings.

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 $\{y_1\dots y_n : y_j\in I\}$. 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 $x_1x_2\cdots x_n=0$ for all $x_1,\dots,x_n\in I$.

An element x of a ring is said to be **nil** (or nilpotent) if $x^n=0$ for some $n\in\mathbb{N}$. An ideal I of a ring is said to be nil if every element of I is nil. Every nilpotent ideal is nil, as $I^n=0$ implies $x^n=0$ for all $x\in I$.

Example 2.26. 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 2.27.** *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 $(rx)^km=m$ (resp. $(xr)^kn=n$) for all $k\geq 1$, a contradiction since $rx\in I$ (resp. $xr\in I$) is a nilpotent element. □

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

exercise:circ **Exercise 2.28.** Let R be a ring. Prove that $R\times R\to R$, $(r,s)\mapsto r\circ s=r+s+rs$, is an associative operation with neutral element 0.

Exercise 2.29. Let $R=\mathbb{Z}/3=\{0,1,2\}$. Compute the multiplication table with respect to the circle operation given by the previous exercise.

If R is unitary, an element $x\in R$ is left quasi-regular (resp. right quasi-regular) if and only if $1+x$ is left invertible (resp. right invertible). In fact, if $r\in R$ is such that

$r+x+rx=0$, then $(1+r)(1+x)=1+r+x+rx=1$. Conversely, if there exists $y\in R$ such that $y(1+x)=1$, then

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

Example 2.30. 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 $y+(-x)+y(-x)=0$.

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

lemma:casiregular

Lemma 2.31. *Let I be a left ideal of R. If I is left quasi-regular, then I is quasi-regular.*

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

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

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

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

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

Our application of Zorn's lemma:

lemma:maxreg

Lemma 2.32. *Let R be a ring and $x\in R$ be an element that is not left quasi-regular Then there exists a maximal left ideal M such that $x\notin M$. Moreover, R/M is a simple R-module and $x\notin \operatorname{Ann}_R(R/M)$.*

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

The only left ideal of R contanining $T\cup\{x\}$ 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 2.12. 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, Lemma 2.32 implies that there exists a simple R-module M such $x \notin \mathrm{Ann}_R(M)$. Thus $x \notin J(R)$.

thm:casireg_eq

Theorem 2.33. *Let R be a ring and $x \in R$. The following statements are equivalent:*

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

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

We now prove $(2) \implies (3)$. If $x \notin J(R)$, then Lemma 2.32 implies that there exists a simple R-module M such that $xm \neq 0$ for some $m \in M$. The simplicity of M implies that $R(xm) = M$. Thus there exists $r \in R$ such that $rxm = -m$. There is an element $s \in R$ such that $s + rx + s(rx) = 0$ and hence

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

a contradiction.

Finally, to prove $(3) \implies (1)$ it is enough to note that x is left quasi-regular. Thus the left ideal generated by x is quasi-regular by Lemma 2.31. □

The theorem immediately implies the following corollary.

Corollary 2.34. *If R is a ring, then $J(R)$ if a quasi-regular ideal that contains every left quasi-regular ideal.*

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

thm:J(R)

Theorem 2.35. *Let R be a ring such that $J(R) \neq R$. Then*

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

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

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

By Proposition 2.12,

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

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

We now review some basic results useful to compute radicals.

Proposition 2.37. *Let $\{R_i : i \in I\}$ be a family of rings. Then*

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

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

For the next result we shall need a lemma.

lemma:trickJ1

Lemma 2.38. *Let R be a ring and $x \in R$. If $-x^2$ is a left quasi-regular element, then x también.*

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

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

proposition:J(I)

Proposition 2.39. *If I is an ideal of R, then $J(I) = I \cap J(R)$.*

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

Let $x \in J(I)$ and $r \in R$. Since $-(rx)^2 = (-rxr)x \in I(J(I)) \subseteq J(I)$, the element $-(rx)^2$ is left quasi-regular a izquierda en I. Thus rx is left quasi-regular by Lemma 2.38. □

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

Example 2.40. If R is a ring, then $J(R)$ is a radical ring, by Proposition 2.39.

Example 2.41. The Jacobson radical of $\mathbb{Z}/8$ is $\{0, 2, 4, 6\}$.

There are several characterizations of radical rings.

theorem:anillo_radical **Theorem 2.42.** *Let R be ring. The following statements are equivalent:*

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

Proof. The equivalence $(1) \iff (5)$ follows from Theorem 2.33.

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

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

To prove $(2) \implies (3)$ we note that for each regular and maximal left ideal I, the quotient R/I is a simple R-module by Proposición 2.12.

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 2.43. 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
$$\left(\frac{2x}{2y+1} \right)' = \frac{-2x}{2(x+y)+1}.$$

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

Exercise 2.44. Prove that a nil ring is a radical ring.

Exercise 2.45. 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.

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

The conjecture is known to be true in several cases. $\boxed{\text{Exercises?}}$

thm:Jnilpotente **Theorem 2.46.** *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

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

the set $\mathscr{S}$ is non-empty. Since R is left artinian, $\mathscr{S}$ has a minimal element I_0. Since $J^kI_0 \neq \{0\}$, let $x \in I_0 \setminus \{0\}$ be such that $J^kx \neq \{0\}$. Moreover, J^kx is a left ideal of R contained in I_0 and such that $J^kx \in \mathscr{S}$, as $J^k(J^kx) = J^{2k}x = J^kx \neq \{0\}$. The minimality of I_0 implies that, $J^kx = I_0$. 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 2.47. *Let R be a left artinian ring. Each nil left ideal is nilpotent and $J(R)$ is the unique maximal nilpotent ideal of R.*

Proof. Let L be a nil left ideal of R. By Proposition 2.27, L is contained in $J(R)$. Thus L is nilpotent, as $J(R)$ is nilpotent by Theorem 2.46. □

Theorem 2.48. *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 $m_1, \dots, m_n \in M$. Then

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

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

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

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

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

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

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

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

Since $u^n = 0$, the element

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

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

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

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

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

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

For completeness we recall basic results on the Jacobson radical in the case of unitary rings.

Exercise 2.49. Let R be a unitary ring. Then

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

Exercise 2.50. 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.

prob:Koethe

Open problem 2.1 (Köthe). Let R be a ring. Is the sum of two arbitrary nil left ideals of R is nil?

Notes

The material on non-commutative ring theory is standard, see for example [**?**]. Radical rings were introduced by Jacobson in [**?**]. Nil rings were used by Zelmanov in his solution to Burnside's problem, see for example [**?**].

Open problem 2.1 is the well-known Köthe's conjecture. The conjecture was first formulated in 1930, see [**?**]. It is known to be true in several cases. In full generality, the problem is still open. In [**?**] 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 [**?**]: If R is a nil ring, then $R[X]$ is a nil ring. In [**?**] 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 [**?**]. See [**?**, **?**] for more information on Köthe's conjecture and related topics.

References

Index