CAPÍTULO 2

Anéis semisimples

Neste capítulo, estudamos a classe importante dos anéis semisimples. Começamos por estudar as propriedades fundamentais dos anéis semisimples e terminamos com a demonstração do Teorema de Wedderburn-Artin que descreve "completamente" a estrutura deste tipo de anéis. Há várias abordagens ao estudo dos anéis semisimples. Aqui, usamos a linguagem "moderna" da teoria dos módulos. Um dos nossos objectivos principais é aplicar esta teoria ao estudo das representações de grupos (finitos) e, mais geralmente, de álgebras de dimensão finita.

Ao longo deste capítulo, salvo menção em contrário, R denota um anel arbitrário.

2.1. Módulos e anéis semisimples

2.1.1. Se M é um R-módulo, dizemos que M é um *R-módulo semisimples* se, para qualquer $N \leq_R M$, existe $N' \leq_R M$ tal que $M = N \oplus N'$.

É claro que qualquer R-módulo simples é semisimples e, também, indecomponível (o recíproco não é necessariamente verdadeiro).

2.1.2. Proposição. *Qualquer R-módulo simples M é cíclico, isto é, existe $0 \neq m \in M$ tal que $M = Rm$.*

Demonstração. Se $0 \neq m \in M$, então $Rm \leq_R M$ é não-nulo, logo $Rm = M$ (porque M é simples). $\square$

2.1.3. Proposição. *Se M é um R-módulo simples e $m \in M$ é tal que $M = Rm$, então $\operatorname{Ann}_R(m)$ é um ideal esquerdo maximal de R.*

Demonstração. Tem-se $Rm \cong_R R/\operatorname{Ann}_R(m)$, de modo que $\operatorname{Ann}_R(m)$ e R são os únicos ideais esquerdos de R que contêm $\operatorname{Ann}_R(m)$ (pelo Teorema 1.2.11 uma vez que M é simples). O resultado segue-se porque $\operatorname{Ann}_R(m) \neq R$ (caso contrário, $M = \{0\}$). $\square$

2.1.4. Teorema (Lema de Schur). *Se M é um R-módulo simples, então:*

(a) $\operatorname{End}_R(M)$ *é um anel de divisão.*

(b) *Para qualquer R-módulo simples N,* $\operatorname{Hom}_R(M, N) \neq \{0\}$ *se e só se $N \cong_R M$.*

Demonstração. (a) Se $0 \neq \varphi \in \operatorname{End}_R(M)$, então $\operatorname{Im}(\varphi) \neq \{0\}$ e $\ker(\varphi) \neq M$, logo $\operatorname{Im}(\varphi) = M$ e $\ker(\varphi) = \{0\}$ (porque M é simples e $\operatorname{Im}(\varphi), \ker(\varphi) \leq_R M$). Sendo assim, qualquer R-endomorfismo não-nulo de M é invertível, o que significa que $\operatorname{End}_R(M)$ é um anel de divisão.

(b) O argumento usado em (a) pode ser imitado para provar que, se N é um R-módulo simples, então qualquer homomorfismo $\alpha\colon M \to N$ é invertível. □

2.1.5. Lema. *Se M é um R-módulo semisimples e $N \leq_R M$, então os R-módulos N e M/N são semisimples.*

Demonstração. Seja $N' \leq_R N$. Como M é semisimples, existe $M'' \leq_R M$ tal que $M = N' \oplus M''$. Tomando $N'' = M'' \cap N$, obtemos $N = N' \oplus N''$ (exercício).

Um submódulo de M/N é da forma M'/N em que $M' \leq_R M$ e $N \subseteq M'$. Como M é semisimples, existe $M'' \leq_R M$ tal que $M = M' \oplus M''$, de modo que $M/N = (M'/N) \oplus ((M'' + N)/N)$ (exercício). □

2.1.6. Lema. *Se $M \neq \{0\}$ é um R-módulo semisimples, então existe um submódulo simples $N \leq_R M$.*

Demonstração. Seja $0 \neq m \in M$ e consideremos o submódulo $Rm \leq_R M$. Pelo lema anterior, Rm é um R-módulo semisimples, de modo que, sem perda de generalidade, podemos admitir que $M = Rm$. Usando o Lema de Zorn, concluímos que o conjunto

$$\Sigma = \{N \leq_R M \colon m \notin N\}$$

tem pelo menos um elemento maximal; seja N este elemento. Como M é semisimples, existe $N' \leq_R M$ tal que

$$M = N \oplus N';$$

claramente, tem de ser $N' \neq 0$. Provamos que N' é simples.

De facto, se $\{0\} \neq N'' \leq_R N'$, então $N \subsetneq N + N''$ (porque $N \cap N'' \subseteq N \cap N' = \{0\}$), logo $m \in N + N''$ (pela maximalidade de $N \in \Sigma$), logo

$$Rm \leq_R N + N'' \leq_R N + N' = M = Rm$$

e, portanto, $N + N'' = N + N'$, de onde resulta que $N'' = N'$ (porque $N'' \subseteq N'$ e a soma $N + N'$ é directa). □

2.1.7. Lema. *Seja M um R-módulo e suponhamos que $M = \sum_{i \in I} M_i$ onde $\{M_i \colon i \in I\}$ é uma família de submódulos simples de M. Então, para qualquer $N \leq_R M$, existe um subconjunto $J \subseteq I$ tal que*

$$M = N \oplus \Big(\bigoplus_{j \in J} M_j \Big).$$

Demonstração. Para simplificar, para qualquer $J \subseteq I$, escrevemos

$$M_J = \sum_{j \in J} M_j;$$

de modo que $M = M_I$.

Seja Σ o conjunto de todos os subconjuntos $J \subseteq I$ tais que

$$N \cap M_J = \{0\} \quad \text{e} \quad M_J = \bigoplus_{j \in J} M_j.$$

Como $M_\emptyset = \{0\}$, é óbvio que $\emptyset \in \Sigma$ (logo, Σ é não-vazio). Com vista a aplicar o Lema de Zorn, seja $\{I_\alpha \colon \alpha \in \Gamma\}$ uma cadeia em Σ e justifiquemos que a união

$$I' = \bigcup_{\alpha \in \Gamma} I_\alpha$$

está em Σ.

Deixamos como exercício a justificação de que $N \cap M_{I'} = \{0\}$ e provamos que

$$M_{I'} = \bigoplus_{i' \in I'} M_{i'}.$$

Suponhamos que $M_{I'} \neq \bigoplus_{i' \in I'} M_i$, de modo que existe $i' \in I'$ tal que $M_{i'} \cap M_{I' \setminus \{i'\}} \neq \{0\}$. Seja $0 \neq m \in M_{i'} \cap M_{I''}$. Então, existem $i_1, \ldots, i_t \in I'$ tais que

$$m = m_1 + \ldots + m_t, \qquad 0 \neq m_i \in M_{i_i},\ 1 \leq i \leq t.$$

Como $\{I_\alpha \colon \alpha \in \Gamma\}$ é uma cadeia, existe $\alpha \in I$ tal que $i', i_1, \ldots, i_t \in I_\alpha$ e, portanto,

$$M_{I_\alpha} = \bigoplus_{i \in I_\alpha} M_i = M_{i'} \oplus M_{i_1} \cdots \oplus M_{i_t} \oplus \left(\bigoplus_{i \in I_\alpha \setminus \{i', i_1, \ldots, i_t\}} M_i \right)$$

(porque $I_\alpha \in \Sigma$), o que contradiz a equação acima. Segue-se que $I' \in \Sigma$ e, portanto o Lema de Zorn garante que Σ tem pelo menos um elemento maximal; seja $J \subseteq I$ este elemento.

Para terminar a demonstração, provemos que

$$M = N + M_J = N \oplus \left(\bigoplus_{j \in J} M_j \right).$$

Se $M \neq N + M_J$, então existe $i \in I$ tal que $M_i \not\subseteq N + M_J$, logo $M_i \not\subseteq N$ e $M_i \not\subseteq M_J$. Assim, $M_i \cap N \lneq_R M_i$ e, portanto, $M_i \cap N = \{0\}$ (porque M_i é simples); analogamente, $M_i \cap M_J = \{0\}$. Daqui resulta que, se $J' = J \cup \{i\}$, então

$$N \cap M_{J'} = \{0\} \qquad \text{e} \qquad M_{J'} = \bigoplus_{j' \in J'} M_{j'},$$

logo $J' \in \Sigma$, contradizendo a maximalidade de J.

A demonstração está completa. $\square$

2.1.8. TEOREMA. *Para qualquer R-módulo M, as afirmações seguintes são equivalentes.*

(a) *M é semisimples.*

(b) *M é soma de uma família de submódulos simples.*

(c) *M é soma directa de uma família de submódulos simples.*

Demonstração. (a) $\Rightarrow$ (b) Seja $M' \leq_R M$ a soma de todos os submódulos simples de M. Como M é semisimples, existe $M'' \leq_R M$ tal que $M \cong_R M' \oplus M''$. Se $M'' \neq 0$, o Lema 2.1.6 garante que M'' tem um submódulo simples N. Mas, por escolha de M', tem de ser $N \leq_R M'$, uma contradição. Por conseguinte, $M'' = 0$ e, portanto $M = M'$.

(b) $\Rightarrow$ (c) Resulta imediatamente do lema anterior, tomando $N = \{0\}$.

(c) $\Rightarrow$ (a) Resulta imediatamente do lema anterior. □

2.1.9. COROLÁRIO. *Se M é um R-módulo semisimples e $N \leq_R M$, então N é simples se e só se é indecomponível.*

Demonstração. Exercício. □

2.1.10. Dizemos que R é um *anel semisimples à esquerda* se o R-módulo regular esquerdo ${}_RR$ é semisimples; analogamente, dizemos que R é um *anel semisimples à direita* se o R-módulo regular direito R_R é semisimples.

Mais tarde, provaremos que estas duas noções são equivalentes: R é anel semisimples à esquerda se e só se é semisimples à direita. Deste modo, faz sentido dizer que R é um *anel semisimples* se R é anel semisimples à esquerda ou à direita.

2.1.11. PROPOSIÇÃO. *Um anel R é semisimples (à esquerda) se e só se*

$$R = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_t$$

para alguns ideais esquerdos minimais(*) $\mathcal{L}_1, \ldots, \mathcal{L}_t$ *de R.*

Demonstração. Como R é anel semisimples, o Teorema 2.1.8 garante que

$$R = \bigoplus_{i \in I} \mathcal{L}_i$$

para alguma família $\{\mathcal{L}_i : i \in I\}$ de submódulos simples de ${}_RR$, isto é, de ideais esquerdos minimais de R. Sendo assim, para estabelecer o resultado, basta provar que I é um conjunto finito.

Como $R = \sum_{i \in I} \mathcal{L}_i$, existe um subconjunto finito $J \subseteq I$ tal que

$$1 = \sum_{j \in J} a_j$$

(*)Um *ideal esquerdo minimal* de R é um ideal esquerdo $\mathcal{L} \neq \{0\}$ tal que, se $\mathcal{L}' \subseteq \mathcal{L}$ é um ideal esquerdo de R, então $\mathcal{L}' \neq \{0\}$ ou $\mathcal{L}' = \mathcal{L}$; dito de outro modo, $\mathcal{L}$ é um submódulo simples do R-módulo regular ${}_RR$.

onde $a_j \in \mathcal{L}_j$ para $j \in J$. Com vista a absurdo, suponhamos que I é infinito e seja $i \in I \setminus J$. Para qualquer $0 \neq a \in \mathcal{L}_i$, temos

$$a = a \cdot 1 = \sum_{j \in J} a a_j \in \sum_{j \in J} \mathcal{L}_j,$$

logo

$$a \in \mathcal{L}_i \cap \big(\sum_{j \in J} \mathcal{L}_j\big) = \{0\},$$

uma contradição. □

2.1.12. Corolário. *Qualquer anel semisimples (à esquerda) é noetheriano à esquerda e artiniano à esquerda.*

Demonstração. Seja R um anel semisimples (à esquerda). Pela Proposição 2.1.11, existem ideais esquerdos minimais $\mathcal{L}_1, \ldots, \mathcal{L}_t$ de R tais que

$$R = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_t.$$

A cadeia

$$\{0\} \subsetneq \mathcal{L}_1 \subsetneq \mathcal{L}_1 \oplus \mathcal{L}_2 \subsetneq \cdots \subsetneq \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_t = R$$

é claramente uma série de composição do R-módulo regular ${}_R R$, pelo que basta aplicar o Teorema 1.4.15. □

2.1.13. Teorema. *As afirmações seguintes são equivalentes:*

(a) *R é um anel semisimples (à esquerda).*

(b) *Qualquer R-módulo é semisimples.*

(c) *Qualquer R-módulo finitamente gerado é semisimples.*

(d) *Qualquer R-módulo cíclico é semisimples.*

(e) *Qualquer sequência exacta $0 \to M' \to M \to M'' \to 0$ de R-módulos é cindível.*

(f) *Qualquer R-módulo é projectivo.*

Demonstração. As implicações (b) $\Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (a) são triviais, a equivalência (b) $\Leftrightarrow$ (e) é clara e a equivalência (e) $\Leftrightarrow$ (f) é aplicação imediata do Teorema 1.3.16.

Resta provar (a) $\Rightarrow$ (b). Para isso, seja M é um R-módulo arbitrário. Supomos que ${}_R R$ é um R-módulo semisimples, com vista a provar que M é semisimples. Para qualquer $m \in M$, temos

$$Rm \cong_R R/\operatorname{Ann}_R(m),$$

logo Rm é um R-módulo semisimples (pelo Lema 2.1.5) e, portanto, é uma soma de submódulos simples (pelo Teorema 2.1.8). Sendo assim,

$$M = \sum_{m \in M} Rm$$

também é uma soma de submódulos simples e, portanto, é semisimples (de novo pelo Teorema 2.1.8). □

2.1.14. Teorema (Maschke). *Para qualquer grupo finito G, o anel de grupo RG é semisimples (à esquerda) se e só se R é um anel semisimples (à esquerda) e $|G| \cdot 1_R$ é um elemento invertível em R.*

Demonstração. ($\Leftarrow$) Admitimos que R é semisimples e que $|G| = |G| \cdot 1_R$(*) é invertível em R, com vista a provar que RG é semisimples. Para isso, provamos que qualquer RG-módulo é semisimples e usamos o Teorema 2.1.13.

Sejam M um RG-módulo e $N \leq_{RG} M$; o objectivo é provar que N é parcela directa de M. Ora, M é um R-módulo com respeito à multiplicação R-escalar definida por

$$rm = (r1_G)m, \qquad r \in R,\ m \in M,$$

e N é um R-submódulo de M. Sendo assim, como R é semisimples, o Teorema 2.1.13 garante que N é parcela directa de M, isto é, existe $N' \leq_R M$ tal que

$$M = N \oplus N'.$$

Consideremos a projecção natural $\pi\colon M \to N$; é claro que π é um R-epimorfismo tal que $\pi(n) = n$ para todo $n \in \mathbb{N}$.

Posto isto, definimos a aplicação $\theta\colon M \to M$ por

$$\theta(m) = |G|^{-1} \sum_{g \in G} g^{-1}\pi(gm), \qquad m \in M.$$

É fácil verificar que θ é um R-homomorfismo(†) tal que $\theta(M) \subseteq N$ (porque $\pi(gm) \in N$ para todo $g \in G$ e todo $m \in M$). Como $N \leq_{RG} M$, temos

$$\theta(n) = |G|^{-1} \sum_{g \in G} g^{-1}\pi(gn) = |G|^{-1} \sum_{g \in G} g^{-1}(gn) = |G|^{-1}|G|n = n, \qquad n \in N;$$

notemos que $g^{-1}(gn) = 1_G n = n$ para todo $n \in N$. Por outro lado, para qualquer $g \in G$ e qualquer $m \in M$, temos

$$\theta(gm) = |G|^{-1} \sum_{h \in G} h^{-1}\pi(h(gm)) = |G|^{-1} \sum_{k \in G} g(hg)^{-1}\pi((hg)m)$$

(*)Uma vez que não há perigo de ambiguidade, identificamos qualquer $n \in \mathbb{Z}$ com o elemento $n \cdot 1_R \in R$; notemos, no entanto, que pode acontecer $n = 0$ em R.

(†)Na prova da R-linearidade, é necessário observar que

$$g(rm) = r(gm), \qquad g \in G,\ r \in R,\ m \in M.$$

Para isto, basta observar que, pela definição da multiplicação em RG, se tem

$$g(r1_G) = (r1_G)g = rg, \qquad g \in G,\ r \in R,$$

e recordar que $rm = (r1_G)m$ para todo $r \in R$ e $m \in M$.

$$= |G|^{-1} \sum_{k \in G} g k^{-1} \pi(km) = g\left(|G|^{-1} \sum_{k \in G} k^{-1} \pi(km)\right) = g\theta(m).$$

Por conseguinte, θ é RG-homomorfismo.

Finalmente, provemos que

$$M \cong_{RG} N \oplus \ker(\theta);$$

recordemos que, como θ é RG-homomorfismo, $\ker(\theta)$ é um RG-submódulo de M. Para qualquer $m \in M$, temos $\theta(m) \in N$, logo $\theta(\theta(m)) = \theta(m)$ e, portanto,

$$\theta(m - \theta(m)) = \theta(m) - \theta(\theta(m)) = 0,$$

isto é, $m - \theta(m) \in \ker(\theta)$. Segue-se que

$$m = \theta(m) + (m - \theta(m)) \in N + \ker(\theta), \qquad m \in M,$$

logo

$$M = N + \ker(\theta).$$

Por outro lado, se $n \in N \cap \ker(\theta)$, então $n = \theta(n) = 0$ e, portanto,

$$N \cap \ker(\theta) = \{0\}.$$

Sendo assim, $M \cong_{RG} N \oplus \ker(\theta)$, o que prova que N é parcela directa de M.

$(\Rightarrow)$ Supomos que o anel RG é semisimples (à esquerda), com vista a provar que o anel R é semisimples (à esquerda) e que $|G| = |G| \cdot 1_R \in R^\times$. Para isso, consideramos a aplicação $\varepsilon \colon RG \to R$ definida por

$$\varepsilon\left(\sum_{g \in G} r_g g\right) = \sum_{g \in G} r_g, \qquad r_g \in R \ (g \in G);$$

notemos que ε é a extensão R-linear da aplicação $\varepsilon \colon G \to R$ definida por $\varepsilon(g) = 1_R$ para todo $g \in G$ (pelo que $\varepsilon(r1_G) = r$ para todo $r \in R$). Não é difícil verificar que ε é um homomorfismo de anéis, de maneira que $\mathcal{A}_R(G) = \ker(\varepsilon)$ é um ideal bilateral de $RG^{(*)}$; além disso, tem-se $\mathcal{A}_R(G) \neq RG$ (por exemplo, $1_G \notin \mathfrak{I}$). Como $R = \varepsilon(RG)$, tem-se

$$_R R \cong_R RG/\mathcal{A}_R(G),$$

de modo que $_R R$ é um R-módulo semisimples (pelo Lema 2.1.5) e, portanto, R é anel semisimples (à esquerda).

Notemos que

$$RG/\mathcal{A}_R(G) = \{r1_R + \mathcal{A}_R(G) \colon r \in R\}$$

e que a multiplicação RG-escalar no R-módulo quociente $RG/\mathcal{A}_R(G)$ é univovamente determinada por

$$g(r1_G + \mathcal{A}_R(G)) = g(r1_G) + \mathcal{A}_R(G) = rg + \mathcal{A}_R(G), \qquad g \in G, \ r \in R;$$

(*) Ao ideal bilateral $\mathcal{A}_R(G)$ chamamos o *ideal de aumentação* de RG.

além disso, como $\varepsilon(rg - r1_G) = 0$ temos $rg - r1_G \in \mathcal{A}_R(G)$, logo

$$g(r1_G + \mathcal{A}_R(G)) = rg + \mathcal{A}_R(G) = r1_G + \mathcal{A}_R(G), \qquad g \in G,\ r \in R.^{(*)}$$

Como $\mathcal{A}_R(G)$ é um ideal esquerdo de RG e RG é semisimples, existe um ideal esquerdo $\mathcal{L}$ de RG tal que

$$RG = \mathcal{L} \oplus \mathcal{A}_R(G),$$

de modo que existe um RG-isomorfismo $\theta\colon \mathcal{L} \to RG/\mathcal{A}_R(G)$. Para qualquer $g \in G$ e qualquer $a \in \mathcal{L}$, temos $\theta(ga) = g\theta(a) = \theta(a)$, de modo que $ga = a$ (porque θ é injectivo); por conseguinte, para qualquer $z \in RG$ e qualquer $a \in \mathcal{L}$, deduzimos que

$$za = \sum_{g\in G} r_g(ga) = \sum_{g\in G} r_g a = \left(\sum_{g\in G} r_g\right)a = \varepsilon(z)a,$$

onde $r_g \in R$, para $g \in G$, são tais que $z = \sum_{g\in G} r_g g$.

Agora, sejam $e \in \mathcal{L}$ e $e' \in \mathcal{A}_R(G)$ tais que

$$1_G = e + e';$$

é fácil verificar que $e^2 = e$ e que $\mathcal{L} = RGe$. Pelo que acabámos de provar, temos

$$ge = \varepsilon(g)e = e, \qquad g \in G.$$

Pondo

$$e = \sum_{h\in G} r_h h, \qquad r_h \in R\ (h \in G),$$

deduzimos que

$$\sum_{h\in G} r_h h = e = ge = \sum_{h\in G} r_h gh = \sum_{k\in G} r_{g^{-1}k} k, \qquad g \in G,$$

pelo que

$$r_{g^{-1}h} = r_h, \qquad g, h \in G.$$

Em particular,

$$r_g = r_{g^{-1}g} = r_{1_G}, \qquad g \in G,$$

de modo que

$$e = r\sum_{g\in G} g$$

onde $r = r_{1_G} \in R$. Finalmente, como $1_G - e = e' \in \mathcal{A}_R(G) = \ker(\varepsilon)$, temos

$$0 = \varepsilon(1_G - e) = \varepsilon(1_G) - \varepsilon(e) = 1 - r\varepsilon\left(\sum_{g\in G} g\right) = 1 - r|G|$$

e, portanto, $r|G| = 1$, provando que $|G|$ é invertível (porque $r|G| = |G|r$). $\square$

$^{(*)}$Sendo assim, tendo em conta o isomorfismo ${}_RR \cong_R RG/\mathcal{A}_R(G)$, podemos definir em R uma estrutura de RG-módulo em que

$$g \cdot r = r, \qquad g \in G,\ r \in R.$$

2.1.15. Teorema. *Se R é um anel semisimples (à esquerda), então qualquer R-módulo simples é R-isomorfo a um ideal esquerdo minimal de R.*

Demonstração. Seja M um R-módulo simples. Então, pela Proposição 2.1.2 existe $0 \neq m \in M$ tal que $M = Rm$ e, portanto,

$$M \cong_R R/\operatorname{Ann}_R(m);$$

além disso, $\operatorname{Ann}_R(m)$ é um ideal esquerdo maximal de R (pela Proposição 2.1.3). Como R é semisimples, existe um ideal esquerdo $\mathcal{L}$ de R tal que

$$R = \operatorname{Ann}_R(m) \oplus \mathcal{L};$$

recordemos que os submódulos do R-módulo regular ${}_RR$ são exactamente os ideais esquerdos do anel R. Daqui, resulta que

$$\mathcal{L} \cong_R R/\operatorname{Ann}_R(m) \cong_R M,$$

pelo que $\mathcal{L}$ é um R-submódulo simples de R (porque M é simples) e, portanto, um ideal esquerdo minimal de R. □

2.1.16. Se $\{M_i \colon i \in I\}$ é uma família de R-módulos simples, dizemos que $\{M_i \colon i \in I\}$ é um *conjunto básico de R-módulos simples* se:

- Para quaisquer $i, j \in I$, $M_i \cong_R M_j$ se e só se $i = j$.
- Para qualquer R-módulo simples M, existe $i \in I$ tal que $M \cong_R M_i$.

Por outras palavras, $\{M_i \colon i \in I\}$ é um conjunto completo de representantes das classes de isomorfismo dos R-módulos simples.

2.1.17. Corolário. *Seja R um anel semisimples (à esquerda). Então, existe apenas um número finito de classes de isomorfismo dos R-módulos simples. Além disso, se $\{M_1, \dots, M_t\}$ é um conjunto básico de R-módulos simples, então*

$${}_RR \cong_R M_1^{(n_1)} \dotplus \cdots \dotplus M_t^{(n_t)}$$

onde $n_1, \dots, n_t \in \mathbb{N}$ são inteiros univocamente determinados.

Demonstração. A primeira afirmação e a existência da decomposição ${}_RR \cong_R M_1^{(n_1)} \dotplus \cdots \dotplus M_t^{(n_t)}$ são consequências imediatas do Teorema 2.1.15 e da Proposição 2.1.11. A unicidade dos inteiros $n_1, \dots, n_t$ resulta do Teorema de Jordan-Hölder (ou do Teorema de Krull-Schmidt (tendo em conta o Corolário 2.1.12)). □

2.1.18. Proposição. *Sejam R um anel semisimples (à esquerda) e $\mathcal{L}$ um ideal esquerdo não-nulo de R. Então, $\mathcal{L} = Re$ para algum idempotente $e \in R$. Além disso, para qualquer homomorfismo $\varphi \in \operatorname{Hom}_R(\mathcal{L}, R)$, existe $a \in R$ tal que $\varphi(x) = xa$ para todo $x \in \mathcal{L}$.*

Demonstração. Como R é semisimples, existe um ideal esquerdo $\mathcal{L}'$ de R tal que

$$R = \mathcal{L} \oplus \mathcal{L}'$$

e, portanto, existem $e \in \mathcal{L}$ e $e' \in \mathcal{L}'$ tais que

$$1 = e + e'.$$

Então, $e = e^2 + ee'$, de modo que

$$e - e^2 = ee' \in \mathcal{L} \cap \mathcal{L}' = \{0\}.$$

Segue-se que $e^2 = e$. Analogamente, como $x = xe + xe'$, obtemos

$$x - xe = xe' \in \mathcal{L} \cap \mathcal{L}' = \{0\}, \qquad x \in \mathcal{L},$$

logo

$$x = xe, \qquad x \in \mathcal{L}.$$

Segue-se que $\mathcal{L} \subseteq \mathcal{L}e \subseteq Re \subseteq \mathcal{L}$ e, portanto, $\mathcal{L} = Re$.

Por outro lado, seja $\varphi \in \mathrm{Hom}_R(\mathcal{L}, R)$ e seja $a = \varphi(e)$. Como $x = xe$ para qualquer $x \in \mathcal{L}$, deduzimos que

$$\varphi(x) = \varphi(xe) = x\varphi(e) = xa, \qquad x \in \mathcal{L},$$

como se pretende. $\square$

2.1.19. Proposição. *Seja $e \in R$ um idempotente (sendo R um anel arbitrário). Então, existe um isomorfismo de anéis*

$$\mathrm{End}_R(Re) \cong (eRe)^{\mathrm{op}};$$

em particular, o ideal esquerdo Re é minimal se e só se eRe é um anel de divisão.

Demonstração. Em primeiro lugar, observamos que eRe é um anel com identidade e (exercício). Definamos $\Theta\colon \mathrm{End}_R(Re) \to eRe$ por

$$\Theta(\varphi) = e\varphi(e)e, \qquad \varphi \in \mathrm{End}_R(Re).$$

Não é difícil verificar que Θ é um anti-homomorfismo de anéis e, portanto, a correspondência

$$\varphi \mapsto \Theta(\varphi)^{\mathrm{op}} = (e\varphi(e)e)^{\mathrm{op}}$$

define um homomorfismo de anéis $\Theta^{\mathrm{op}}\colon \mathrm{End}_R(Re) \to (eRe)^{\mathrm{op}}$.

Para provar que Θ^{op} é injectivo, seja $\varphi \in \mathrm{End}_R(Re)$ tal que $\Theta(\varphi)^{\mathrm{op}} = 0$. Então, $\Theta(\varphi) = 0$ e, portanto,

$$\varphi(e)e = \varphi(e^2)e = e\varphi(e)e = 0.$$

Como $\varphi(e) \in Re$ e $xe = x$ para todo $x \in Re$, concluímos que $\varphi(e) = \varphi(e)e = 0$ e, portanto,

$$\varphi(x) = x\varphi(e) = 0, \qquad x \in Re.$$

Por outro lado, provemos que Θ^{op} é sobrejectivo. Seja $a \in eRe$ arbitrário. Então,

$$eae = ea = ae = a$$

e, portanto, a correspondência $x \mapsto xa$ define uma aplicação $\varphi\colon Re \to Re$ (porque $x = xe$ para todo $x \in Re$). É óbvio que $\varphi \in \mathrm{End}_R(Re)$ e que $\varphi(e) = a$. Sendo assim,

$$\Theta(\varphi) = e\varphi(e)e = eae = a,$$

logo $\Theta^{\mathrm{op}}(\varphi) = \Theta(\varphi)^{\mathrm{op}} = a^{\mathrm{op}}$.

Segue-se que Θ^{op} é um isomorfismo de anéis.

A última asserção é consequência do Lema de Schur: se Re é simples, então $\mathrm{End}_R(Re)$ é um anel de divisão e, portanto, $(eRe)^{\mathrm{op}}$ e eRe também são anéis de divisão. □

2.1.20. Corolário. *A correspondência $\varphi \mapsto \varphi(1)^{\mathrm{op}}$ define um isomorfismo de anéis*

$$\mathrm{End}_R({}_RR) \cong R^{\mathrm{op}}.$$

Demonstração. Basta considerar $e = 1$ na proposição anterior. □

2.2. Componentes homogéneas e componentes de Wedderburn

2.2.1. Seja $\{M_i \colon i \in I\}$ um conjunto básico de R-módulos simples (em que R é um anel arbitrário). Se M é um R-modulo semisimples, definimos as *componentes homogéneas* (ou, *componentes isotípicas*) de M como sendo os submódulos

$$H_i = H_i(M) = \sum_{\substack{N \leq_R M \\ N \cong_R M_i}} N, \qquad i \in I;$$

para cada $i \in I$, referimo-nos a $H_i = H_i(M)$ como sendo a *componente homogénea (ou, isotípica) de tipo M_i.*

2.2.2. Teorema. *Seja M um R-módulo semisimples (em que R é um anel arbitrário), seja $\{M_i \colon i \in I\}$ um conjunto básico de R-módulos simples e sejam $H_i = H_i(M)$, $i \in I$, as componentes homogéneas de M. Então:*

(a) $M = \bigoplus_{i \in I} H_i$.

(b) *Para qualquer submódulo simples $N \leq_R M$ e qualquer $i \in I$, tem-se $N \cong_R M_i$ se e só se $N \subseteq H_i$.*

(c) $\mathrm{Hom}_R(H_i, H_{i'}) = \{0\}$ *para quaisquer $i, i' \in I$, $i \neq i'$.*

(d) *Se $\{N_j \colon j \in J\}$ é um conjunto de submódulos simples de M tais que $M = \bigoplus_{j \in J} N_j$, então*

$$H_i = \sum_{\substack{j \in J \\ N_j \cong_R M_i}} N_j, \qquad i \in I.$$

Demonstração. Como M é semisimples, existe uma decomposição

$$M = \bigoplus_{j \in J} N_j$$

como em (d); sejam $\pi_j \colon M \to M$, $j \in J$, as projecções associadas a esta decomposição (de modo que $\pi_j(M) = N_j$ para todo $j \in J$.

Provemos que qualquer submódulo simples $N \leq_R M$ é isomorfo a N_j para algum $j \in J$. Ora, se $0 \neq n \in N$, então

$$n = \sum_{j \in J} \pi_j(n)$$

onde $J' = \{j \in J \colon \pi_j(n) \neq 0\}$ é um conjunto finito; além disso, $J' \neq \emptyset$ (porque $n \neq 0$). Sendo assim, existe $j \in J$ tal que $\pi_j(n) \neq 0$ e, portanto, $\pi_j(N) \neq 0$. Segue-se que a restrição $(\pi_j)_N$ de π_j a N define um homomorfismo não-nulo $(\pi_j)_N \colon N \to N_j$, pelo que

$$\mathrm{Hom}_R(N, N_j) \neq \{0\}.$$

Como N e N_j são R-módulos simples, o Lema de Schur garante que $N \cong_R N_j$.

Agora, para cada $i \in I$, definimos

$$\tilde{H}_i = \sum_{\substack{j \in J \\ N_j \cong_R M_i}} N_j;$$

notemos que, pela definição de H_i, se tem $\tilde{H}_i \subseteq H_i$ para todo $i \in I$. Pela definição de soma directa, é fácil verificar que

$$M = \bigoplus_{i \in I} \tilde{H}_i.$$

Por outro lado, para cada $i \in I$, existe um subconjunto $J' \subseteq J$ tal que

$$\tilde{H}_i = \bigoplus_{\substack{j' \in J' \\ N_{j'} \cong_R M_i}} N_{j'}$$

(pelo Lema 2.1.7) e, portanto, pelo que vimos no parágrafo anterior, qualquer submódulo simples de $\tilde{H}_i$ é isomorfo a $N_{j'}$ para algum $j' \in J'$.

Seja $N \leq_R M$ um submódulo simples e seja $i \in I$ tal que $N \cong_R M_i$. Provamos que $N \subseteq \tilde{H}_i$, de onde resulta que $H_i \subseteq \tilde{H}_i$ e, portanto que $H_i = \tilde{H}_i$. Para isso, seja $n \in N$ e escrevamos

$$n = \sum_{j \in J} \pi_j(n)$$

onde $\{j \in J \colon \pi_j(n) \neq 0\}$ é finito. Se $j \in J$ é tal que $\pi_j(n) \neq 0$, então $M_i \cong_R N \cong_R N_j$ (como provámos acima). Daqui resulta que $\pi_j(n) = 0$ sempre que $j \in J$ é tal que $N_j \not\cong_R M_i$ e, portanto,

$$n = \sum_{\substack{j \in J \\ N_j \cong_R M_i}} \pi_j(n) \in \sum_{\substack{j \in J \\ N_j \cong_R M_i}} N_j = \tilde{H}_i.$$

Nesta ponto, provámos que $H_i = \tilde{H}_i$ para todo $i \in I$, como afirmamos em (d). Provámos também que

$$M = \bigoplus_{i \in I} \tilde{H}_i$$

(logo (a) é verdadeira) e que, para qualquer $i \in I$ e qualquer submódulo $N \leq_R M$, se tem

$$N \cong_R M_i \quad \Longleftrightarrow \quad N \subseteq \tilde{H}_i = H_i$$

(o que prova (b)). Assim, para terminar a demonstração, falta justificar que

$$\mathrm{Hom}_R(H_i, H_{i'}) = \{0\}, \qquad i, i' \in I,\ i \neq i'.$$

Sejam $i, i' \in I$ e suponhamos que existe $0 \neq \varphi \in \mathrm{Hom}_R(H_i, H_{i'})$. Então, existe um submódulo simples $N \leq_R H_i$ tal que $\varphi(N) \neq \{0\}$. Deste modo, $\varphi(N)$ é um submódulo simples de $H_{i'}$, logo $\varphi(N) \cong_R M_{i'}$ (por (b)). Como $N \cong_R \varphi(N)$ (porque N é simples), concluímos que $N \subseteq H_{i'}$ (de novo, por (b)) e, portanto, tem de ser $i = i'$ (caso contrário, $H_i \cap H_{i'} = \{0\}$, o que contraria (a)). □

2.2.3. Suponhamos que R é um anel semisimples (à esquerda). Pelo Corolário 2.1.17, sabemos que existe um número finito de classes de isomorfismo dos R-módulos simples. Por conseguinte, o R-módulo regular ${}_RR$ tem um número finito de componentes homogéneas; de facto, se $\{M_1, \ldots, M_t\}$ é um conjunto básico de R-módulos simples, então as componentes homogéneas de ${}_RR$ são definidas por

$$\mathcal{B}_i = \sum_{\substack{\mathcal{L} \trianglelefteq_{\mathrm{esq}} R \\ \mathcal{L} \cong_R M_i}} \mathcal{L}, \qquad 1 \leq i \leq t.$$

Às componentes homogéneas $\mathcal{B}_1, \ldots, \mathcal{B}_t$ de ${}_RR$ chamamos as *componentes de Wedderburn* de R.

2.2.4. Lema. *Se R é um anel semisimples (à esquerda) e $\mathcal{B}_1, \ldots, \mathcal{B}_t$ são as componentes de Wedderburn de R, então*

$$R = \mathcal{B}_1 \oplus \cdots \oplus \mathcal{B}_t.$$

Demonstração. É consequência imediata do Teorema 2.2.2. □

2.2.5. Lema. *Se R é um anel semisimples e $\mathcal{B}_1, \ldots, \mathcal{B}_t$ são as componentes de Wedderburn de R, então $\mathcal{B}_1, \ldots, \mathcal{B}_t$ são ideais bilaterais de R tais que*

$$\mathcal{B}_i\mathcal{B}_j = 0, \qquad 1 \leq i \neq j \leq t.$$

Além disso, existem idempotentes centrais(*) $e_1, \ldots, e_t \in R$ *tais que:*

(a) $1 = e_1 + \cdots + e_n$.

(b) $e_1, \ldots, e_n$ *são ortogonais dois-a-dois.*

(c) *Para qualquer* $1 \leq i \leq n$, $\mathcal{B}_i = e_iRe_i$ *é um anel com identidade* e_i.

(*) Um idempotente $e \in R$ diz-se *central* se $ea = ae$ para todo $a \in R$, isto é, se $e \in Z(R)$.

Demonstração. Seja $1 \leq i, j \leq t$ quaisquer e consideremos a componentes de Wedderburn $\mathcal{B}_i$ e $\mathcal{B}_j$ (possivelmente, $\mathcal{B}_i = \mathcal{B}_j$). Seja $\mathcal{L}$ um ideal esquerdo minimal de R tal que $\mathcal{L} \subseteq \mathcal{B}_i$ e seja $a \in \mathcal{B}_j$. Como $\mathcal{B}_j$ é um ideal esquerdo de R (porque é uma soma de ideais esquerdos), tem-se

$$\mathcal{L}a \subseteq Ra \subseteq \mathcal{B}_j.$$

Como a correspondência $x \mapsto xa$, $x \in \mathcal{L}$, define um R-homomorfismo $a_{\mathrm{R}} \colon \mathcal{L} \to \mathcal{L}a$ e, como $\mathcal{L}$ é um R-módulo simples, concluímos que $\mathcal{L}a = \{0\}$ ou $\mathcal{L}a \cong_R \mathcal{L}$. Em qualquer dos casos, temos $\mathcal{L}a \subseteq \mathcal{B}_i$ (se $\mathcal{L}a \cong_R \mathcal{L}$, usamos o Teorema 2.2.2(b)), de maneira que

$$\mathcal{L}\mathcal{B}_j \subseteq \mathcal{B}_i.$$

Como $R = \mathcal{B}_1 \oplus \cdots \oplus \mathcal{B}_t$, concluímos que

$$\mathcal{L}R \subseteq \mathcal{L}\mathcal{B}_1 + \cdots + \mathcal{L}\mathcal{B}_t \subseteq \mathcal{B}_i$$

e, portanto,

$$\mathcal{B}_i R \subseteq \mathcal{B}_i$$

(pela definição de $\mathcal{B}_i$).

Por outro lado, se $i \neq j$, então

$$\mathcal{L}a \subseteq \mathcal{B}_i \cap \mathcal{B}_j = \{0\}.$$

Daqui resulta que $\mathcal{L}\mathcal{B}_j = \{0\}$ e, portanto,

$$\mathcal{B}_i\mathcal{B}_j = \{0\},$$

como se queria.

Finalmente, pondo $1 = e_1 + \cdots + e_n$ onde $e_i \in \mathcal{B}_i$ para $1 \leq i \leq t$, verificamos que

$$e_i e_j \in \mathcal{B}_i\mathcal{B}_j = 0, \qquad 1 \leq i \neq j \leq t,$$

e que

$$e_i = e_i \cdot 1 = e_i e_1 + \cdots + e_i e_t = e_i^2, \qquad 1 \leq i \leq t.$$

Por outro lado, para qualquer $a \in \mathcal{B}_i$, tem-se

$$a = ae_1 + \cdots + ae_t = ae_i \qquad \text{e} \qquad a = e_1 a + \cdots + e_t a = e_i a$$

e, portanto,

$$\mathcal{B}_i = Re_i = e_i R = e_i R e_i, \qquad 1 \leq i \leq t.$$

A demonstração está completa. □

O resultado que se segue garante que as componentes de Wedderburn são univocamente determinadas pela decomposição de R como soma directa de ideais bilaterais.

2.2.6. Lema. *Seja R é um anel arbitrário tal que*

$$R = \mathcal{B}_1 \oplus \cdots \oplus \mathcal{B}_m = \mathcal{B}'_1 \oplus \cdots \oplus \mathcal{B}'_n$$

onde $\mathcal{B}_1, \ldots, \mathcal{B}_m$ e $\mathcal{B}'_1, \ldots, \mathcal{B}'_n$ são ideais bilaterais não-nulos de R. Se $\mathcal{B}_1, \ldots, \mathcal{B}_m$ e $\mathcal{B}'_1, \ldots, \mathcal{B}'_n$ são indecomponíveis(*)*, então $m = n$ e $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\} = \{\mathcal{B}'_1, \ldots, \mathcal{B}'_m\}$.*

Demonstração. Escrevendo $1 = e_1 + \cdots + e_m$ onde $e_i \in \mathcal{B}_i$ para $1 \le i \le m$, verificamos que $\mathcal{B}_1, \ldots, \mathcal{B}_m$ são anéis com identidades $e_1, \ldots, e_m$, respectivamente; além disso, existe um isomorfismo de anéis $\varphi \colon R \to \mathcal{B}_1 \times \cdots \times \mathcal{B}_m$.

Consideremos o ideal bilateral $\mathcal{B}'_1$ de R. Como $\varphi(\mathcal{B}'_1)$ é um ideal bilateral de $\mathcal{B}_1 \times \cdots \times \mathcal{B}_m$, temos $\varphi(\mathcal{B}'_1) = \mathcal{I}_1 \times \cdots \times \mathcal{I}_m$ onde, para cada $1 \le i \le m$, $\mathcal{I}_i$ é um ideal bilateral de $\mathcal{B}_i$. Como

$$\varphi(\mathcal{I}_1 + \cdots + \mathcal{I}_m) = \mathcal{I}_1 \times \cdots \times \mathcal{I}_m,$$

concluímos que

$$\mathcal{B}'_1 = \mathcal{I}_1 \oplus \cdots \oplus \mathcal{I}_m.$$

Como $\mathcal{B}'_1$ é um ideal indecomponível, só um dos ideais $\mathcal{I}_1, \ldots, \mathcal{I}_m$ pode ser não-nulo. Sem perda de generalidade, podemos admitir que $\mathcal{I}_2 = \ldots = \mathcal{I}_m = 0$, pelo que

$$\mathcal{B}'_1 = \mathcal{I}_1 \subseteq \mathcal{B}_1.$$

Analogamente, provamos que $\mathcal{B}_1 \subseteq \mathcal{B}'_j$ para algum $1 \le j \le n$, logo

$$\mathcal{B}'_1 \subseteq \mathcal{B}_1 \subseteq \mathcal{B}'_j$$

e, portanto, tem de ser $j = 1$ (porque $R = \mathcal{B}'_1 \oplus \cdots \oplus \mathcal{B}'_n$), de modo que $\mathcal{B}'_1 = \mathcal{B}_1$.

O resultado segue-se (basta aplicar o mesmo argumento a cada um dos ideais restantes). □

2.2.7. Dizemos que R é um *anel simples* se $\{0\}$ e R são os únicos ideais (bilaterais) de R; mais tarde, veremos que esta noção é equivalente a exigir que o R-módulo regular, tanto esquerdo, como direito, é um R-módulo simples.

Como exemplo, é claro que *qualquer anel de divisão é um anel simples*: se D é um anel de divisão e $\{0\} \neq \mathcal{B} \trianglelefteq D$, então existe $0 \neq b \in \mathcal{B}$, logo $1 = b^{-1}b \in \mathcal{B}$ e, portanto, $\mathcal{B} = D$.

2.2.8. Lema. *Se R é um anel simples e $n \in \mathbb{N}$, então $\mathbb{M}_n(R)$ também é um anel simples.*

Demonstração. Basta aplicar a Proposição 1.1.21. □

2.2.9. Proposição. *Se R é um anel simples artiniano à esquerda, então R é semisimples (à esquerda).*

(*) Um ideal bilateral de R diz-se *indecomponível* se não é soma directa de dois ideais bilaterais não-nulos de R.

Demonstração. Como R é artiniano, o conjunto de todos os ideais esquerdos não-nulos de R tem (pelo menos) um elemento minimal (pelo Lema de Zorn), isto é, R tem pelo menos um ideal esquerdo minimal $\mathcal{L}$. Então,

$$\mathcal{B} = \sum_{a \in R} \mathcal{L}a$$

é um ideal bilateral de R e, portanto, $\mathcal{B} = R$ (porque R é simples e $\{0\} \neq \mathcal{L} \subseteq \mathcal{B}$). Se $a \in R$ é tal que $\mathcal{L}a \neq 0$, então $\mathcal{L}a \cong_R \mathcal{L}$ e, portanto, $\mathcal{L}a$ é um submódulo simples de ${}_RR$ (porque $\mathcal{L}$ é um submódulo simples de ${}_RR$). Por conseguinte,

$${}_RR = \sum_{a \in R} \mathcal{L}a$$

é uma soma de submódulos simples e, portanto, é semisimples. $\square$

2.2.10. LEMA. *Se R é um anel semisimples (à esquerda) e $\mathcal{B}_1, \ldots, \mathcal{B}_t$ são as componentes de Wedderburn de R, então $\mathcal{B}_1, \ldots, \mathcal{B}_t$ são anéis simples e, além disso, são anéis noetherianos à esquerda e anéis artinianos à esquerda.*

Demonstração. Seja $1 \leq i \leq t$ e seja $\{0\} \neq \mathcal{B} \trianglelefteq \mathcal{B}_i$. Como $\mathcal{B}_i \trianglelefteq R$ e $\mathcal{B}_i\mathcal{B}_j = \{0\}$ para $1 \leq j \neq i \leq t$, é claro que $\mathcal{B} \trianglelefteq R$. De facto, como

$$\mathcal{B}\mathcal{B}_j \subseteq \mathcal{B}_i\mathcal{B}_j = \{0\}, \qquad 1 \leq j \neq i \leq t,$$

obtemos

$$\mathcal{B}R = \mathcal{B}(\mathcal{B}_1 + \cdots + \mathcal{B}_t) = \mathcal{B}\mathcal{B}_i \subseteq \mathcal{B}.$$

Analogamente, $R\mathcal{B} \subseteq \mathcal{B}$.

Seja $\mathcal{L}$ e $\mathcal{L}'$ ideais esquerdos minimais de R tais que $\mathcal{L} \subseteq \mathcal{B}$ e $\mathcal{L}' \subseteq \mathcal{B}_i$. Como $\mathcal{B} \subseteq \mathcal{B}_i$, temos $\mathcal{L} \subseteq \mathcal{B}_i$ e, portanto, $\mathcal{L} \cong_R \mathcal{L}'$. Se $\varphi\colon \mathcal{L} \to \mathcal{L}'$ é um R-isomorfismo, então φ pode ser considerado um R-homomorfismo $\varphi\colon \mathcal{L} \to R$ (porque $\mathcal{L}' \subseteq R$) e, portanto, pela Proposição 2.1.18, existe $a \in R$ tal que

$$\varphi(x) = xa, \qquad x \in \mathcal{L}.$$

Sendo assim,

$$\mathcal{L}' = \varphi(\mathcal{L}) = \mathcal{L}a \subseteq \mathcal{B}$$

(porque $\mathcal{B} \trianglelefteq R$). Pela definição de $\mathcal{B}_i$, concluímos que $\mathcal{B} = \mathcal{B}_i$ e, portanto, $\mathcal{B}_i$ é um anel simples.

Como R é soma finita de ideais esquerdos minimais, também $\mathcal{B}_i$ é uma soma finita de ideais esquerdos minimais. Como qualquer ideal esquerdo de R é um submódulo simples de ${}_RR$, concluímos que o R-módulo esquerdo $\mathcal{B}_i$ é uma soma finita de submódulos simples e, portanto, $\mathcal{B}_i$ admite uma série de composição, o que prova que $\mathcal{B}_i$ é um anel noetheriano à esquerda e um anel artiniano à esquerda (pelo Teorema 1.4.15). $\square$

2.3. Teorema de Wedderburn-Artin

2.3.1. LEMA. *Se D é um anel de divisão e M é um D-módulo de dimensão finita, então existe um isomorfismo de anéis*

$$\mathrm{End}_D(M) \cong \mathbb{M}_n(D)$$

onde $n = \dim_D M$.

Demonstração. Seja $\{m_1, \ldots, m_n\}$ uma base de M; recordemos que, como D é anel de divisão, qualquer D-módulo é livre. Para cada $A \in \mathbb{M}_D(M)$, em que $A = [a_{i,j}]_{1 \leq i,j \leq n}$, definimos $\varphi_A \colon M \to M$ por

$$\varphi_A(m_i) = \sum_{1 \leq j \leq n} a_{i,j} m_j, \qquad 1 \leq i \leq n.$$

É fácil justificar que a correspondência $A \mapsto \varphi_A$ define um anti-isomorfismo de anéis

$$\varphi \colon M_n(D) \to \mathrm{End}_D(M)$$

em que $\varphi(A) = \varphi_A$ para todo $A \in \mathbb{M}_n(D)$; a título de exemplo, para quaisquer $A, B \in \mathbb{M}_n(D)$, em que $A = [a_{i,j}]_{1 \leq i,j \leq n}$ e $B = [b_{i,j}]_{1 \leq i,j \leq n}$, tem-se

$$\begin{aligned}(\varphi_B \varphi_A)(m_i) = \varphi_B\big(\varphi_A(m_i)\big) &= \sum_{1 \leq j \leq n} a_{i,j} \varphi_B(m_j) = \sum_{1 \leq j \leq n} \sum_{1 \leq k \leq n} a_{i,j} b_{j,k} m_k \\ &= \sum_{1 \leq k \leq n} \Bigg(\sum_{1 \leq j \leq n} a_{i,j} b_{j,k} \Bigg) m_k = \varphi_{AB}(m_i)\end{aligned}$$

para todo $1 \leq i \leq n$, de maneira que $\varphi_{AB} = \varphi_B \varphi_A$, ou seja, $\varphi(AB) = \varphi(B)\varphi(A)$.

Para terminar a demonstração, basta definir $\psi \colon \mathbb{M}_n(D) \to \mathrm{End}_D(M)$ por

$$\psi(A) = \varphi(A^T), \qquad A \in \mathbb{M}_n(D),$$

onde, para cada $A \in \mathbb{M}_n(D)$, denotamos por A^T a matriz transposta de A.(*) □

2.3.2. PROPOSIÇÃO. *Sejam D um anel de divisão e $R = \mathbb{M}_n(D)$ para algum $n \in \mathbb{N}$. Para cada $1 \leq i \leq n$, seja $\mathcal{L}_i$ o conjunto de todas as matrizes em R que têm todas as entradas nulas excepto as da i-ésima coluna. Então:*

(a) *$\mathcal{L}_1, \ldots, \mathcal{L}_n$ são ideais esquerdos minimals de R tais que*

$$R = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_n;$$

em particular, R é um anel semisimples (à esquerda).

(b) *A menos de isomorfismo, existe um e um só R-módulo simples M.*

(*) Podemos considerar $A^{\mathrm{op}} = A^T$ para qualquer $A \in \mathbb{M}_n(D)$, de modo que a multiplicação do anel $\mathbb{M}_n(D)^{\mathrm{op}} = \{A^T \colon A \in \mathbb{M}_n(D)\}$ é definida por

$$A \cdot B = (BA)^T = A^T B^T, \qquad A, B \in \mathbb{M}_n(D).$$

(c) *Existe um R-isomorfismo*

$$_R R \cong_R M^{(n)}.$$

(d) *Existe um isomorfismo de anéis*

$$D \cong \mathrm{End}_R(M)^{\mathrm{op}}.$$

Demonstração. (a) Seja $\{e_{i,j} \colon 1 \leq i, j \leq n\}$ a base canónica de $R = \mathbb{M}_n(D)$. Para qualquer $1 \leq i \leq n$, tem-se $\mathcal{L}_i = Re_{i,i}$ de modo que $\mathcal{L}_i$ é ideal esquerdo de R. É fácil justificar que $\mathcal{L}_i$ é minimal e que $R = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_n$.

(b) Qualquer R-módulo simples é isomorfo a $\mathcal{L}_i$ para algum $1 \leq i \leq n$ (pelo Teorema 2.1.15). Como $\mathcal{L}_i \cong_R D^{(n)}$ para qualquer $1 \leq i \leq n$, concluímos que $\mathcal{L}_i \cong_R \mathcal{L}_j$ para todos $1 \leq i, j \leq n$, o que prova que (b).

(c) Tem-se $R = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_n \cong_R M^{(n)}$ onde $M = D^{(n)}$.

(d) Como $M \cong_R \mathcal{L}_1 = Re_{1,1}$ e como $e_{1,1} \in R$ é idempotente, existem isomorfismos de anéis

$$\mathrm{End}_R(M) \cong \mathrm{End}_R(Re_{1,1}) \cong (e_{1,1}Re_{1,1})^{\mathrm{op}}$$

(pelo Corolário 2.1.20). Como

$$e_{1,1}Re_{1,1} = \{\alpha e_{1,1} \colon \alpha \in D\},$$

é claro que $e_{1,1}Re_{1,1} \cong D$ (como anéis). □

2.3.3. Proposição. *Suponhamos que R é um anel simples, seja $0 \neq e \in R$ um idempotente e consideremos o ideal esquerdo Re de R. Para cada $a \in R$, definimos $a_{\mathrm{L}} \colon Re \to Re$ por*

$$a_{\mathrm{L}}(x) = ax, \qquad x \in Re.$$

Então, a correspondência $a \mapsto a_{\mathrm{L}}$ define um isomorfismo de anéis

$$R \cong \mathrm{End}_{eRe}(Re)$$

onde Re é considerado como um eRe-módulo direito de maneira natural (por meio da multiplicação escalar $Re \times eRe \mapsto Re$ definida por $(x, b) \mapsto xb$).

Demonstração. É fácil verificar que

$$a_{\mathrm{L}} \in \mathrm{End}_{eRe}(Re), \qquad a \in R,$$

e que a correspondência $a \mapsto a_{\mathrm{L}}$ define um homomorfismo de anéis

$$\theta \colon R \to \mathrm{End}_{eRe}(Re)$$

(em que $\theta(a) = a_{\mathrm{L}}$ para todo $a \in R$).

Como R é simples e $\ker(\theta)$ é um ideal bilateral de R, tem de ser $\ker(\theta) = \{0\}$ (porque θ é não-nulo uma vez que $\theta(1) = \mathrm{id}_{Re} \neq 0$), logo θ é injectivo. Para provar que θ é sobrejectivo, basta verificar que $\theta(R)$ é um ideal esquerdo de $\mathrm{End}_{eRe}(Re)$; de facto, se isto acontece, temos

$$\mathrm{id}_{Re} = \theta(1) \in \theta(R)$$

e, portanto, tem de ser $\theta(R) = \mathrm{End}_{eRe}(Re)$. Sendo assim, devemos provar que

$$\varphi\theta(R) \subseteq \theta(R), \qquad \varphi \in \mathrm{End}_{eRe}(Re).$$

Em primeiro lugar, provamos que

$$\varphi\theta(Re) \subseteq \theta(Re), \qquad \varphi \in \mathrm{End}_{eRe}(Re).$$

Para isso, sejam $\varphi \in \mathrm{End}_{eRe}(Re)$ e $a \in Re$ arbitrários. Para qualquer $b \in Re$, tem-se $b = be$ e, portanto,

$$ab = aebe \qquad \text{e} \qquad \varphi(a)b = \varphi(a)ebe$$

(porque $\varphi(a) \in Re$). Como $\varphi \in \mathrm{End}_{eRe}(Re)$, deduzimos que

$$\begin{aligned}(\varphi\theta(a))(b) &= (\varphi a_{\mathrm{L}})(b) = \varphi(a_{\mathrm{L}}(b)) = \varphi(ab) = \varphi(aebe)\\ &= \varphi(a)ebe = \varphi(a)b = \varphi(a)_{\mathrm{L}}(b) = \theta(\varphi(a))(b)\end{aligned}$$

para todo $b \in Re$. Sendo assim,

$$\varphi\theta(a) = \theta(\varphi(a)) \in \theta(Re)$$

e, portanto, $\varphi\theta(Re) \subseteq \theta(Re)$.

Agora, como R é um anel simples e ReR é um ideal bilateral de R, temos

$$ReR = R$$

(porque $\{0\} \neq Re \subseteq ReR$) e, portanto,

$$\theta(R) = \theta(ReR) = \theta(Re)\theta(R),$$

de onde resulta que

$$\varphi\theta(R) = \varphi\theta(Re)\theta(R) \subseteq \theta(Re)\theta(R) \subseteq \theta(R).$$

Como $\varphi \in \mathrm{End}_{eRe}(Re)$ é arbitrário, concluímos de $\theta(Re)$ é um ideal esquerdo de $\mathrm{End}_{eRe}(Re)$, como se queria. □

2.3.4. Teorema. *Se R é um anel simples artiniano à esquerda, então existe um isomorfismo de anéis*

$$R \cong \mathrm{End}_D(M)$$

para algum anel de divisão D e algum D-módulo M com dimensão finita; em particular, se $n = \dim_D M$, então existe um isomorfismo de anéis $R \cong \mathbb{M}_n(D)$. Além disso, o par (D, M) é univocamente determinado a menos de isomorfismo (de modo que $n \in \mathbb{N}$ também é univocamente determinado)

Demonstração. Como R é artiniano, existe (pelo menos) um ideal esquerdo minimal $\mathcal{L}$ de R. Pela Proposição 2.1.18, existe um idempotente $e \in R$ tal que $\mathcal{L} = Re$. Além disso, pela Proposição 2.1.19, eRe é um anel de divisão. Pela Proposição 2.3.3, a correspondência $a \mapsto a_{\mathrm{L}}$ define um isomorfismo de anéis $R \cong \mathrm{End}_{eRe}(\mathcal{L})$ onde $\mathcal{L} = Re$ é considerado, de maneira natural, como um eRe-módulo direito. Deste modo, $\mathcal{L}$ é um $(eRe)^{\mathrm{op}}$-módulo esquerdo (em que a multiplicação escalar é dada por $a^{\mathrm{op}}b = ba$ para todo $a \in eRe$ e todo $b \in \mathcal{L}$) e, além disso, é um exercício simples verificar que

$$\mathrm{End}_{(eRe)^{\mathrm{op}}}(\mathcal{L}) = \mathrm{End}_{eRe}(\mathcal{L}).$$

Por conseguinte, pondo $D = (eRe)^{\mathrm{op}}$, obtemos um isomorfismo de anéis $R \cong \mathrm{End}_D(\mathcal{L})$.

De seguida, provamos que $\mathcal{L}$ tem dimensão finita com D-módulo. Para isso, consideramos o ideal

$$\mathcal{I} = \{\theta \in \mathrm{End}_D(\mathcal{L}) \colon \dim_D \theta(\mathcal{L}) < \infty\}$$

de $\mathrm{End}_D(\mathcal{L})$; é fácil provar que $\mathcal{I}$ é, de facto, um ideal bilateral de $\mathrm{End}_D(\mathcal{L})$. Como D é anel de divisão, $\mathcal{L}$ tem uma D-base $\{m_i \colon i \in I\}$ (pelo Teorema 1.3.13). Se $J \neq \emptyset$ é qualquer subconjunto finito de I, então, por extensão D-linear, existe $\theta \in \mathrm{End}_D(\mathcal{L})$ tal que

$$\theta(m_i) \in \{m_j \colon j \in J\}, \qquad i \in I,$$

pelo que $\dim_D \theta(\mathcal{L}) = |J| < \infty$ e, portanto, $\theta \in \mathcal{I}$. Segue-se que $\mathcal{I} \neq \{0\}$ e, uma vez que $\mathrm{End}_D(\mathcal{L})$ é um anel simples (porque é isomorfo a R), tem de ser $\mathcal{I} = \mathrm{End}_D(\mathcal{L})$. Em particular, temos $\mathrm{id}_{\mathcal{L}} \in \mathcal{I}$ e, portanto, $\dim_D \mathcal{L} < \infty$ (porque $\mathcal{L} = \mathrm{id}_{\mathcal{L}}(\mathcal{L})$).

Pondo $n = \dim_D \mathcal{L}$, o isomorfismo $\mathrm{End}_R(\mathcal{L}) \cong \mathbb{M}_n(D)$ é consequência do Lema 2.3.1. Deste modo, para terminar a demonstração, falta provar que o anel de divisão D e o D-módulo $\mathcal{L}$ são univocamente determinados a menos de isomorfismo. Sejam $n' \in \mathbb{N}$ e D' um anel de divisão tais que $\mathbb{M}_{n'}(D') \cong \mathbb{M}_n(D)$. Pela Proposição 2.3.2, n (resp., n') é o número de ideais esquerdos minimais que ocorrem numa decomposição em soma directa de $\mathbb{M}_n(D)$ (resp., $\mathbb{M}_{n'}(D')$) e, portanto, $n = n'$. Por outro lado, seja $e = e_{1,1}$ a $(1,1)$-ésima matriz elementar em $\mathbb{M}_n(D)$ e $e' = e_{1,1}$ a $(1,1)$-ésima matriz elementar em $\mathbb{M}_n(D)$, de modo que existem isomorfismos de anéis

$$D \cong e\mathbb{M}_n(D)e \qquad \text{e} \qquad D' \cong e'\mathbb{M}_n(D')e' \cong f\mathbb{M}_n(D)f$$

onde $f \in \mathbb{M}_n(D)$ é o idempotente que corresponde a $e' \in \mathbb{M}_n(D')$ por meio do isomorfismo $\mathbb{M}_n(D') \cong \mathbb{M}_n(D)$. Para terminar, notemos que $\mathbb{M}_n(D')e'$ é um ideal esquerdo minimal de $\mathbb{M}_n(D')$ e, portanto, $\mathbb{M}_n(D)f$ é um ideal esquerdo minimal de $\mathbb{M}_n(D)$. Como $\mathbb{M}_n(D)e$ também é um ideal esquerdo minimal de $\mathbb{M}_n(D)$, tem-se

$$M_n(D)e \cong_{\mathbb{M}_n(D)} \mathbb{M}_n(D)f$$

(pela Proposição 2.3.2(b)). Deste modo, a Proposição 2.1.19 garante que existem isomorfismos de anéis

$$e\mathbb{M}_n(D)e \cong \mathrm{End}_{M_n(D)}(\mathbb{M}_n(D)e)^{\mathrm{op}} \cong \mathrm{End}_{\mathbb{M}_n(D)}(\mathbb{M}_n(D)f)^{\mathrm{op}} \cong f\mathbb{M}_n(D)f.$$

Em conclusão, $D \cong D'$, como se pretendia; notemos que o D-módulo M é livre com dimensão n, logo $M \cong_D D^{(n)}$ é univocamente determinado a menos de isomorfismo. □

2.3.5. Teorema (Wedderburn-Artin). *Se R é um anel semisimples (à esquerda), então existe um isomorfismo de anéis*

$$R \cong \mathbb{M}_{n_1}(D_1) \dot{+} \cdots \dot{+} \mathbb{M}_{n_t}(D_t)$$

para alguns $n_1, \ldots, n_t \in \mathbb{N}$ e alguns anéis de divisão $D_1, \ldots, D_t$. Além disso, o número de componentes t é igual ao número total de classes de isomorfismo dos R-módulos simples e os pares $(n_1, D_1), \ldots, (n_t, D_t)$ são univocamente determinados (a menos de permutação e de isomorfismo).

Demonstração. Se $\mathcal{B}_1, \ldots, \mathcal{B}_t$ são as componentes de Wedderburn de R, então

$$R = \mathcal{B}_1 \oplus \cdots \oplus \mathcal{B}_t$$

(pelo Lema 2.2.4) e, além disso, $\mathcal{B}_1, \ldots, \mathcal{B}_t$ são anéis simples artinianos à esquerda (pelo Lema 2.2.10). Pelo Teorema 2.3.4, para cada $1 \le i \le t$, existe um isomorfismo de anéis

$$\mathcal{B}_i \cong \mathbb{M}_{n_i}(D_i)$$

para algum $n_i \in \mathbb{N}$ e algum anel de divisão D_i; além disso, o par (n_i, D_i) é univocamente determinado (a menos de isomorfismo). Para terminar a demonstração, falta justificar que o número de componentes t é univocamente determinado o que resulta do Lema 2.2.6. □

2.3.6. Corolário. *Qualquer anel semisimples à esquerda é semisimples à direita (e reciprocamente).*

Demonstração. Para qualquer anel de divisão D e qualquer $n \in \mathbb{N}$, o anel $\mathbb{M}_n(D)$ é semisimples, tanto à esquerda, como à direita, pelo que basta usar o isomorfismo do teorema anterior. □

2.4. Radical de Jacobson

2.4.1. Definimos o *radical de Jacobson* $\mathrm{rad}(R)$ do anel R como sendo a intersecção de todos os ideais esquerdos maximais de R; no caso em que $R = \{0\}$, não existem ideais esquerdos maximais, de modo que definimos $\mathrm{rad}(R) = \{0\}$.(*)

Pelo Lema de Zorn, qualquer anel não-nulo tem pelo menos um ideal esquerdo maximal e, portanto, $\mathrm{rad}(R) \neq R$ sempre que $R \neq \{0\}$.

2.4.2. Lema. *Para qualquer $a \in R$, as afirmações seguintes são equivalentes:*

(a) $a \in \mathrm{rad}(R)$.

(b) $1 - ra$ *é invertível à esquerda para qualquer* $r \in R$.

(*)Mais adiante, provamos que $\mathrm{rad}(R)$ é também a intersecção de todos os ideais direitos maximais de R, de modo que não é necessária qualquer distinção entre "radical esquerdo" e "radical direito".

(c) *$aM = \{0\}$ para qualquer R-módulo simples M.*

Demonstração. (a) $\Rightarrow$ (b) Supomos $a \in \operatorname{rad}(R)$ e que existe $r \in R$ tal que $1 - ra$ não é invertível à esquerda. Então, o ideal esquerdo $R(1 - ra)$ é próprio e, portanto,

$$1 - ra \in R(1 - ra) \subseteq \mathcal{L}$$

para algum ideal esquerdo maximal $\mathcal{L}$ de R. Como $\operatorname{rad}(R) \subseteq \mathcal{L}$, temos $a \in \mathcal{L}$, logo $ra \in \mathcal{L}$. Sendo assim,

$$1 = (1 - ra) + ra \in \mathcal{L}$$

e, portanto, $\mathcal{L} = R$, o que não acontece.

(b) $\Rightarrow$ (c) Suponhamos que $am \neq 0$ para algum $m \in M$. Então, $\{0\} \neq R(am) \leq_R M$ e, portanto, $M = R(am)$ (porque M é simples). Em particular, $m = r(am) = (ra)m$ para algum $r \in R$, donde $(1 - ra)m = 0$. Como $1 - ra$ é invertível À esquerda, existe $s \in R$ tal que $s(1 - ra) = 1_R$ e, portanto,

$$m = 1_R m = s(1 - ra)m = 0,$$

uma contradição.

(c) $\Rightarrow$ (a) Seja $\mathcal{L}$ um ideal esquerdo maximal de R. Então, $R/\mathcal{L}$ é um R-módulo simples e, portanto, $a(R/\mathcal{L}) = 0$ (por (c)). Sendo assim, $aR \subseteq \mathcal{L}$, logo $a = a1_R \in \mathcal{L}$. Como $\mathcal{L}$ é arbitrário, concluímos que $a \in \operatorname{rad}(R)$. □

2.4.3. Para qualquer R-módulo M, definimos o *anulador de M em R* com sendo

$$\operatorname{Ann}_R(M) = \{a \in R \colon aM = \{0\}\}\,;$$

não é difícil verificar que $\operatorname{Ann}_R(M)$ é um ideal bilateral de R.

2.4.4. Corolário. *$\operatorname{rad}(R)$ é um ideal bilateral de R.*

Demonstração. Basta observar que, pelo Lema 2.4.2,

$$\operatorname{rad}(R) = \bigcap_M \operatorname{Ann}_R(M)$$

onde a intersecção é sobre todos os R-módulos simples. □

2.4.5. Lema. *Para qualquer $a \in R$, as afirmações seguintes são equivalentes:*

(a) *$a \in \operatorname{rad}(R)$.*

(b) *$1 - ras \in R^\times$ para quaisquer $r, s \in R$.*

Demonstração. (a) $\Rightarrow$ (b) Suponhamos $a \in \operatorname{rad}(R)$ e sejam $r, s \in R$. Pelo Corolário 2.4.4, temos $as \in \operatorname{rad}(R)$ e, portanto, $1 - ras$ é invertível à esquerda, de modo que existe $u \in R$ tal que $u(1 - ras) = 1$; em particular, u é invertível à direita. Da mesma forma, como $ras \in \operatorname{rad}(R)$, $u = 1 + u(ras)$ é invertível à esquerda, logo $u \in R^\times$. Dada a unicidade do inverso, concluímos que $u^{-1} = 1 - ras$ e, portanto, $1 - ras \in R^\times$.

(b) $\Rightarrow$ (a) Como $1 - ra \in R^\times$ para todo $r \in R$ (tomando $s = 1$ em (b)), o Lema 2.4.2 garante que $a \in \mathrm{rad}(R)$. □

2.4.6. COROLÁRIO. *$\mathrm{rad}(R)$ é o maior ideal (esquerdo, direito e/ou bilateral) $\mathcal{I}$ de R tal que $1 + \mathcal{I} \subseteq R^\times$.*

Demonstração. Exercício. □

2.4.7. PROPOSIÇÃO. *Se $\mathcal{B}$ é um ideal bilateral de R, então $\mathrm{rad}(R/\mathcal{B}) = \mathrm{rad}(R)/\mathcal{B}$.*

Demonstração. Exercício. □

2.4.8. Dizemos que um ideal (esquerdo, direito ou bilateral) $\mathcal{I}$ de R é *nilpotente* se $\mathcal{I}^n = \{0\}$ para algum $n \in \mathbb{N}$.

2.4.9. LEMA. *Se $\mathcal{L}_1, \ldots, \mathcal{L}_t$ são ideais esquerdos nilpotentes de R, então $\mathcal{L}_1 + \cdots + \mathcal{L}_t$ também é nilpotente.*

Demonstração. Basta considerar $t = 2$; o caso geral segue-se por indução. Sejam $\mathcal{L}_1$ e $\mathcal{L}_2$ ideais esquerdos nilpotentes de R e seja $n \in \mathbb{N}$ tal que

$$(\mathcal{L}_1)^n = (\mathcal{L}_2)^n = \{0\}.$$

Um elemento de $(\mathcal{L}_1 + \mathcal{L}_2)^{2n}$ é uma soma de produtos da forma

$$(a_1 + b_1) \cdots (a_{2n} + b_{2n}), \qquad a_1, \ldots, a_{2n} \in \mathcal{L}_1,\ b_1, \ldots, b_{2n} \in \mathcal{L}_2.$$

Por sua vez, um produto deste tipo é uma soma de produtos de $2n$ elementos em que pelo menos n factores estão em $\mathcal{L}_1$ ou em $\mathcal{L}_2$. Segue-se que

$$(a_1 + b_1) \cdots (a_{2n} + b_{2n}) = 0, \qquad a_1, \ldots, a_{2n} \in \mathcal{L}_1,\ b_1, \ldots, b_{2n} \in \mathcal{L}_2,$$

e, portanto, $(\mathcal{L}_1 + \mathcal{L}_2)^{2n} = \{0\}$. □

2.4.10. TEOREMA. *Se R é artiniano à esquerda, então $\mathrm{rad}(R)$ é o maior ideal esquerdo nilpotente de R.*

Demonstração. Em primeiro lugar, provamos que, se $\mathcal{L}$ é um ideal esquerdo nilpotente de R, então $\mathcal{L} \subseteq \mathrm{rad}(R)$. Para isso, se $a \in \mathcal{L}$, $r \in R$ e $n \in \mathbb{N}$ é tal que $\mathcal{L}^n = 0$, então $(ra)^n = 0$ (porque $ra \in \mathcal{L}$) e, portanto, $1 - ra \in R^\times$ (com inverso $(1 - ra)^{-1} = 1 + ra + \cdots + (ra)^{n-1}$). Pelo Lema 2.4.2, concluímos que $a \in \mathrm{rad}(R)$, como se queria.

Por outro lado, provamos que $\mathcal{J} = \mathrm{rad}(R)$ é nilpotente. Para isso, consideremos a cadeia descendente

$$\mathcal{J} \supseteq \mathcal{J}^2 \supseteq \mathcal{J}^3 \supseteq \cdots$$

de ideias de R. Com R é artiniano (à esquerda), existe $n \in \mathbb{N}$ tal que

$$\mathcal{J}^n = \mathcal{J}^{n+1} = \mathcal{J}^{n+2} = \cdots .$$

Provamos que $\mathfrak{J}^n = \{0\}$. Com efeito, suponhamos que $\mathfrak{J}^n \neq \{0\}$ e consideremos o conjunto

$$\Sigma = \{\mathcal{L} \colon \mathcal{L} \text{ é ideal esquerdo de } R \text{ e } \mathfrak{J}^n \mathcal{L} \neq \{0\}\}\,.$$

Como $\Sigma \neq \emptyset$ (porque $\mathcal{L} \in \Sigma$) e R é artiniano à esquerda, Σ tem pelo menos um elemento minimal $\mathcal{L}$. Escolhendo $0 \neq a \in \mathcal{L}$ tal que $\mathfrak{J}^n a \neq \{0\}$, temos

$$\mathfrak{J}^n(\mathfrak{J}^n a) = \mathfrak{J}^{2n} a = \mathfrak{J}^n a \neq \{0\}$$

e, portanto, $\mathfrak{J}^n a = \mathcal{L}$ (pela minimalidade de $\mathcal{L}$). Sendo assim, existe $r \in \mathfrak{J}^n \subseteq \mathfrak{J}$ tal que $a = ra$, ou seja, tal que $(1-r)a = 0$. Como $r \in \mathfrak{J} = \mathrm{rad}(R)$, temos $1 - r \in R^\times$ (pelo Lema 2.4.5), logo $a = 0$, uma contradição. Segue-se que $\mathfrak{J}^n = \{0\}$ e, portanto, $\mathfrak{J} = \mathrm{rad}(R)$ é nilpotente.

A demonstração está completa. $\square$

2.4.11. Teorema. *Um anel R é semisimples se e só se R é artiniano à esquerda e* $\mathrm{rad}(R) = \{0\}$.

Demonstração. $(\Rightarrow)$ Se R é semisimples, existe um ideal esquerdo $\mathcal{L}$ de R tal que

$$R = \mathrm{rad}(R) \oplus \mathcal{L}.$$

Se $\mathrm{rad}(R) \neq \{0\}$, então $\mathcal{L} \neq R$ e, portanto, existe um ideal esquerdo maximal $\mathcal{L}'$ de R tal que $\mathcal{L} \subseteq \mathcal{L}'$. Como $\mathrm{rad}(R) \subseteq \mathcal{L}'$, segue-se que $R \subseteq \mathcal{L}'$, uma contradicção.

$(\Leftarrow)$ Supomos que R é artiniano à esquerda e que $\mathrm{rad}(R) = \{0\}$. Seja $\mathcal{L}_1$ um ideal esquerdo minimal de R (este ideal existe porque R é artiniano à esquerda). Como $\mathrm{rad}(R) = \{0\} \subsetneq \mathcal{L}_1$, existe um ideal esquerdo maximal $\mathcal{L}_1'$ de R tal que $\mathcal{L}_1 \cap \mathcal{L}_1' = \{0\}$; caso contrário, a minimalidade de $\mathcal{L}_1$ implica que $\mathcal{L}_1 = \mathcal{L}_1 \cap \mathcal{L}' \subseteq \mathcal{L}'$ para todo o ideal esquerdo maximal $\mathcal{L}'$ de R e, portanto, $\mathcal{L}_1 \subseteq \mathrm{rad}(R)$. Sendo assim,

$$R = \mathcal{L}_1 \oplus \mathcal{L}_1'$$

(pela maximalidade de $\mathcal{L}_1'$ porque $\mathcal{L}_1' \subsetneq \mathcal{L}_1 + \mathcal{L}_1'$).

Se $\mathcal{L}_1' = \{0\}$, então $R = \mathcal{L}_1$ e, portanto, R é semisimples. Por outro lado, no caso em que $\mathcal{L}_1' \neq \{0\}$, existe um ideal esquerdo minimal $\mathcal{L}_2$ de R tal que $\mathcal{L}_2 \subseteq \mathcal{L}_1'$ (porque R é artiniano à esquerda). Repetindo o argumento acima, existe um ideal esquerdo maximal $\mathcal{L}_2'$ de R tal que $R = \mathcal{L}_2 \oplus \mathcal{L}_2'$ e, portanto,

$$\mathcal{L}_1' = \mathcal{L}_1' \cap (\mathcal{L}_2 \oplus \mathcal{L}_2') = \mathcal{L}_2 \oplus (\mathcal{L}_1' \cap \mathcal{L}_2')$$

e

$$R = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus (\mathcal{L}_1' \cap \mathcal{L}_2').$$

Se $\mathcal{L}_1' \cap \mathcal{L}_2' = \{0\}$, então $R = \mathcal{L}_1' \oplus \mathcal{L}_2'$ e, portanto, R é semisimples. Por outro lado, no caso em que $\mathcal{L}_1' \cap \mathcal{L}_2' \neq \{0\}$, escolhemos um ideal esquerdo minimal $\mathcal{L}_3$ de R tal que $\mathcal{L}_3 \subseteq \mathcal{L}_1' \cap \mathcal{L}_2'$ e um ideal esquerdo maximal $\mathcal{L}_3'$ de R tal que $R = \mathcal{L}_3 \oplus \mathcal{L}_3'$. Como antes, temos

$$\mathcal{L}_1' \cap \mathcal{L}_2' = (\mathcal{L}_1' \cap \mathcal{L}_2') \cap (\mathcal{L}_3 \oplus \mathcal{L}_3') = \mathcal{L}_3 \oplus (\mathcal{L}_1' \cap \mathcal{L}_2' \cap \mathcal{L}_3')$$

e

$$R = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3 \oplus (\mathcal{L}'_1 \cap \mathcal{L}'_2 \cap \mathcal{L}'_3).$$

Continuando este processo, depois de n etapas, encontramos ideais esquerdos minimais $\mathcal{L}_1, \dots, \mathcal{L}_n$ e ideais esquerdos maximais $\mathcal{L}'_1, \dots, \mathcal{L}'_n$ de R tais que

$$\mathcal{L}_m \subseteq \mathcal{L}'_{m-1} \quad \text{e} \quad R = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_m \oplus (\mathcal{L}'_1 \cap \cdots \cap \mathcal{L}'_m)$$

sempre que $m \leq n$. Além disso, obtemos uma cadeia descendente

$$\mathcal{L}'_1 \supsetneq \mathcal{L}'_1 \cap \mathcal{L}'_2 \supsetneq \cdots \supsetneq \mathcal{L}'_1 \cap \cdots \cap \mathcal{L}'_n$$

de ideais esquerdos de R. Como R é artiniano à esquerdo, esta cadeia tem de terminar, isto é, tem de existir $n \in \mathbb{N}$ tal que $\mathcal{L}'_1 \cap \cdots \cap \mathcal{L}'_n = \{0\}$, de modo que

$$R = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_n$$

e, portanto, R é semisimples. □

2.4.12. Corolário. *Se R é um anel artiniano à esquerda, então $R/\operatorname{rad}(R)$ é um anel semisimples.*

Demonstração. Basta observar que $R/\operatorname{rad}(R)$ é artiniano à esquerda (pela Proposição 1.4.7(b)) e que $\operatorname{rad}(R/\operatorname{rad}(R)) = \operatorname{rad}(R)/\operatorname{rad}(R) = \{0\}$ (usando a Proposição 2.4.7). □

2.4.13. Teorema (Lema de Nakayama). *Para qualquer ideal esquerdo $\mathcal{L}$ de R, as afirmações seguintes são equivalentes:*

(a) $\mathcal{L} \subseteq \operatorname{rad}(R)$.

(b) *Se M é um R-módulo finitamente gerado e $\mathcal{L}M = \{0\}$, então $M = \{0\}$.*

(c) *Se M é um R-módulo finitamente gerado e $N \leq_R M$ é tal que $N + \mathcal{L}M = M$, então $N = M$.*

Demonstração. (a) ⇒ (b) Supomos que $\mathcal{L} \subseteq \operatorname{rad}(R)$ e provamos que, se $M \neq \{0\}$ é um R-módulo finitamente gerado, então $\mathcal{L}M \neq M$. Usando o Lema de Zorn e tendo em conta que M é finitamente gerado, é fácil provar que existe um R-módulo maximal $N \leq_R M$. Então, o R-módulo quociente M/N é simples e, portanto, $\mathcal{L}(M/N) = \{0\}$ (pelo Lema 2.2.2(c)). Como $\mathcal{L}(M/N) = (\mathcal{L}M + N)/N$, concluímos que $\mathcal{L}M + N = N$, logo $\mathcal{L}M \subseteq N$. Em particular, $\mathcal{L}M \neq M$.

(b) ⇒ (c) Sejam M um R-módulo finitamente gerado e $N \leq_R M$ tal que $N + \mathcal{L}M = M$. Então, o R-módulo quociente M/N é finitamente gerado e $\mathcal{L}(M/N) = (\mathcal{L}M + N)/N = M/N$. Por (b), concluímos que $M/N = \{0\}$ e, portanto, $N = M$.

(c) ⇒ (a) Com vista a contradição, suponhamos que $\mathcal{L} \nsubseteq \operatorname{rad}(R)$ e seja $a \in \mathcal{L}$ tal que $a \notin \operatorname{rad}(R)$. Então, existe um ideal esquerdo maximal $\mathcal{L}'$ de R tal que $a \notin \mathcal{L}'$ e, portanto, $\mathcal{L}' + Ra = R$. Como $Ra \subseteq \mathcal{L}$, concluímos que $\mathcal{L}' + \mathcal{L} = R$ e, portanto, $\mathcal{L}' + \mathcal{L}R = R$ (porque

$\mathcal{L} = \mathcal{L}1_R \subseteq \mathcal{L}R$). Como R é finitamente gerado como R-módulo (porque $R = R1_R$), (c) implica que $\mathcal{L}' = R$, o que contraria a maximalidade de $\mathcal{L}'$. $\square$