Publicações do CENTRO DE ESTUDOS DE MATEMÁTICA
DA FACULDADE DE CIÊNCIAS DO PORTO
N.º 34

TRÊS LIÇÕES SOBRE A TEORIA GERAL DOS ANÉIS

(APLICAÇÕES E COMPLEMENTOS, I)

POR

A. ALMEIDA COSTA

Publicação subsidiada pelo INSTITUTO DE ALTA CULTURA

1 9 5 4

Extracto do fasc. III do tomo XXXVII
dos
«Anais da Faculdade de Ciências do Porto»

TRÊS LIÇÕES SOBRE A TEORIA GERAL DOS ANÉIS

(Aplicações e complementos, I)

Somas sub-directas de módulos. Módulos semi-simples. Sub-módulos — G

1) **Introdução** — As três lições sobre a teoria geral dos anéis, que inserimos anteriormente nesta Revista, e que, de harmonia com observações já feitas, podem ser citadas com as designações respectivas de Caps. XVI, XVII e XVIII, vão ser completadas em certos pontos. Ao mesmo tempo, serão tratadas algumas aplicações. Em termos já assinalados num trabalho de 1948, [10], transportaremos, por vezes, para a teoria dos módulos, raciocínios conhecidos, da teoria dos anéis. As questões relativas a somas sub-directas e a módulos sub-directamente irredutíveis serão agora exemplos desse transporte.

Dentro do mesmo espírito que tem presidido às nossas últimas publicações, vamos dar, em jogo com a bibliografia citada nas mesmas, as indicações seguintes, nas quais julgamos conveniente introduzir também números para representar os Capítulos XIII e XIV, XV, XVI, XVII e XVIII: [19] — O. GOLDMAN, *A characterisation of semi-simple rings with the descending chain condition,* «Bulletin of the American Mathematical Society», vol. 52, 1946, págs. 1021 a 1027; [21] — O. GOLDMAN, *Semi-simple extensions of rings,* na mesma Revista, págs. 1028 a 1032; [22] — A. FORSYTHE e N. H. MCCOY, *On the commutativity of certain rings,* igualmente no «Bulletin», vol. 52, 1946, págs. 523 a 526; [23, ou Caps. XIII e XIV] — A. ALMEIDA COSTA, *Sobre a teoria dos anéis e ideais não comutativos,* tomo I das «Actas do XIII Congresso Luso-Espanhol para o Progresso das Ciências», Lisboa, 1950; [24, ou Cap. XV] — A. ALMEIDA COSTA, *Sobre ideais de contracção e aniquiladores* *na teoria geral dos módulos*, «Anais da Faculdade de Ciências do Porto», tomo XXXV, 1951, págs. 79 a 158; [25, ou Cap. XVI] — A. ALMEIDA COSTA, Três lições sobre a teoria geral dos anéis (1.ª lição: *Radical — G, Anti-radical, Ideal regular máximo dum anel)*, também nos «Anais», tomo XXXVI, 1952, págs. 65 a 83; [26, ou Cap. XVII] — A. ALMEIDA COSTA, Três lições sobre a teoria geral dos anéis (2.ª lição: *Anéis primitivos)*, igualmente nos «Anais», tomo XXXVI, 1952, págs. 169 a 200; [27 ou Cap. XVIII] — A. ALMEIDA COSTA, Três lições sobre a teoria geral dos anéis (3.ª lição: *Somas sub-directas de anéis, Anéis semi-simples)*, ainda nos «Anais», tomo XXXVI, 1952, págs. 221 a 247; [28] — N. JACOBSON, *Structure theory for algebraic algebras of bounded degree*, «Annals of Mathematics», vol. 46, 1945, págs. 695 a 707; [30] — A. ALMEIDA COSTA, *Über die unterdirekten Modulnsummen*, «Revista da Faculdade de Ciências de Lisboa», vol. II, 1952, págs. 115 a 160; [32] — N. JACOBSON, *Lectures in Abstract Algebra*, vol. II, 1953, New York.

2) **Somas sub-directas especiais de módulos** — As considerações desenvolvidas em [27, §§ 2 e 3] vão ter aqui as suas semelhantes. Ao lado das somas directas completas e discretas de módulos — Ω, [24, § 11], há também somas sub-directas e somas sub-directas especiais. Os teoremas 1, 1a e 2, do referido § 2, adaptam-se imediatamente ao caso dos módulos. Vamos simplesmente reproduzir alguns raciocínios respeitantes ao teorema 3, lema 1, corolário 1 e teorema 4, de [27, § 2].

TEOREMA 1: — *É condição necessária, para que $\mathfrak{M}$ seja isomorfo — Ω duma soma sub-directa especial dos módulos $\mathfrak{m}_\mu$, (todos, como $\mathfrak{M}$, supostos módulos — Ω), que haja em $\mathfrak{M}$ um sistema de sub-módulos $\mathfrak{M}_\mu$, correspondentes aos $\mathfrak{m}_\mu$ pelo isomorfismo em causa, e um segundo sistema de sub-módulos $\mathfrak{N}_\mu$, nas condições seguintes: $\mathfrak{M}_\mu \cap \mathfrak{M}_\nu = (o)$, se $\mu \neq \nu$; $\mathfrak{M}_\mu + \mathfrak{N}_\mu = \mathfrak{M}$; $\Pi\, \mathfrak{N}_\mu = (o)$.* Como na teoria dos anéis, é a inversa desta proposição que carece de uma nova hipótese, em relação com o seguinte

LEMA 1: — *Se $\mathfrak{M}$ é um módulo — Ω, que pode ser escrito sob as formas $\mathfrak{M} = \mathfrak{M}_1 + \mathfrak{N}_1 = \mathfrak{M}_2 + \mathfrak{N}_2$, onde os $\mathfrak{M}_i$, $\mathfrak{N}_i$ se supõem módulos — $(\Omega, \overline{\Omega})$, e $\mathfrak{M}_1 \cap \mathfrak{M}_2 = (o)$, tem-se $\mathfrak{M}_1 \subseteq \mathfrak{N}_2$, $\mathfrak{M}_2 \subseteq \mathfrak{N}_1$.* Demonstremos, por ex., que $\mathfrak{M}_1 \subseteq \mathfrak{N}_2$,

servindo-nos de resultados estabelecidos no Cap. XV, § 10. Sabemos que $\overline{\Omega} = \mathfrak{s}_1 + \mathfrak{r}_1 = \mathfrak{s}_2 + \mathfrak{r}_2$, onde os $\mathfrak{s}_i$ e os $\mathfrak{r}_i$, $(i = 1, 2)$, que são ideais bilaterais, representam, respectivamente, os aniquiladores [1] dos $\mathfrak{M}_i$ e dos $\mathfrak{N}_i$. Também sabemos que os $\mathfrak{r}_i$ são ideais de contracção nos $\mathfrak{M}_i$ e os $\mathfrak{s}_i$ ideais de contracção nos $\mathfrak{N}_i$. A hipótese $\mathfrak{M}_1 \cap \mathfrak{M}_2 = (o)$ arrasta $[\mathfrak{r}_1, \mathfrak{r}_2] = (o)$, de sorte que $\mathfrak{r}_1 \subseteq \mathfrak{s}_2$, $\mathfrak{r}_2 \subseteq \mathfrak{s}_1$, [Cap. XVIII, § 2, lema 1]. Pondo $1 \in \overline{\Omega}$ sob as formas $1 = E_1 + E'_1 = E_2 + E'_2$, onde os idempotentes das decomposições pertencem aos respectivos ideais das decomposições de $\overline{\Omega}$, vemos que, para cada $m_1 \in \mathfrak{M}_1$, escrito sob a forma $m_1 = m_2 + n_2$, $(m_2 \in \mathfrak{M}_2, n_2 \in \mathfrak{N}_2)$, se tem $m_1 E'_1 = m_1 = m_2 E'_1 + n_2 E'_1 = n_2 E'_1 \in \mathfrak{N}_2$. A demonstração está feita.

COROLÁRIO 1: — *Nas condições do lema, se for $\mathfrak{M} = \mathfrak{N}_1 + \mathfrak{M}_1 = \mathfrak{M}_1 + \mathfrak{N}_2$, tem-se necessàriamente $\mathfrak{N}_1 = \mathfrak{N}_2$.*

A inversa do teorema 1 pode agora enunciar-se:

TEOREMA 2: — *Dado $\mathfrak{M}$, suposto módulo — Ω, e dados $\mathfrak{m}_\mu$, igualmente módulos — Ω, é suficiente, para que $\mathfrak{M}$ seja isomorfo — Ω duma soma sub-directa especial dos $\mathfrak{m}_\mu$, que se realizem as condições seguintes: 1.ª) existam em $\mathfrak{M}$ sub-módulos $\mathfrak{M}_\mu$, isomorfos — Ω dos $\mathfrak{m}_\mu$, que sejam, além disso, sub-módulos — $\overline{\Omega}$; 2.ª) valha $\mathfrak{M}_\mu \cap \mathfrak{M}_\nu = (o)$, quando $\mu \neq \nu$; 3.ª) seja $\mathfrak{M}_\mu + \mathfrak{N}_\mu = \mathfrak{M}$, para certos $\mathfrak{N}_\mu$, supostos módulos — $(\Omega, \overline{\Omega})$; 4.ª) valha a igualdade $\Pi\, \mathfrak{N}_\mu = (o)$.* Relativamente à demonstração, tendo em conta o lema, basta reproduzir os raciocínios do teorema 4, Cap. XVIII, § 2.

LEMA 2: — *Se $\mathbf{M}$ [2] é um módulo — Ω, dado $\mathfrak{N} \subseteq \mathbf{M}$, suposto sub-módulo — $(\Omega, \overline{\Omega})$, admitindo que é $\mathfrak{N} = \mathbf{M}\mathrm{E}$, em que E é elemento um de $\overline{\Omega}\mathrm{E}$, na decomposição* $\mathbf{M} = \mathbf{M}\mathrm{E} +$

(1) Estes aniquiladores, compostos de endomorfismos — Ω (portanto, contidos em $\overline{\Omega}$), não se confundem com os aniquiladores que sejam compostos de elementos de Ω.

(2) Veja-se a nota 1 no fim da pág. que contém o teorema 3a, § 2, Cap. XVII.

$+\mathbf{M}(1-\mathrm{E})$, *a 2.ª parcela é igualmente sub-módulo — $-\Omega, \overline{\Omega}$)*. Trata-se de provar que, para cada $A \in \overline{\Omega}$, se tem $\mathbf{M}(1-E)A \subseteq \mathbf{M}(1-E)$. Ora isso resulta de ser $\mathbf{M}(1-E)AE = \mathbf{M}(1-E)EAE = (o)$.

No teorema a que vamos passar, apenas a 2.ª parte utiliza o lema anterior. Empregando também a letra $\mathfrak{T}$ para designar uma soma sub-directa de módulos $\mathfrak{m}_\mu$, todos supostos módulos $-\Omega$, representaremos por $\overline{\overline{\Omega}}$ o anel dos endomorfismos $-\Omega$, de $\mathfrak{T}$. É válido este

TEOREMA 3: — *Seja $\mathfrak{T}$ uma soma sub-directa especial de módulos $\mathfrak{m}_\mu$, nas condições seguintes: 1) os $\mathfrak{m}_\mu$ são módulos — $-(\Omega, \overline{\overline{\Omega}})$ simples; 2) cada um deles é imagem homomorfa de $\mathfrak{T}$ da forma $\mathfrak{m}_\mu = \mathfrak{T}\overline{\mathrm{E}}_\mu$, onde $\overline{\mathrm{E}}_\mu \in \overline{\overline{\Omega}}$ é elemento um de $\overline{\overline{\Omega}}\,\overline{\mathrm{E}}_\mu$; então, é condição necessária e suficiente, para que $\mathbf{M}$, suposto módulo — Ω, seja isomorfo de $\mathfrak{T}$, que cada sub-módulo — $(\Omega, \overline{\Omega})$, de $\mathbf{M}$, contenha um sub-módulo — $(\Omega, \overline{\Omega})$ simples, igualmente imagem homomorfa de $\mathbf{M}$ definida por idempotente que é elemento um do respectivo ideal de contracções.* A condição é *necessária:* Partindo do isomorfismo $\mathbf{M} \simeq \mathfrak{T}$, seja $(o) \neq \mathfrak{N} \subseteq \mathbf{M}$, onde $\mathfrak{N}$ se supõe módulo — $(\Omega, \overline{\Omega})$. Pelo isomorfismo, passa-se de $\mathfrak{N}$ a $\mathfrak{T}_1 \subseteq \mathfrak{T}$, onde $\mathfrak{T}_1 \neq (o)$ é sub-módulo — $(\Omega, \overline{\overline{\Omega}})$. Tomemos, então, $o \neq t_1 \in \mathfrak{T}_1$. Por via de $\mathfrak{T} \sim \mathfrak{m}_\mu$, a t_1 corresponde, quando $\mu = \lambda$ (por ex.), um elemento $m_\lambda \in \mathfrak{m}_\lambda$, sendo $m_\lambda \neq o$. Como se tem $\mathfrak{T}\overline{E}_\lambda = \mathfrak{m}_\lambda$, será $\mathfrak{T}_1\overline{E}_\lambda \subseteq \mathfrak{m}_\lambda$. O facto $t_1 \to t_1\overline{E}_\lambda = m_\lambda \neq o$ mostra ser $(o) \neq \mathfrak{T}_1\overline{E}_\lambda \subseteq \mathfrak{T}_1$. Daqui se tira $(o) \neq \mathfrak{m}_\lambda \cap \mathfrak{T}_1 = \mathfrak{m}_\lambda$, como se deseja.

A condição é *suficiente:* Dado $\mathbf{M}$, consideremos o conjunto $\{\mathbf{M}_\nu\}$ dos sub-módulos — $(\Omega, \overline{\Omega})$ simples que são imagens homomorfas definidas por idempotentes, elementos um dos respectivos ideais de contracção: $\mathbf{M}_\nu = \mathbf{M}E_\nu$. As condições 1) e 2) do teorema 2 são verificadas. A condição 3), do mesmo teorema, é consequência do lema 2. Só resta verificar, por isso, que, consideradas as decomposições $\mathbf{M} = \mathbf{M}_\nu + \mathfrak{N}_\nu$, se tem $\Pi\mathfrak{N}_\nu = (o)$. Se assim não fosse, existiria um $\mathbf{M}_\lambda$ contido na intersecção; e o endomorfismo E_λ daria $(o) = \mathfrak{N}_\lambda E_\lambda \supseteq \Pi\mathfrak{N}_\nu \,.\, E_\lambda \neq (o)$, o que é

absurdo. O teorema está provado: $\mathbf{M}$ é soma directa especial dos $\mathbf{M}_\nu$.

A última proposição a estabelecer sobre somas sub-directas especiais assenta nos lemas a seguir.

LEMA 3: — *Dado $\mathbf{M}$, suposto módulo — Ω, seja $\mathbf{N}$ um sub-módulo — Ω, nas condições seguintes: 1) o ideal de contracções em $\mathbf{N}$ não tem nilideal; 2) cada sub-módulo — Ω não nulo, contido em $\mathbf{N}$, tem um ideal de contracções $\neq (o)$, 3) é válida em $\mathbf{N}$ a condição de mínimo para os sub-módulos — Ω que contém; então, admitindo ser $\mathfrak{P} = \mathbf{M}\mathrm{E} \subset \mathbf{N}$; existe idempotente $\mathrm{G} \in \overline{\Omega}$ tal que $\mathbf{M}\mathrm{E} \subset \mathbf{M}\mathrm{G} = \mathfrak{P}' \subseteq \mathbf{N}$.*

De $\mathbf{M} = \mathbf{M}E + \mathbf{M}(1-E)$, tiramos $\mathbf{N} = \mathbf{M}E + \mathbf{N} \cap \mathbf{M}(1-E)$. Pela condição 3), existe sub-módulo mínimo em $\mathbf{N} \cap \mathbf{M}(1-E)$, o qual, pelas condições 1) e 2), é de forma $\mathbf{M}E'$, com $o \neq E' \neq E$, [Cfr. 24, § 6, teoremas 22 e 23]. Como se verifica a igualdade $E'E = o$, pondo $E_1 = E$, $E_2 = E' - EE'$, vê-se que $E_1E_2 = E_2E_1 = o$, $E_2^2 = E_2$, de sorte que o idempotente $G = E_1 + E_2$ dá precisamente $\mathfrak{P}' = \mathbf{M}G = \mathbf{M}E_1 + \mathbf{M}E_2 \supset \mathbf{M}E$.

LEMA 4: — *O sub-módulo $\mathbf{N}$, do lema anterior, é soma directa de sub-módulos — Ω simples, de $\mathbf{M}$.* A demonstração faz-se exactamente pelas mesmas considerações que levaram a estabelecer o teorema 64, do Cap. XVIII, § 17.

LEMA 5: — *Nas condições do lema 3, $\mathbf{N}$ é imagem homomorfa de $\mathbf{M}$ definida por idempotente.* De facto, a construção sucessiva de $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \ldots,$ satisfazendo a $\mathfrak{P} \subset \mathfrak{P}' \subset \mathfrak{P}'' \subset \ldots \subseteq \mathbf{N}$ é forçosamente limitada, pois que $\mathbf{N}$ é completamente redutível, possuindo uma série de composição de comprimento limitado.

LEMA 6: — *Ainda com as mesmas hipóteses, suponhamos mais que $\mathbf{N} = \mathbf{M}\mathrm{E}$ é módulo — $(\Omega, \overline{\Omega})$; então, E é elemento um de $\overline{\Omega}\mathrm{E}$.* De facto, $\overline{\Omega}E$ é ideal bilateral. Se escrevermos $\overline{\Omega} = E\overline{\Omega} + (1-E)\overline{\Omega}$, como $E\overline{\Omega} \subseteq \overline{\Omega}E$, pode pôr-se $\overline{\Omega}E = E\overline{\Omega} + \overline{\Omega}E \cap (1-E)\overline{\Omega}$. Representando por $\mathfrak{s}$ esta última intersecção, que é um ideal direito de $\overline{\Omega}$ contido em $\overline{\Omega}E$, obtém-se $\mathfrak{s}^2 = \mathfrak{s}E . \mathfrak{s} = \mathfrak{s} . E\mathfrak{s} = (o)$. A condição 1), do lema 3, dá $\mathfrak{s} = (o)$, $\overline{\Omega} E = E \overline{\Omega}$, o que prova o lema.

TEOREMA 4: — *Seja* $\mathfrak{T}$ *uma soma sub-directa especial de módulos* $\mathfrak{m}_\mu$, *nas condições seguintes:* 1) *os* $\mathfrak{m}_\mu$ *são módulos* — $(\Omega, \overline{\overline{\Omega}})$ *simples;* 2) *cada um deles é imagem homomorfa de* $\mathfrak{T}$ *da forma* $\mathfrak{m}_\mu = \mathfrak{T}\overline{\mathrm{E}}_\mu$, *onde* $\overline{\mathrm{E}}_\mu \in \overline{\overline{\Omega}}$ *é elemento um de* $\overline{\overline{\Omega}}\,\overline{\mathrm{E}}_\mu$; 3) *os* $\mathfrak{m}_\mu$ *zão somas directas de módulos* — Ω *simples e o respectivo ideal de contracções não tem nilideal; então, é condição necessária e suficiente, para que* $\mathbf{M}$, *suposto módulo* — Ω, *seja isomorfo de* $\mathfrak{T}$, *que cada* $\mathbf{N} \neq (\mathrm{o})$, *suposto módulo* — $(\Omega, \overline{\Omega})$ *de* $\mathbf{M}$, *contenha um sub-módulo* — $(\Omega, \overline{\Omega})$ *simples, nos termos seguintes:* a) *se* $\mathfrak{P}$ *é o referido sub-módulo, o seu ideal de contracções não tem nilideal;* b) *cada sub-módulo* — Ω, *contido em* $\mathfrak{P}$, *tem um ideal de contracções* $\neq (\mathrm{o})$; c) *é válida em* $\mathfrak{P}$ *a condição de mínimo para os sub-módulos* — Ω. A condição é *necessária:* Partindo do isomorfismo $\mathbf{M} \simeq \mathfrak{T}$, seja $(o) \neq \mathbf{N} \subseteqq \mathbf{M}$, onde $\mathbf{N}$ se supõe sub-módulo — $(\Omega, \overline{\Omega})$. Como estamos nas condições do teorema 3, há, em $\mathbf{N}$, um sub-módulo — $(\Omega, \overline{\Omega})$ simples, definido por idempotente que é elemento um do respectivo ideal de contracções. Podemos precisar, até, que esse sub-módulo simples $\mathfrak{P}$ é isomorfo dum certo $\mathfrak{m}_\lambda$, de sorte que, por virtude de 3), o ideal de contracções em $\mathfrak{P}$ não tem nilideal e é válida em $\mathfrak{P}$ a condição de mínimo para os sub-módulos — Ω. Por último, b) é igualmente válido, pelo facto de cada sub-módulo — Ω, contido em $\mathfrak{P}$, ser soma directa de sub-módulos mínimos, cada um dos quais é imagem de $\mathbf{M}$ definida por idempotente.

A condição é *suficiente:* Dado $\mathbf{M}$, consideremos o conjunto $\{\mathbf{M}_\nu\}$ dos seus sub-módulos — $(\Omega, \overline{\Omega})$ simples, verificando os termos a), b) e c) do enunciado. Os lemas 3 a 6 são aplicáveis, de modo que cada $\mathbf{M}_\nu$, além de verificar a condição 1), é, pelos lemas 5 e 6, da forma $\mathbf{M}_\nu = \mathbf{M} E_\nu$, onde E_ν é elemento um de $\overline{\Omega} E_\nu$, de tal sorte que a condição 2) é também válida. Quanto à condição 3), basta termos em conta o lema 4 e a hipótese a), para se concluir que tem igualmente lugar. O teorema fica, portanto, demonstrado, visto que, pelo teorema 3, $\mathbf{M}$ é soma sub-directa especial dos $\mathbf{M}_\nu$.

3) **Somas directas discretas** — Já nos ocupámos largamente, em [24, §§ 11 a 14], com a teoria das somas directas discretas de módulos. Neste momento, limitar-nos-emos a um enunciado em correlação com o teorema 36 de [27] e a algumas observações referentes a [24, § 12].

TEOREMA 5: — *Seja* $\mathfrak{T}$ *uma soma directa discreta de módulos* $\mathfrak{m}_\mu$, *nas condições seguintes:* 1) *os* $\mathfrak{m}_\mu$ *são módulos* — $(\Omega, \overline{\overline{\Omega}})$ *simples;* 2) *cada um deles é imagem homomorfa de* $\mathfrak{T}$ *da forma* $\mathfrak{m}_\mu = \mathfrak{T}\overline{\mathrm{E}}_\mu$, *onde* $\overline{\mathrm{E}}_\mu \in \overline{\overline{\Omega}}$ *é elemento um de* $\overline{\overline{\Omega}}\,\overline{\mathrm{E}}_\mu$; *então, é condição necessária e suficiente, para que* $\mathbf{M}$, *suposto módulo* — Ω, *seja isomorfo de* $\mathfrak{T}$, *que* $\mathbf{M}$ *seja gerado pelos seus sub-módulos* — $(\Omega, \overline{\Omega})$ *simples, cada um dos quais imagem homomorfa de* $\mathbf{M}$ *definida por idempotente, elemento um do respectivo ideal de contracções.* Enquanto — que a 1.ª parte do teorema é uma trivialidade, a segunda demonstra-se por analogia com o teorema 36 do Cap. XVIII, tendo em conta os lemas 1 e 2, assim como o teorema 2.

As observações respeitantes ao § 12 do Cap. XV, acima referidas, são simples.

Suporemos que o domínio Ω dos operadores comuns aos $\mathfrak{m}_\mu$ e à sua soma directa discreta $\mathbf{M} = \Sigma\,\mathfrak{m}_\mu$ é um anel $\mathfrak{R}$, que pode não estar «mergulhado» nos diferentes anéis de endomorfismos, mas que tem nesses anéis imagens anulares homomorfas [(I), págs. 231 e seguintes]. Tem-se, então:

TEOREMA 6: — *O anel* $\overline{\mathfrak{R}}$, *dos endomorfismos* — $\mathfrak{R}$ *da soma directa discreta* $\mathbf{M} = \sum_{\mu \in \mathrm{M}} \mathfrak{m}_\mu$, *dos módulos* $\mathfrak{m}_\mu$, *supondo* $1 = \sum_{\rho \in \mathrm{M}} \mathrm{E}_\rho$, *é soma directa completa dos ideais direitos* $\mathrm{E}_\rho \overline{\mathfrak{R}}$. Bem entendido que a soma considerada de ideais é simplesmente uma soma completa de módulos.

TEOREMA 7: — *O anel* $\overline{\mathfrak{R}}$ *do teorema anterior é soma directa completa dos anéis* $\overline{\mathfrak{R}}_{\alpha\beta} = \mathrm{E}_\alpha \overline{\mathfrak{R}}\,\mathrm{E}_\beta$.

TEOREMA 8: — *Dada a soma directa discreta* $\mathbf{M} = \Sigma\,\mathfrak{m}_\mu$, *referida no teorema 6, o anel* $\overline{\mathfrak{R}}_{\alpha\alpha} = \mathrm{E}_\alpha \overline{\mathfrak{R}}\,\mathrm{E}_\alpha$ *é isomorfo do anel dos endomorfismos* — $\mathfrak{R}$ *do sub-módulo* $\mathfrak{m}_\alpha$. Deve ter-se em conta que o teorema 49 do § em referência supunha os $\mathfrak{m}_\mu$ todos isomorfos — $\mathfrak{R}$ e que o lema 1 do mesmo § foi demonstrado nessa concordância.

4) **Módulos sub-directamente irredutíveis** — Como módulo sub-directamente irredutível, entende-se aquele que só pode ser representado por uma soma sub-directa, se uma das componentes for isomorfa do módulo. Ou ainda: módulo — — Ω sub-directamente irredutível é aquele em que a intersecção de todos os sub-módulos — Ω diferentes de zero é diferente de zero. O módulo (o) considera-se sub-directamente irredutível. Um módulo simples é sub-directamente irredutível. Inversamente, um módulo sub-directamente irredutível $\mathbf{M}$, tal que, para todo o sub-módulo $\mathbf{N}$, exista sub-módulo $\mathbf{N}'$ verificando a igualdade $\mathbf{M}=\mathbf{N}+\mathbf{N}'$, é simples; uma das parcelas é (o).

O teorema 6, de [27, § 3], tem aqui o seguinte:

TEOREMA 9: — *Todo o módulo — Ω é isomorfo duma soma sub-directa de módulos — Ω sub-directamente irredutíveis.*

Se $\mathbf{M}$ é um módulo — Ω com uma característica finita q, sabemos que é soma directa de sub-módulos — Ω cujas características são as potências dos números primos que entram na decomposição de q, [veja-se, adiante, o § 8]. Suposto $\mathbf{M}$ sub-directamente irredutível, tem-se:

TEOREMA 10: — *Um módulo — Ω sub-directamente irredutível tem a característica igual a zero ou a uma potência dum número primo.*

Outras propriedades dos módulos sub-directamente irredutíveis exprimem-se pelas proposições que vão seguir-se.

Consideremos o sub-módulo mínimo $\mathfrak{L}\neq(o)$, de $\mathbf{M}$, e designemos por $\mathfrak{n}$ o respectivo ideal de contracções. A hipótese $\mathfrak{n}^2\neq(o)$ arrasta a regularidade de $\mathfrak{n}$ e a existência de idempotente $E\in\overline{\Omega}$ tal que $\mathbf{M}E=\mathfrak{L}$. Como não pode ter-se $\mathbf{M}=\mathbf{M}E+\mathbf{M}(1-E)$, a não ser que $1-E=o$, $\mathbf{M}=$ $=\mathbf{M}E=\mathfrak{L}$, conclui-se $\mathbf{M}=\mathfrak{L}$. Inversamente, se $\mathbf{M}$ é simples, é $\mathfrak{L}=\mathbf{M}$, $\mathfrak{n}^2\neq(o)$. Assim:

TEOREMA 11: — *É condição necessária e suficiente, para que um módulo — Ω sub-directamente irredutível seja simples, que seja regular o ideal $\mathfrak{n}$ de contracções de $\mathbf{M}$ no seu sub-módulo mínimo $\mathfrak{L}\neq(o)$.*

Suponhamos, em seguida, $\mathfrak{n}^2=(o)$, com $\mathfrak{n}\neq(o)$. Se $o\neq$ $\neq A\in\overline{\Omega}$ é um divisor de zero à direita, tem-se, por ex., $BA=o$, com $B\neq o$. Será $\mathfrak{L}\subseteq\mathbf{M}B$, $\mathfrak{L}A=(o)$. Se A não é divisor de zero à direita, não pode ter-se $\mathfrak{L}A=(o)$, visto que, de contrário, seria $\mathbf{M}\mathfrak{n}=\mathfrak{L}$, $\mathbf{M}\mathfrak{n}A=\mathfrak{L}A=(o)$, $\mathfrak{n}A=(o)$, contra a hipótese feita sobre A. Deste modo, vale o

TEOREMA 12: — *O ideal aniquilador de $\mathfrak{L}$ compõe-se dos divisores de zero à direita, do anel $\overline{\Omega}$, suposto $\mathfrak{n}^2=(o)$, $\mathfrak{n}\neq(o)$.*

Podemos fazer ainda as seguintes observações: 1.ª) se $\mathfrak{n}\neq(o)$, existe sempre $A\in\overline{\Omega}$ tal que $\mathfrak{L}=\mathbf{M}A$; 2.ª) se $\mathfrak{n}=(o)$, tem-se, para cada $A\in\overline{\Omega}$, $\mathfrak{L}\subset\mathbf{M}A$; 3.ª) se $\mathfrak{n}\neq(o)$, o ideal aniquilador $\mathfrak{D}$, de $\mathfrak{L}$, é o mesmo que o ideal direito aniquilador de $\mathfrak{n}$, em $\overline{\Omega}$; 4.ª) o módulo — Ω, aniquilador de $\mathfrak{D}$, tem um ideal de contracções igual ao ideal esquerdo que aniquila $\mathfrak{D}$, à esquerda.

É ocasião de transportarmos para a teoria dos módulos sub-directamente irredutíveis os raciocínios de N. H. McCoy, estabelecidos em [18] e reproduzidos em [27, § 3]. Pelo que respeita ao teorema 8 do referido §, limitamo-nos a dar aqui uma sucessão de enunciados, que faz a decomposição do seu conteúdo no caso em questão. O domínio Ω vai ser substituído por um anel comutativo $\mathfrak{S}$.

TEOREMA 13: — *Seja $\mathbf{M}$ um módulo — $\mathfrak{S}$ sub-directamente irredutível e suponhamos $\mathfrak{S}$ comutativo e tal que o sub-módulo mínimo $\mathfrak{L}\neq(o)$, de $\mathbf{M}$, é trivial — $\mathfrak{S}$ (significa: $\mathfrak{L}\mathfrak{S}=(o)$); então, $\mathfrak{L}$ é finito e cíclico e tem uma característica igual a um número primo p.*

TEOREMA 14: — *Seja $\mathbf{M}$ um módulo — $\mathfrak{S}$ sub-directamente irredutível, nas condições do teorema anterior; então, admitindo que $o\neq\mathrm{x}\in\mathbf{M}$ é tal que $\mathrm{x}\,\mathfrak{S}=(o)$, existem um número* *primo fixo (característica de* $\mathfrak{L}\neq(\mathrm{o})$*) e um inteiro* ρ*, função de* x*, satisfazendo a* $\mathrm{p}^{\rho}\mathrm{x}=\mathrm{o}$.

TEOREMA 15: — *Seja* M *um módulo* — $\mathfrak{S}$ *sub-directamente irredutível, nas condições do teorema 13; então, é condição necessária e suficiente, para que* $\mathrm{y}\in\mathfrak{L}$*, que tenham lugar as duas relações:* $\mathrm{y}\,\mathfrak{S}=(\mathrm{o})$, $\mathrm{p}\,\mathrm{y}=\mathrm{o}$.

TEOREMA 16: — *Se* M *é um módulo* — $\mathfrak{S}$ *nas condições dos teoremas 13 a 15, para cada* x *tal que* $\mathrm{o}\neq\mathrm{x}\in\mathrm{M}$, $\mathrm{x}\,\mathfrak{S}\neq(\mathrm{o})$*, existe* $\mathrm{A}\in\mathfrak{S}$ *verificando a relação* $\mathrm{x}\,\mathrm{A}=\mathrm{x}_{\mathrm{o}}$*, suposto* x_{o} *um elemento fixo gerador de* $\mathfrak{L}$: $\mathfrak{L}=\}\mathrm{m}\,\mathrm{x}_{\mathrm{o}}+\mathrm{x}_{\mathrm{o}}\mathfrak{S}\{$*, com* m *inteiro.*

As propriedades expressas nos teoremas 13 a 16 são características, nos termos do seguinte

TEOREMA 17: — *Seja* M *um módulo* — $\mathfrak{S}$ *e suponhamos* $\mathfrak{S}$ *comutativo; é suficiente, para que* M *seja sub-directamente irredutível, que* M *possua as propriedades seguintes:* 1) *exista um sub-módulo da forma* $\mathfrak{L}=\}\mathrm{m}\,\mathrm{x}_{\mathrm{o}}\{\neq(\mathrm{o})$*, tal que* $\mathfrak{L}\,\mathfrak{S}=(\mathrm{o})$; 2) *para cada* $\mathrm{o}\neq\mathrm{x}\in\mathrm{M}$*, tal que* $\mathrm{x}\,\mathfrak{S}=(\mathrm{o})$*, existam um número primo fixo* p *e um inteiro* ρ *satisfazendo a* $\mathrm{p}^{\rho}\,\mathrm{x}=\mathrm{o}$; 3) *sempre que* $\mathrm{x}\,\mathfrak{S}=(\mathrm{o})$, $\mathrm{p}\,\mathrm{x}=\mathrm{o}$*, e apenas nesse caso, seja* $\mathrm{x}\in\mathfrak{L}$; 4) *supondo* $\mathrm{x}\,\mathfrak{S}\neq(\mathrm{o})$*, exista* $\mathrm{A}\in\mathfrak{S}$ *tal que* $\mathrm{x}\,\mathrm{A}=\mathrm{x}_{\mathrm{o}}$.

Quanto ao teorema 7 do citado § 3, de [27], as proposições correspondentes a estabelecer aqui implicam raciocínios que alteram ligeiramente os de N. H. McCoy. Esse facto obriga-nos a detalhá-los.

Vamos supor a existência, em $\mathfrak{S}$, de certos elementos que não anulam $\mathfrak{L}$. A primeira proposição a estabelecer é a seguinte:

TEOREMA 18: — *Se* $\mathfrak{S}$ *é comutativo e* M *é módulo* — $\mathfrak{S}$ *sub-directamente irredutível, supondo que o sub-módulo mínimo* $\mathfrak{L}\neq(\mathrm{o})$*, de* M*, tem um aniquilador* $\Delta=(\mathrm{o})$*, então* $\mathfrak{S}$ *é um corpo e* M *é simples* — $\mathfrak{S}$. Escrevamos $\mathfrak{L}=\}m\,x_o+x_o\mathfrak{S}\{$, onde $o\neq x_o\in\mathfrak{L}$ e m percorre os inteiros. É claro que o aniquilador de x_o é $\Delta=(o)$ e que $\mathfrak{S}$ é anel irredutível, concretizado como anel de endomorfismos de $\mathfrak{L}$. Sabemos que $\mathfrak{S}$ é um corpo, [26, § 2, teor. 8]. Reconhece-se directamente esse facto do modo que vai ver-se. O comu-

tador de $\mathfrak{S}$, no anel dos endomorfismos de $\mathfrak{L}$, é um anel de divisão $\overline{\mathfrak{S}}\supseteq\mathfrak{S}$. Se tomarmos $o\neq C$, $A\in\mathfrak{S}$, a equação $C X=A$ é solúvel em $\mathfrak{S}$, pois que, tendo-se $x_o C\neq o$, $x_o C\,\mathfrak{S}=\mathfrak{L}$, existe $X\in\mathfrak{S}$ tal que $x_o C X=x_o A\neq o$. Daqui tira-se $x_o(C X-A)=o$, $C X=A$, como se deseja. Passemos a provar que M é simples. Se for $o\neq x\in\mathrm{M}$, do facto de se ter $\mathfrak{L}\subseteq\}m\,x+x\,\mathfrak{S}\{$, conclui-se que o aniquilador de x é nulo. Ter-se-á $\mathfrak{L}\subseteq x\,\mathfrak{S}$, e, assim, existe $B\in\mathfrak{S}$ tal que $x B=x_o$. O elemento $1\in\mathfrak{S}$ é necessàriamente operador unitário do módulo, pois, de $x-x.1\neq o$, deduziríamos $(x-x.1)A\neq o$, se $A\neq o$, o que é absurdo. Em face disso, tem-se $x B B^{-1}=x=x_o B^{-1}\in\mathfrak{L}$, e, portanto, $\mathrm{M}=\mathfrak{L}$. O teorema está completamente provado.

Depois disto, surge o caso de $\mathfrak{L}$ não ser trivial — $\mathfrak{S}$ e de o seu aniquilador ser $\Delta\neq(o)$. Vamos mostrar, ainda directamente, que a congruência $A X\equiv B\,(\Delta)$ é solúvel, sempre que $A\notin\Delta$. Ponhamos $\mathfrak{L}=(x_o)=\}m\,x_o+x_o\mathfrak{S}\{$. Visto que $x_o A\neq o$, é também $x_o A\,\mathfrak{S}\neq(o)$, pois a igualdade $x_o A\,\mathfrak{S}=(o)$ daria $\mathfrak{L}=\{m\,x_o A\}$, $\mathfrak{L}=x_o\mathfrak{S}$, e daqui concluiríamos a existência de $B\in\mathfrak{S}$ tal que $x_o B=x_o$, $x_o B A=x_o A B=x_o A=o$. Será, deste modo, válida a relação $x_o A\,\mathfrak{S}=\mathfrak{L}$, que implica haver $T\in\mathfrak{S}$ tal que $x_o A T=x_o$. Deduz-se, então, $x_o(A T B-B)=o$, $A T B-B\in\Delta$, ou seja $A T B\equiv B\,(\Delta)$. A congruência em questão é resolvida pondo $X=T B$. O anel cociente $\mathfrak{S}/\Delta$ é um corpo. O seu elemento um $=\overline{1}$ é operador unitário de $\mathfrak{L}$, visto que, se fosse $x_o-x_o.\overline{1}=y\neq o$, ter-se-ia $\mathfrak{L}=\{m\,y\}$, $\mathfrak{L}\,\mathfrak{S}=(o)$. É válido o

TEOREMA 19: — *Se* $\mathfrak{S}$ *é comutativo e* M *é módulo* — $\mathfrak{S}$ *sub-directamente irredutível, supondo que o módulo mínimo* $\mathfrak{L}\neq(\mathrm{o})$*, de* M*, tem um aniquilador* $\Delta\neq(\mathrm{o})$ *mas não é trivial* — $\mathfrak{S}$*, então,* $\mathfrak{S}/\Delta$ *é um corpo, cujo elemento um é operador unitário de* $\mathfrak{L}$.

A relação $\mathfrak{L}\,\Delta=(o)$ mostra-nos haver elementos não nulos pertencentes ao sub-módulo — $\mathfrak{S}$ que aniquila Δ. Se x é um tal elemento, não pode ter-se $x\,\mathfrak{S}=(o)$, por esta razão: seria $\mathfrak{L}\subseteq\{m\,x\}$, $\mathfrak{L}\,\mathfrak{S}=(o)$, contra a hipótese de $\mathfrak{L}$ não ser trivial — $\mathfrak{S}$. Sendo, desse modo, $x\,\mathfrak{S}\neq(o)$, $\mathfrak{L}\subseteq x\,\mathfrak{S}$, existirá $A\in\mathfrak{S}$ tal que $x A=x_o$. Então, se $B\notin\Delta$,

$xAB = x_0 B \neq o$, e, consequentemente, $AB \notin \Delta$, pois foi feita a hipótese $x\Delta = (o)$. Da congruência acima estudada, resulta $ABS = B + D$, com $S \in \mathfrak{S}$, $D \in \Delta$. Em seguida, tem-se $xABS = xB$. Por ser $xA = x_0$, é também $x_0 BS = xB$, $(x_0 S - x) B = o$, e daqui vamos deduzir $x_0 S = x$. Na verdade, se $y = x_0 S - x \neq o$, será $y\mathfrak{S} \neq (o)$, pela mesma razão que acima. Concluiríamos $\mathfrak{L} \subseteqq y\mathfrak{S}$, $\mathfrak{L}B \subseteqq yB\mathfrak{S} = (o)$, contra a hipótese $B \notin \Delta$. É, assim, $x = x_0 S \in \mathfrak{L}$, o que nos permite afirmar:

TEOREMA 20: — *Se* $\mathfrak{S}$ *é comutativo e* $\mathbf{M}$ *é módulo* — $\mathfrak{S}$ *sub-directamente irredutível, supondo que o módulo mínimo* $\mathfrak{L} \neq (\mathrm{o})$, *de* $\mathbf{M}$, *tem um aniquilador* $\Delta \neq (\mathrm{o})$ *mas não é trivial* — $\mathfrak{S}$, *então* $\mathfrak{L}$ *e* Δ *são aniquiladores recíprocos.*

Finalmente, do facto de se ter, para $x \notin \mathfrak{L}$, $x\Delta \neq (o)$, concluímos $\mathfrak{L} \subseteqq x\Delta$, e, portanto, concluímos também a existência de $D_1 \in \Delta$ tal que $xD_1 = x_0$. Tem lugar o seguinte

TEOREMA 21: — *Se* $\mathbf{M}$ *é um módulo* — $\mathfrak{S}$ *nas condições dos teoremas 19 e 20, para cada* $\mathrm{x} \notin \mathfrak{L}$, *deduz-se a existência de* $\mathrm{D}_1 \in \Delta$ *tal que* $\mathrm{x}\,\mathrm{D}_1 = \mathrm{x}_0$.

As propriedades expressas nos teoremas 19 a 21 são características, à face desta inversa:

TEOREMA 22: — *Seja* $\mathbf{M}$ *um módulo* — $\mathfrak{S}$ *e suponhamos* $\mathfrak{S}$ *comutativo; é suficiente, para que* $\mathbf{M}$ *seja sub-directamente irredutível, que tenham lugar as seguintes propriedades:* 1) *existe um sub-módulo* — $\mathfrak{S}$ *da forma* $\mathfrak{L} = \{\mathrm{m}\,\mathrm{x}_0 + \mathrm{x}_0\mathfrak{S}\} \neq (\mathrm{o})$, *com um aniquilador* $\Delta \neq \mathfrak{S}$; 2) $\mathfrak{S}/\Delta$ *seja um corpo, com o elemento um operador unitário de* $\mathfrak{L}$; 3) $\mathfrak{L}$ *e* Δ *sejam aniquiladores recíprocos;* 4) *para cada* $\mathrm{x} \notin \mathfrak{L}$, *exista* $\mathrm{D}_1 \in \Delta$ *tal que* $\mathrm{x}\,\mathrm{D}_1 = \mathrm{x}_0$. Se as quatro propriedades têm lugar, vamos provar que, sendo $o \neq x \in \mathbf{M}$, é sempre $\mathfrak{L} \subseteqq (x) = \{mx + x\mathfrak{S}\}$. Quando $x \notin \mathfrak{L}$, em virtude de 4), tem-se $xD_1 = x_0$, $\mathfrak{L} \subseteqq x\mathfrak{S} \subseteqq (x)$. Se $x \in \mathfrak{L}$, é $x\Delta = (o)$, em face de 3). Distinguiremos, então, dois casos. Pode existir $F \notin \Delta$ tal que $xF \neq o$, ou não existir. No 2.° caso, teríamos $x\mathfrak{S} = (o)$, $x\mathfrak{S}/\Delta = (o)$, o que iria de encontro a 2). Será, assim, $xF \neq o$, para um certo $F \notin \Delta$. Se escrevermos $x = x_0 B + nx_0$, onde $B \in \mathfrak{S}$ e n é inteiro, deduzimos $xF = x_0 BF + nx_0 F \neq o$. Então, $BF + nF \notin \Delta$, o que leva a uma igualdade da forma $(BF + nF + \Delta)(G + \Delta) = \overline{1} \in \mathfrak{S}/\Delta$, e, consequentemente, leva a $x_0(BF + nF)G = x_0$, ou seja $xFG = x_0$. Ter-se-á $\mathfrak{L} \subseteqq (x)$, q. e. d.

OBSERVAÇÕES: — Não há necessidade de excluir, no teorema anterior, a hipótese $\Delta = (o)$. De facto, em virtude de 3), será $\mathfrak{L} = \mathbf{M}$, o que implica desde logo a exclusão de 4). Depois, recai-se na proposição seguinte:

Se $\mathbf{M}$ é um módulo sobre um corpo comutativo $\mathfrak{S}$, cujo elemento um é operador unitário de $\mathbf{M}$, e se tem um único gerador, então $\mathbf{M}$ é simples — $\mathfrak{S}$. Admitindo, porém, que se toma a hipótese $\Delta = (o)$, com exclusão das propriedades 3) e 4), então $\mathfrak{L}$ será irredutível — $\mathfrak{S}$, mas não se prova a irredutibilidade sub-directa de $\mathbf{M}$. Pelo contrário, decompondo $\mathbf{M}$ sob a forma $\mathbf{M} = \mathbf{M}' + \mathbf{M}''$, onde $\mathbf{M}'$ é o sub-módulo — $\mathfrak{S}$ composto dos elementos que são anulados por $\mathfrak{S}$ e $\mathbf{M}''$ é o sub-módulo — $\mathfrak{S}$ para cujos elementos $1 \in \mathfrak{S}$ é operador unitário, resulta, da teoria dos módulos semi-simples, [§ 5], que $\mathbf{M}''$ é semi-simples, $\mathfrak{L}$ é sua parcela directa, e, portanto, parcela directa de $\mathbf{M}$.

5) **Módulos semi-simples** — Um módulo $\mathbf{M}$, com um domínio operatório $\mathfrak{R}$, que pode não ser um anel, diz-se *semi-simples*, se for gerado pelos seus sub-módulos simples — $\mathfrak{R}$. Dos resultados estabelecidos no § 4, de [27], conclui-se que, para todo o anel $\mathfrak{S} \neq (o)$, semi-simples no sentido de JACOBSON, existe módulo — $\mathfrak{S}$ semi-simples fiel. Vamos provar a inversa, por forma a ficar estabelecido este

TEOREMA 23: — *É condição necessária e suficiente, para que* $\mathfrak{S} \neq (\mathrm{o})$ *seja semi-simples, que exista módulo* — $\mathfrak{S}$ *semi-simples fiel.* A suficiência da condição assenta no seguinte

LEMA 7: — *É condição necessária e suficiente, para que* $\mathbf{M}$ *seja semi-simples, que* $\mathbf{M}$ *possa tomar a forma* $\mathbf{M} = \Sigma\,\mathfrak{m}_\nu$, *como soma directa discreta de sub-módulos* $\mathfrak{m}_\nu$ *simples*. A condição é *necessária:* Se $\mathbf{M}$ é semi-simples, tomemos o conjunto C de todos os sub-módulos simples de $\mathbf{M}$: $C = \{\mathfrak{m}_\alpha, \mathfrak{m}_\beta, \ldots, \mathfrak{m}_\lambda, \ldots\}$. Em seguida, designemos por S o conjunto de todas as somas directas discretas formadas com elementos de C. Será $S=\{\mathfrak{m}_\alpha, \mathfrak{m}_\beta, \dots, \mathfrak{m}_\alpha+\mathfrak{m}_\beta, \dots, \Sigma\mathfrak{m}_\lambda, \dots\}$, suposto, bem entendido, $\mathfrak{m}_\alpha \neq \mathfrak{m}_\beta$, assim como $\Sigma\mathfrak{m}_\lambda$ uma soma tal que todo o seu elemento $m_\rho + m_\sigma + \dots + m_\tau$, com $m_\rho \in \mathfrak{m}_\rho$, etc., só pode ser o elemento nulo, se for, em separado, $m_\rho = m_\sigma = \dots = m_\tau = o$. O conjunto S é uma ordem parcial. Vamos tomar, em S, um sub-conjunto ordenado T. Existe um majorante mínimo para T, que é aquela soma directa discreta construída com o conjunto unido dos $\mathfrak{m}_\mu$ pertencentes às somas que figuram em T. Vê-se imediatamente, com efeito, que não pode ter-se $m_{\alpha'} + m_{\beta'} + \dots + m_{\sigma'} = o$, quando $m_{\alpha'}, \dots, m_{\sigma'}$ pertencem aos citados $\mathfrak{m}_\mu$, sem que seja $m_{\alpha'} = \dots = m_{\sigma'} = o$, pois, figurando $m_{\alpha'}, \dots, m_{\sigma'}$ numa soma do conjunto T, a hipótese contrária levaria à dependência de $m_{\alpha'}, \dots, m_{\sigma'}$. Conclui-se, deste modo, que S é um conjunto indutivo, [23, § 5], havendo em S, pelo princípio de ZORN, um elemento máximo $\Sigma\mathfrak{m}_\nu$. Então será $\mathbf{M}=\Sigma\mathfrak{m}_\nu$, porque, se pudesse existir $\mathfrak{m}_\alpha$ não pertencente a $\Sigma\mathfrak{m}_\nu$, a soma directa discreta $\mathfrak{m}_\alpha + \Sigma\mathfrak{m}_\nu$ mostraria que $\Sigma\mathfrak{m}_\nu$ não era máxima.

A condição é *suficiente:* Esta afirmação é trivial.

Passemos à 2.ª parte do teorema 23. Dado $\mathfrak{S} \neq (o)$, suponhamos $\mathbf{M}$ um módulo semi-simples fiel. Escrevendo, nos termos do lema, $\mathbf{M}=\Sigma\mathfrak{m}_\mu$, o teorema 17′, do referido § 4, de [27], leva à conclusão desejada.

Eis agora outro teorema característico dos módulos semi-simples.

TEOREMA 24: — *É condição necessária e suficiente, para que* $\mathbf{M}$ *seja semi-simples, que todo o sub-módulo* $\mathbf{N}$, *de* $\mathbf{M}$, *seja parcela directa duma soma da forma* $\mathbf{M}=\mathbf{N}+\mathbf{N}'$. Partamos de $\mathbf{M}$, suposto semi-simples. Tomemos $\mathbf{N} \neq \mathbf{M}$ e consideremos os sub-módulos simples $\mathfrak{m}_\alpha, \mathfrak{m}_\beta, \dots$, de $\mathbf{M}$, não contidos em $\mathbf{N}$. Claramente que $\mathbf{M}$ será gerado por $\mathbf{N}$ e por esses sub-módulos. Tomemos em seguida, como conjunto S, o conjunto das somas directas $S=\{\mathbf{N}, \mathbf{N}+\mathfrak{m}_\alpha, \dots, \mathbf{N}+\Sigma\mathfrak{m}_\lambda, \dots\}$. Um raciocínio análogo ao do teorema anterior leva à existência de elemento máximo em S, para o qual se tem $\mathbf{M}=\mathbf{N}+\Sigma\mathfrak{m}_\nu$, de sorte que

se responde ao teorema pondo $\mathbf{N}'=\Sigma\mathfrak{m}_\nu$. Passemos à inversa. Por um lado, sabemos que, dado $\mathbf{M}$, este é sempre isomorfo duma soma sub-directa de módulos sub-directamente irredutíveis $\mathfrak{m}_\mu$. Então, do homomorfismo $\mathbf{M} \sim \mathfrak{m}_\mu$, concluímos $\mathfrak{m}_\mu \simeq \mathbf{M}/\mathbf{M}_\mu$, e, da propriedade atribuída a $\mathbf{M}$ no enunciado, deduzimos $\mathbf{M}=\mathbf{M}_\mu+\mathbf{M}'_\mu$. Os sub-módulos $\mathbf{M}'_\mu$ são sub-directamente irredutíveis; e, como gozam da mesma propriedade são simples. Consideremos, em seguida, a soma directa $\mathbf{M}'$, de todos os sub-módulos simples de $\mathbf{M}$. Ter-se-á $\mathbf{M}=\mathbf{M}'+\mathbf{M}''$. O sub-módulo $\mathbf{M}''$ é nulo, como vamos ver. Em primeiro lugar, ele goza da propriedade atribuída a $\mathbf{M}$; por isso ao escrever-se $\mathbf{M}''$ como soma sub-directa de módulos sub-directamente irredutíveis $\mathfrak{m}''_\rho$ e ao pôr-se $\mathfrak{m}''_\rho \simeq \mathbf{M}''/\mathbf{M}''_\rho$, também é $\mathbf{M}''=\mathbf{M}''_\rho+\mathbf{M}'''_\rho$. Depois, todos os $\mathbf{M}'''_\rho \simeq \mathfrak{m}''_\rho$ são simples, consequentemente nulos, visto que $\mathbf{M}''$ não tem sub-módulos simples. Daí resulta $\mathbf{M}''=\mathbf{M}''_\rho$, $\mathfrak{m}''_\rho=(o)$, $\mathbf{M}''=(o)$. O teorema está provado.

O modo de raciocinar na 1.ª parte do teorema anterior leva ao seguinte

TEOREMA 25: — *Se o módulo semi-simples* $\mathbf{M}$ *tem a forma de soma directamente* $\mathbf{M}=\Sigma\mathfrak{m}_\mu$, *onde os* $\mathfrak{m}_\mu$ *são simples, dado um sub-módulo* $\mathbf{N}$, *de* $\mathbf{M}$, *ao escrever-se* $\mathbf{M}=\mathbf{N}+\mathbf{N}'$, *podemos supor o sub-módulo* $\mathbf{N}'$ *soma directa discreta de certos módulos* $\mathfrak{m}_\mu$. Na verdade, chega a estabelecer-se também $\mathbf{M}=\mathbf{N}+\Sigma\mathfrak{m}_\nu$, tendo o cuidado de tomar os sub-módulos simples de $\mathbf{M}$ não contidos em $\mathbf{N}$ que façam parte da soma $\Sigma\mathfrak{m}_\mu$.

Na decomposição dum módulo semi-simples $\mathbf{M}$ sob a forma $\mathbf{M}=\Sigma\mathfrak{m}_\nu$, $(\nu \in M)$, há uma última propriedade que é importante assinalar. Suponhamos $\mathbf{M}=\Sigma\mathfrak{n}_j$, $(j \in N)$, uma nova soma directa discreta representando $\mathbf{M}$. É válido o

TEOREMA 26: — *Os dois conjuntos* M *e* N *têm a mesma cardinalidade,* (Cfr. [32], págs. 240-241, assim como H. LÖVIG, *Über die Dimension linearer Räume,* «Studia Mathematica», vol. 5, 1934, págs. 18-23). A demonstração é a que vai ver-se. Se o número de parcelas de uma das somas directas for finito, o mesmo sucederá com a outra soma e os dois números são iguais. Faremos, assim, a hipótese de serem infinitos os dois conjuntos M e N. Admitamos mais que os $\mathfrak{m}_\nu$, $\mathfrak{n}_j$, $\mathbf{M}$ são módulos — $\mathfrak{S}$, por forma que $\mathfrak{m}_\nu = \{\dot{m}\, e_\nu + e_\nu \mathfrak{S}\}$, $\mathfrak{n}_j = \{n f_j + f_j \mathfrak{S}\}$, ($m, n$ inteiros; $e_\nu \in \mathfrak{m}_\nu$, $f_j \in \mathfrak{n}_j$).

Dado e_λ, tem-se sempre $e_\lambda = n_i f_i + \ldots + n_k f_k + f_i s_i + \ldots + f_k s_k$, onde os $n n$ são inteiros e os $s s$ pertencem a $\mathfrak{S}$. Nestas expressões dos e_λ intervêm todos os f_j, visto que, se f_q não figurasse em qualquer decomposição, escrevendo, por sua vez, $f_q = m_\alpha e_\alpha + \ldots + m_\rho e_\rho + e_\alpha t_\alpha + \ldots + e_\rho t_\rho$, onde os $m m$ são inteiros e os $t t$ pertencem a $\mathfrak{S}$, ao fazer aqui a substituição dos $e_\alpha, \ldots, e_\rho$ pelas suas expressões nos f_j, chegava-se a concluir não ser $\Sigma\, \mathfrak{n}_j$ uma soma directa discreta. Tomado agora $j \in N$, consideremos f_j e procuremos os e_ν em cujas expressões figura f_j. A cada j fazemos corresponder dessa maneira um sub-conjunto não vazio $\{\lambda, \mu, \ldots\} \subset M$, precisamente o sub-conjunto formado pelos índices ν, dos e_ν referidos. O axioma da escolha permite, em seguida, considerar uma função Θ de conjunto, seleccionando um elemento em cada sub-conjunto. Poremos $\nu = \Theta(j)$. Os $\nu\nu$ percorrerão uma parte $M' \subset M$, tendo sentido falar de $j = \Theta^{-1}(\nu)$. A função $\Theta^{-1}(\nu)$ é multívoca, contràriamente a Θ. Podem, de facto, vários jj levar a sub-conjuntos com elementos comuns, de sorte que, na escolha determinada por Θ, pode um mesmo elemento ser repetido. Em qualquer caso, só aparecerá um número finito de vezes, existindo uma correspondência biunívoca entre os $\nu \in M'$ e os sub-conjuntos *finitos e disjuntos* $\Theta^{-1}(\nu) \subset N$. O número cardinal do conjunto dos $\Theta^{-1}(\nu)$ é o mesmo que o de uma parte M', de M. Invertendo os papéis de M e de N, chega-se a uma parte N', de N, com o mesmo número cardinal que M. Assim, M e N têm a mesma cardinalidade, como se afirmou.

Exemplo importante de módulo — $\mathfrak{S}$ semi-simples é dado por todo o módulo $\mathbf{M}$ relativo a um anel $\mathfrak{S}$ semi-simples noetheriano, sob a hipótese de $1 \in \mathfrak{S}$ ser operador unitário de $\mathbf{M}$. Fazendo, com efeito, a decomposição $\mathfrak{S} = \mathfrak{r}_1 + \ldots + \mathfrak{r}_n$, em ideais direitos simples, tem-se, para cada $m \in \mathbf{M}$, $m = m \cdot 1 = m e_1 + \ldots + m e_n$, onde os $e_i \in \mathfrak{r}_i$ são idempotentes ortogonais. A correspondência $\mathfrak{r}_i \to m\, \mathfrak{r}_i$,

$(i = 1, 2, \ldots, n)$, ou é o homomorfismo nulo ou um isomorfismo. Na decomposição anterior de m, as parcelas não nulas pertencem a sub-módulos simples do tipo $m\, \mathfrak{r}_j$. Então, $\mathbf{M}$ é gerado pelos seus sub-módulos simples, pelo que é semi-simples — $\mathfrak{S}$.

Quando $1 \in \mathfrak{S}$ não é operador unitário, a decomposição $\mathbf{M} = \mathbf{N} + \mathbf{N}'$, referida no teorema 24, é ainda válida, para cada $\mathbf{N}$ onde $1 \in \mathfrak{S}$ opere como operador unitário. É o que se reconhece imediatamente decompondo $\mathbf{M}$ sob a forma $\mathbf{M} = \mathbf{M}' + \mathbf{M}''$, na qual $\mathbf{M}'$ e $\mathbf{M}''$ são os dois sub-módulos — $\mathfrak{S}$ seguintes: o primeiro compõe-se dos elementos de $\mathbf{M}$ que são anulados por $\mathfrak{S}$; o segundo dos elementos de $\mathbf{M}$ para os quais $1 \in \mathfrak{S}$ é operador unitário. Então, será $\mathbf{N} \subseteq \mathbf{M}''$, $\mathbf{M}'' = \mathbf{N} + \mathfrak{L}$, $\mathbf{M} = \mathbf{N} + \mathfrak{L} + \mathbf{M}'$. Assim:

TEOREMA 27: — *Se $\mathfrak{S}$ é um anel semi-simples noetheriano e $\mathbf{M}$ um módulo — $\mathfrak{S}$, todo o sub-módulo — $\mathfrak{S}$, como $\mathbf{N}$, sob a hipótese de $1 \in \mathfrak{S}$ ser operador unitário de $\mathbf{N}$, é parcela directa duma soma igual a $\mathbf{M}$.*

Posto isto, tendo escrito, como no teorema 25, $\mathbf{M} = \Sigma\, \mathfrak{m}_\mu$, associemos separadamente os sub-módulos simples isomorfos. Pode obter-se

$$\mathbf{M} = \sum_{\nu' \in M'} \mathfrak{L}_{\nu'}, \quad M' = \{\alpha', \beta', \ldots, \nu', \ldots\}, \quad (1)$$

onde cada $\mathfrak{L}_{\nu'}$ é soma directa discreta de sub-módulos simples isomorfos, não isomorfos dos sub-módulos simples que entram noutro $\mathfrak{L}_{\mu'}$, $(\mu' \neq \nu')$. Precisemos, de resto, que, nos $\mathfrak{m}_\mu$, figuram sub-módulos isomorfos de *qualquer* sub-módulo simples de $\mathbf{M}$, pois que, se $\mathfrak{m}$ for um tal sub-módulo simples, dado $m \in \mathfrak{m}$, supondo $o \neq m_\alpha \in \mathfrak{m}_\alpha$ um elemento que figura na representação de m, tem-se, necessàriamente, $\mathfrak{m}_\alpha \simeq \mathfrak{m}$. Assim, se, para duas parcelas da soma (1), considerarmos a homomorfia $\mathfrak{L}_{\alpha'} \sim \mathfrak{L}'_{\beta'} \subseteq \mathfrak{L}_{\beta'}$, a hipótese $\beta' \neq \alpha'$ arrasta $\mathfrak{L}'_{\beta'} = (o)$. É válido este

TEOREMA 28: — *O anel $\overline{\mathfrak{R}}$, dos endomorfismos — $\mathfrak{R}$ dum módulo $\mathbf{M}$, semi-simples — $\mathfrak{R}$, é uma soma directa completa dos anéis $\overline{\mathfrak{R}}_{\alpha'\alpha'}$, soma que pode ser entendida no sentido anular. O produto de dois anéis parcelas distintos é nulo.*

Relativamente à estrutura de $\overline{\mathfrak{R}}_{\alpha'\alpha'} \simeq E_{\alpha'}\, \overline{\mathfrak{R}}\, E_{\alpha'}$, o teorema 8 deste artigo, combinado com o teorema 49 de [24, ou Cap. XV], permite o seguinte

Aditamento: — *Cada anel $\overline{\mathfrak{R}}_{\alpha'\alpha'}$ é isomorfo do anel formado pela totalidade das matrizes (transfinitas) de linhas somáveis de endomorfismos — $\mathfrak{R}$ pertencentes ao comutador de $\mathfrak{R}$ no anel dos endomorfismos — $\mathfrak{R}$ dum sub-módulo simples de $\mathfrak{L}_{\alpha'}$. Esse comutador é um anel de divisão.*

Podemos ir um pouco mais longe no estudo do anel dos endomorfismos duma soma directa discreta de sub-módulos isomorfos simples, quando o conjunto $\mathfrak{R}$ se supõe vazio, ou, pelo menos, se supõe um anel comutativo.

Se $\mathfrak{R}$ é vazio, o teorema 53 de [24] permite afirmar, então, que, se for $\mathfrak{A}$ o anel dos endomorfismos de $\mathbf{M} = \Sigma\, \mathfrak{m}_\mu$, $\mathbf{M}$ é irredutível — $\mathfrak{A}$. Assim:

Teorema 29: — *Se $\mathfrak{R}$ é um anel comutativo, o anel $\overline{\mathfrak{R}}$, dos endomorfismos — $\mathfrak{R}$, dum módulo $\mathbf{M} = \Sigma\, \mathfrak{m}_\mu$, soma directa discreta de módulos — $\mathfrak{R}$, simples e isomorfos, é um anel primitivo.* Mais geralmente ainda:

Teorema 30: — *Se $\mathfrak{R}$ é comutativo, um módulo — $\mathfrak{R}$ semi-simples tem um anel $\overline{\mathfrak{R}}$, de endomorfismos — $\mathfrak{R}$, que é semi-simples.* De facto, pelos teoremas 28 e 29, $\overline{\mathfrak{R}}$ é isomorfo duma soma directa completa de anéis primitivos. Então, à face de [27, teor. 19], a afirmação é imediata.

Exemplos importantes de módulos semi-simples são dados pelos módulos sobre um corpo (comutativo). Tomemos $\mathbf{M}$, sobre o corpo $\mathfrak{K}$, e suponhamos $1 \in \mathfrak{K}$ operador unitário em $\mathbf{M}$. Do teorema 51 de [24] resulta imediatamente, à face do actual teorema 24, que $\mathbf{M}$ é semi-simples. Tendo em conta que um módulo simples sobre $\mathfrak{K}$, quando $1 \in \mathfrak{K}$ é operador unitário, tem a forma $v\,\mathfrak{K}$, podemos afirmar que é

$$\mathbf{M} = \sum_{\lambda \in M} u_\lambda \mathfrak{K}, \qquad u_\lambda \mathfrak{K} \simeq v\,\mathfrak{K},$$

onde v deve ser compreendido como um simples símbolo e M é um conjunto determinado. Vale o seguinte

Teorema 31: — *É condição necessária e suficiente, para que $\mathbf{M}$ seja módulo sobre um corpo $\mathfrak{K}$ (cujo elemento um se supõe operador unitário de $\mathbf{M}$), que $\mathbf{M}$ seja semi-simples — $\mathfrak{K}$.*

Visto que $\mathfrak{K}$ é anel denso em $v\,\mathfrak{K}$, sobre $\mathfrak{K}$, $\mathfrak{K}$ é irredutível e é o seu próprio comutador, [Cap. XV, teor. 57]. Representando, como em geral, por $\overline{\mathfrak{K}}$, o comutador de $\mathfrak{K}$, mas agora no anel $\mathfrak{E}(\mathbf{M})$ dos endomorfismos de $\mathbf{M}$, sabemos que os sub-módulos — $\overline{\mathfrak{K}}$, de $\mathbf{M}$, estão em correspondência biunívoca com os sub-módulos — $\mathfrak{K}$, de $v\,\mathfrak{K}$, [Cap. XV, teor. 53]. Isto significa que $\mathbf{M}$ é irredutível — $\overline{\mathfrak{K}}$. *A fortiori*, $\mathbf{M}$ é irredutível — $\mathfrak{E}(\mathbf{M})$, o que também se exprime dizendo: $\mathbf{M}$ *é absolutamente irredutível*. Tem lugar o

Teorema 32: — *Se $\mathfrak{E}(\mathbf{M})$ significa o anel dos endomorfismos do módulo $\mathbf{M}$, todo o módulo $\mathbf{M}$ sobre um corpo é absolutamente irredutível, ou seja: é irredutível — $\mathfrak{E}(\mathbf{M})$.*

Como aplicação, tomemos um anel arbitrário $\mathfrak{S}$. Se p for um número primo, $p\,\mathfrak{S}$ é um ideal bilateral e $\mathfrak{S}/p\,\mathfrak{S} = \mathfrak{S}_p$ é um anel cociente. Para cada $\bar{a} \in \mathfrak{S}_p$ é $p\,\bar{a} = o$. Representando por (p) o ideal principal gerado por p no domínio dos inteiros, o anel cociente é módulo sobre o corpo $\mathfrak{K}_p = \{o + (p), 1 + (p), \ldots, p - 1 + (p)\}$, sendo $\overline{1} = 1 + (p)$ operador unitário no módulo. Pode ter-se $\mathfrak{S}_p = (o)$, o que implica $\mathfrak{S} = p\,\mathfrak{S}$. Se for, porém, $\mathfrak{S}_p \neq (o)$, todo o elemento não nulo do anel cociente tem a ordem p. Podemos formular este enunciado:

Teorema 33: — *Dado um anel arbitrário $\mathfrak{S}$, se, supondo p primo, for $\mathfrak{S} \neq \mathrm{p}\,\mathfrak{S}$, o anel cociente $\mathfrak{S}/\mathrm{p}\,\mathfrak{S}$, considerado como módulo, é absolutamente irredutível e compõe-se de elementos todos da mesma ordem prima p.*

Em vez de $\mathfrak{K}$, tomemos agora um anel de divisão $\mathfrak{D}$, cujo elemento um se supõe ainda operador unitário do módulo $\mathbf{M}$, sobre $\mathfrak{D}$. Tem-se igualmente:

Teorema 34: — *Dado um módulo $\mathbf{M}$, supondo $\mathfrak{D}$ um anel de divisão de endomorfismos de $\mathbf{M}$, $\mathbf{M}$ é semi-simples — $\mathfrak{D}$.*

Escrevamos, então, $\mathrm{M} = \sum_{\nu \in M} u_\nu \mathfrak{D}$, como soma directa discreta de módulos — $\mathfrak{D}$, simples, isomorfos — $\mathfrak{D}$ e com uma única dimensão. Para o anel $\overline{\mathfrak{D}}$, dos endomorfismos — $\mathfrak{D}$, de M, é válido o seguinte

TEOREMA 35: — *Se* M *se considera módulo sobre um anel de divisão* $\mathfrak{D}$ *dos seus endomorfismos, escrevendo* $\mathrm{M} = \sum_{\nu \in \mathrm{M}} \mathrm{u}_\nu \mathfrak{D}$, *como soma directa discreta, o anel* $\overline{\mathfrak{D}}$, *dos endomorfismos* — $\mathfrak{D}$, *de* M, *é isomorfo do anel de todas as matrizes com* M *dimensões, formadas por elementos dum anel de divisão* $\mathfrak{D}'$, *anti-isomorfo de* $\mathfrak{D}$, *de tal modo que cada linha da matriz tenha um número finito de elementos não nulos. E o anel dos endomorfismos* — $\overline{\mathfrak{D}}$, *de* M, *é isomorfo de* $\mathfrak{D}'$. *Além disso,* M *é irredutível* — $\overline{\mathfrak{D}}$, *e* $\mathfrak{D}$ *e* $\overline{\mathfrak{D}}$, *são comutadores recíprocos.* Dos 3 períodos em que se decompôs o enunciado, as afirmações contidas no 1.° e no 2.° são consequência imediata do corolário 16, § 14, de [24]. Que M é irredutível — $\overline{\mathfrak{D}}$, conclui-se do teorema 53, do mesmo § 14, de [24]. Finalmente, para se ver $\mathfrak{D}$ e $\overline{\mathfrak{D}}$ são comutadores recíprocos, bastará, em face de [24, § 12, teor. 50], identificar cada endomorfismo — $\overline{\mathfrak{D}}$ com um elemento de $\mathfrak{D}$. Se θ é um endomorfismo — $\overline{\mathfrak{D}}$, tomemos uma parcela fixa $u_\alpha \mathfrak{D}$, de M. Podemos escrever $u_\alpha \mathfrak{D} = u_\alpha \mathfrak{D}'$ (1), onde $\mathfrak{D}'$, anti-isomorfo de $\mathfrak{D}$, é aqui, precisamente, o anel de divisão dos endomorfismos — $\mathfrak{D}$, de $u_\alpha \mathfrak{D}$. Os raciocínios do citado teorema 50 mostram que θ define em $u_\alpha \mathfrak{D} = u_\alpha \mathfrak{D}'$ um endomorfismo — $\mathfrak{D}'$, ou seja, portanto, um elemento de $\mathfrak{D}$, que é independente do índice α.

OBSERVAÇÃO: — Querendo ter em vista o teorema de CHEVALLEY-JACOBSON, [24, § 16, teor. 57], do facto de $\overline{\mathfrak{D}}$ ser anel denso de endomorfismos — $\mathfrak{D}$, de M, resulta desde logo que $\mathfrak{D}$ é o comutador de $\overline{\mathfrak{D}}$. O poder, a elegância e a simplicidade do método de JACOBSON são manifestos a cada passo.

(1) Não se significa, com esta igualdade, $u_\alpha d = u_\alpha d'$, se d e d' se correspondem no anti-isomorfismo.

6) **Duas caracterizações dos anéis semi-simples noetherianos** — Neste §, assim como no próximo, ocupar-nos-emos dos resultados estabelecidos por GOLDMAN em [19] e [21], relativos a anéis semi-simples. Começaremos por demonstrar duas proposições gerais, também devidas àquele autor, e passaremos depois às duas caracterizações referidas em epígrafe.

$\mathfrak{S}$ significará, em geral, um anel não comutativo. São bem conhecidas as seguintes circunstâncias. Dado $\mathfrak{S}$, há sempre módulos — $\mathfrak{S}$. O próprio anel é um exemplo. Se $\mathfrak{S}$ tem elemento um, concretiza-se como anel de endomorfismos do seu grupo aditivo. Não existindo elemento um, $\mathfrak{S}$ pode «mergulhar-se» num anel $\mathfrak{S}^*$ contendo um tal elemento. Assim, qualquer que seja $\mathfrak{S}$, há sempre módulos — $\mathfrak{S}$ fiéis.

Um módulo — $\mathfrak{S}$ de que adiante faremos uso é o seguinte: considera-se o anel $\mathfrak{J}$ dos números inteiros, e, em seguida, define-se $\mathfrak{S} \times \mathfrak{J}$ como o conjunto dos elementos (a, n), $[a \in \mathfrak{S},\ n \in \mathfrak{J}]$, algebrizado por via da definição $(a, m) + (b, n) = (a + b, m + n)$. Obtém-se um módulo, que passa a módulo — $\mathfrak{S}$, pondo $(a, n)\, a' = (a a' + n a', o)$, $(a' \in \mathfrak{S},\ o =$ inteiro zero).

São úteis os dois teoremas que vão tratar-se.

TEOREMA 36: — *Se* $\mathfrak{S}$ *é um anel tal que todo o módulo* — $\mathfrak{S}$ *se escreve sob a forma* $\mathrm{M} = \mathrm{N} + \mathrm{N}'$, *como soma directa de módulos* — $\mathfrak{S}$, *o primeiro dos quais é o aniquilador modular de* $\mathfrak{S}$, *então, escrevendo* $\mathfrak{S} = \mathfrak{a} + \mathfrak{b}$, *onde* $\mathfrak{a}$ *é o aniquilador esquerdo de* $\mathfrak{S}$, *tem-se* $\mathfrak{a} = (\mathrm{o})$. Se existe $1 \in \mathfrak{S}$, a afirmação é trivial. Não sendo assim, «megulhemos» $\mathfrak{S}$ em $\mathfrak{S}^*$, como acima se disse. Escrevendo $\mathfrak{S}^* = \mathfrak{a}' + \mathfrak{b}'$, nos termos do enunciado, tem-se $\mathfrak{S}^* \mathfrak{a} = (\mathfrak{a}' \mathfrak{a}, \mathfrak{b}' \mathfrak{a}) = \mathfrak{b}' \mathfrak{a} \subseteq \mathfrak{b}'$, $(\mathfrak{S}^* \mathfrak{a}) \mathfrak{S} = \mathfrak{S}^* (\mathfrak{a} \mathfrak{S}) = (o)$, de sorte que $\mathfrak{S}^* \mathfrak{a} \subseteq \mathfrak{a}'$, $\mathfrak{S}^* \mathfrak{a} = (o)$, e, portanto, em virtude de existir $1 \in \mathfrak{S}^*$, $\mathfrak{a} = (o)$, q. e. d.

TEOREMA 37: — *Se o anel* $\mathfrak{S}$ *do teorema anterior tem uma característica finita* k, *existe elemento* $1 \in \mathfrak{S}$, [GOLDMAN, 19, pág. 1025]. Escrevamos, com efeito, $\mathfrak{S} \times \mathfrak{J} = \mathrm{N}_1 + \mathrm{N}_2$, onde N_1 é o aniquilador modular de $\mathfrak{S}$. Supondo $(o, 1) = (-a_o, 1 - n) + (a_o, n)$, onde as parcelas pertencem, respectivamente, a N_1 e a N_2, vamos verificar que é $n = o$.

Tem-se $k(a_o, n) = (k a_o, k n) = (o, k n) \in \mathbf{N}_2$, assim como $(o, k n)\, a = (k n a, o) = o$, qualquer que seja $a \in \mathfrak{S}$. Conclui-se também $(o, k n) \in \mathbf{N}_1$, e, portanto, $(o, k n) = o$, $k n = o$, $n = o$, como se afirmou. Deste modo, vale $(o, 1) = (-a_o, 1) + (a_o, o)$, de sorte que $(-a_o, 1) \in \mathbf{N}_1$ e $(-a_o, 1)\, a = o = (-a_o a + a, o)$, o que leva a $a = a_o a$. O elemento $a_o \in \mathfrak{S}$ é unidade esquerda. Dado agora qualquer $b \in \mathfrak{S}$, como se tem $(b - b a_o)\, a = o$, qualquer que seja a, valerá a inclusão $b - b a_o \in \mathfrak{a}$, onde $\mathfrak{a} = (o)$ foi referido no teorema anterior. Portanto, $b = b a_o$, como se deseja.

Os anéis semi-simples noetherianos, na ordem de ideias que estamos seguindo, são susceptíveis da caracterização seguinte, [19]:

Teorema 38: — *É condição necessária e suficiente, para que $\mathfrak{S}$ seja um anel semi-simples noetheriano, que todo o módulo — $\mathfrak{S}$ seja soma directa dum sub-módulo — $\mathfrak{S}$, que é o aniquilador modular de $\mathfrak{S}$, e dum sub-módulo — $\mathfrak{S}$, soma directa discreta de sub-módulos — $\mathfrak{S}$ simples.* A condição é *necessária:* Suponhamos $\mathfrak{S}$ um anel semi-simples noetheriano e $\mathbf{M}$ um módulo — $\mathfrak{S}$ qualquer. Façamos a decomposição $\mathbf{M} = \mathbf{M}' + \mathbf{M}''$, onde $\mathbf{M}'$ é aniquilado por $\mathfrak{S}$ e $\mathbf{M}''$ é um sub-módulo — $\mathfrak{S}$ que admite o elemento um de $\mathfrak{S}$ como operador unitário, [(I), pág. 81]. Trata-se de provar que $\mathbf{M}''$ é módulo — $\mathfrak{S}$ semi-simples. Façamos a decomposição $\mathfrak{S} = \mathfrak{r}_1 + \ldots + \mathfrak{r}_n$, em ideais direitos simples. Se $m \in \mathbf{M}''$ é tal que $m \mathfrak{r}_i \neq (o)$, a correspondência $\mathfrak{r}_i \sim m \mathfrak{r}_i$ é isomorfismo operatório relativamente a $\mathfrak{S}$. Assim, $m \mathfrak{r}_i$ é simples — $\mathfrak{S}$. Ora, dado $m \in \mathbf{M}''$ qualquer, é sempre $m . 1 = m e_1 + \ldots + m e_n$, onde os $e_i \in \mathfrak{r}_i$ são idempotentes ortogonais. Cada $m \in \mathbf{M}''$ pertence a uma soma finita de sub-módulos — $\mathfrak{S}$, simples, de $\mathbf{M}''$, pelo que $\mathbf{M}''$ é semi-simples, por ser gerado pelos seus sub-módulos simples.

A condição é *suficiente:* A demonstração assenta sobre o lema seguinte, devido a Goldman, [Cfr. teor. 35 e 36]:

Lema 8: — *Se $\mathfrak{S}$ é um anel tal que todo o módulo — $\mathfrak{S}$ se escreve sob a forma $\mathbf{M} = \mathbf{N} + \mathbf{N}'$, como soma directa de módulos — $\mathfrak{S}$, o primeiro dos quais é o aniquilador modular de $\mathfrak{S}$ e o outro é semi-simples, $\mathfrak{S}$ possui elemento um.*

Partamos da decomposição $\mathfrak{S} \times \mathfrak{J} = \mathbf{N}_1 + \mathbf{N}_2$, referida atrás, e demonstremos que é $\mathbf{N}_1 \neq (o)$. A hipótese $\mathbf{N}_1 = (o)$ acarretaria a semi-simplicidade de $\mathfrak{S} \times \mathfrak{J} = \mathbf{N}_2$. Pelo facto de ser $(\mathfrak{S}, o)$ um sub-módulo — $\mathfrak{S}$ próprio de $\mathfrak{S} \times \mathfrak{J}$, a igualdade $\mathfrak{S} \times \mathfrak{J} = (\mathfrak{S}, o) + \mathbf{N}_3$ dá $\mathbf{N}_3 \neq (o)$, sendo $\mathbf{N}_3 \mathfrak{S} \subseteq \mathbf{N}_3$. A forma dos elementos de $\mathbf{N}_3 \mathfrak{S}$ é (a, o), de sorte que é também $\mathbf{N}_3 \mathfrak{S} \subseteq (\mathfrak{S}, o)$, ou seja $\mathbf{N}_3 \mathfrak{S} = (o)$. Então, ter-se-á $(o) \neq \mathbf{N}_3 \subseteq \mathbf{N}_1$, o que não pode ter lugar com $\mathbf{N}_1 = (o)$.

Nestas condições, tomemos $o \neq (a_1, n_1) \in \mathbf{N}_1$. Para cada $b \in \mathfrak{S}$ é $a_1 b + n_1 b = o$, não podendo ter-se $n_1 = o$, visto que, de contrário, seria $a_1 b = o$, e, portanto, $a_1 \in \mathfrak{a}$, (Cfr. teor. 36), o que implicaria $a_1 = o$, $(a_1, n_1) = (o, o) = o$. Se, para o inteiro fixo n_1, fosse $n_1 \mathfrak{S} = (o)$, o teorema 34 era aplicável e o lema ficaria provado. Não sendo assim, vamos demonstrar que tem lugar a soma directa $\mathfrak{S} = \mathfrak{A} + \mathfrak{B}$, onde $\mathfrak{A}$ é o ideal bilateral de $\mathfrak{S}$ composto dos elementos a tais que $n_1 a = o$, e $\mathfrak{B} = n_1 \mathfrak{S}$. Em face das hipóteses e do teorema 33, $\mathfrak{S}$ é uma soma directa discreta de ideais direitos simples $\mathfrak{r}_\lambda$: $\mathfrak{S} = \sum_{\lambda \in C} \mathfrak{r}_\lambda$. As correspondências — $\mathfrak{S}$ da forma $\mathfrak{r}_\lambda \to n_1 \mathfrak{r}_\lambda$ implicam $n_1 \mathfrak{r}_\lambda = \mathfrak{r}_\lambda$ ou $n_1 \mathfrak{r}_\lambda = (o)$. Na primeira hipótese, a relação $n_1 t_\lambda = o$, com $t_\lambda \in \mathfrak{r}_\lambda$, leva a $t_\lambda = o$. Designando por C_o o sub-conjunto de C tal que, sendo $\alpha \in C_o$, é $n_1 \mathfrak{r}_\alpha = (o)$, tem-se

$$\mathfrak{S} = \sum_{\lambda \in C_o} \mathfrak{r}_\lambda + \sum_{\lambda \in C - C_o} \mathfrak{r}_\lambda, \quad n_1 \mathfrak{S} = \sum_{\lambda \in C - C_o} n_1 \mathfrak{r}_\lambda = \sum_{\lambda \in C - C_o} \mathfrak{r}_\lambda. \quad (1)$$

A primeira parcela da decomposição de $\mathfrak{S}$ está contida em $\mathfrak{A}$; por outro lado, se $a' \in \mathfrak{A}$, pondo $a' = r_\alpha + r_\beta + \ldots + r_\sigma$, $(o \neq r_\alpha \in \mathfrak{r}_\alpha, \ldots)$, não pode ter-se, por ex., $\alpha \in C - C_o$, visto que, sendo $n_1 a' = n_1 r_\alpha + \ldots + n_1 r_\sigma = o$, é $n_1 r_\alpha = o$, e aquela hipótese daria $r_\alpha = o$. Assim, tem-se

$$\mathfrak{A} = \sum_{\lambda \in C_o} \mathfrak{r}_\lambda, \qquad \mathfrak{S} = \mathfrak{A} + \mathfrak{B},$$

como se afirmou.

Posto isto, o anel $\mathfrak{S}/\mathfrak{B} \simeq \mathfrak{A}$ está nas mesmas condições de $\mathfrak{S}$, no tocante às hipóteses do lema, como é imediato. O mesmo se diz de $\mathfrak{A}$, que, por outro lado, é anel de característica finita. O teorema 36 é aplicável e $\mathfrak{A}$ tem elemento um $=e_1$. Se existir elemento um $=e_2$, em $\mathfrak{B}$, o lema fica provado. É o seguinte o raciocínio de GOLDMAN nesta última parte. Voltemos ao elemento determinado $(a_1, n_1) \in \mathrm{N}_1$ e não esqueçamos que, para cada $b \in \mathfrak{S}$, é $a_1 b = -n_1 b$. Escrevendo $a_1 = \alpha + \beta$, onde $\alpha \in \mathfrak{A}$, $\beta \in \mathfrak{B}$, e tomando $b_o \in \mathfrak{B}$, obtém-se, pois que $\mathfrak{A}\mathfrak{B} = (o)$, $a_1 b_o = -n_1 b_o = (\alpha + \beta) b_o = \beta b_o$. Para cada $c_o \in \mathfrak{B}$ é agora $(n_1 c_o + c_o \beta) b_o = n_1 c_o b_o - n_1 c_o b_o = o$; e, para cada $a \in \mathfrak{S}$, é $(n_1 c_o + c_o \beta) a = o$. Assim, em face do teorema 36, conclui-se $n_1 c_o + c_o \beta = o$, de sorte que $\beta \in \mathfrak{B}$, para qualquer $b_o \in \mathfrak{B}$, dá $\beta b_o = b_o \beta = -n_1 b_o$. Pondo $\beta' = -\beta$, o facto de se ter $\beta' \in \mathfrak{B} = n_1 \mathfrak{S}$ mostra que β'/n_1 existe como elemento de $\mathfrak{S}$. Fazendo a sua decomposição sob a forma $\beta'/n_1 = \alpha_1 + \beta_1$, $(\alpha_1 \in \mathfrak{A}, \beta_1 \in \mathfrak{B})$, vê-se que $\beta'/n_1 \in \mathfrak{B}$. O elemento um de $\mathfrak{B}$ é, pois, $e_2 = -\dfrac{1}{n_1}\beta$.

A suficiência a provar é agora fácil de estabelecer. Decomposto $\mathfrak{S}$ sob a forma indicada em (1), ponhamos $1 = e_\alpha + e_\beta + \ldots + e_\rho$, onde $o \neq e_\alpha \in \mathfrak{r}_\alpha$, etc. Sabemos que é $\mathfrak{S} = e_\alpha \mathfrak{S} + \ldots + e_\rho \mathfrak{S} = \mathfrak{r}_\alpha + \ldots + \mathfrak{r}_\rho$, o que caracteriza $\mathfrak{S}$ como anel completamente redutível. Esta propriedade e a existência de $1 \in \mathfrak{S}$ bastam para garantir que os diferentes radicais se reduzem a (o). O teorema 35 fica provado.

As considerações feitas permitem dar uma nova caracterização dos anéis semi-simples noetherianos. É válido este

TEOREMA 39: — *É condição necessária e suficiente, para que $\mathfrak{S}$ seja um anel semi-simples noetheriano, que todo o ideal direito de $\mathfrak{S}$ seja gerado por um idempotente.* Da teoria dos anéis em causa, desenvolvida no Cap. II, de (I), resulta imediatamente que a condição é necessária. Vamos provar que é também *suficiente*. O próprio anel $\mathfrak{S}$ é gerado por um idempotente e. Escrevendo a decomposição de PEIRCE $\mathfrak{S} = e\mathfrak{S} + \mathfrak{B}$, o ideal direito $\mathfrak{B}$, conjunto dos elementos da forma $b - eb$ é o ideal nulo. Passemos à decomposição esquerda $\mathfrak{S} = \mathfrak{S}e + \mathfrak{A}$, [Cfr. (I), pág. 17]. O ideal esquerdo $\mathfrak{A}$, conjunto dos elementos da forma $a - ae$, é ideal direito, porque $(a - ae)s = as - a.es = as - as = o$, visto ser e uma unidade esquerda. Então, designando por e' o idempotente gerador de $\mathfrak{A}$, será

$e'e' = o = e'$, o que leva a $\mathfrak{A} = (o)$, $\mathfrak{S} = \mathfrak{S}e$. Assim, e é elemento um.

Considerando $\mathfrak{S}$ como módulo — $\mathfrak{S}$, com os operadores à direita, qualquer que seja o ideal direito $\mathfrak{r}$, tem-se sempre, para um certo idempotente f, $\mathfrak{r} = f\mathfrak{S}$, $\mathfrak{S} = f\mathfrak{S} + (1-f)\mathfrak{S} = \mathfrak{r} + \mathfrak{r}'$. O teorema 24 garante-nos que $\mathfrak{S}$ é módulo semi-simples. A existência de elemento $1 \in \mathfrak{S}$ leva agora, como no final do lema 8, ao resultado desejado.

7) Sobre a caracterização abstracta dos sub-anéis dos anéis semi-simples — A doutrina dada em [21], a que vamos passar agora, é relativa a anéis que podem «mergulhar-se» num anel semi-simples no sentido de JACOBSON. Em correlação com a teoria do radical — J, [27, § 4], e com certas proposições do § 5, vamos considerar o ideal bilateral D, contido no radical — J, de $\mathfrak{S}$, e definido como a intersecção dos aniquiladores dos módulos M que admitam $\mathfrak{S}$ como domínio operatório e que sejam irredutíveis — $\mathfrak{E}(\mathrm{M})$. Designaremos por *módulos — $\mathfrak{S}$ quase-simples* os módulos em questão. No § 5, falámos já de exemplos de tais módulos.

A relação de inclusão $\mathrm{D} \subseteq \mathfrak{R}_{**}$ é consequência imediata desta proposição:

TEOREMA 40: — *Um módulo — $\mathfrak{S}$ simples é um módulo quase-simples.* De facto, dado M, nas condições do teorema, se $\mathfrak{a}$ for o ideal bilateral de $\mathfrak{S}$ tal que $\mathrm{M}\mathfrak{a} = (o)$, então M é irredutível — $\mathfrak{S}/\mathfrak{a}$, e, *a fortiori*, irredutível — $\mathfrak{E}(\mathrm{M})$.

Eis aqui o enunciado relativo ao resultado de GOLDMAN:

TEOREMA 41: — *É condição necessária e suficiente, para que $\mathfrak{S}$ possa «mergulhar-se» num anel semi-simples $\mathfrak{T}$, que seja $\mathrm{D} = (o)$.* A condição é *necessária:* Se $\mathfrak{S} \subseteq \mathfrak{T}$ e este último é semi-simples, então $\mathfrak{T}$ é isomorfo duma sôma sub-directa de anéis irredutíveis $\mathfrak{A}_\lambda$. Se M_λ for irredutível — $\mathfrak{A}_\lambda$, $\mathfrak{T}$ é domínio operatório de M_λ, pois que, sendo $\mathfrak{T} \sim \mathfrak{A}_\lambda \simeq \mathfrak{T}/\mathfrak{T}_\lambda$, podemos imaginar $t \in \mathfrak{T}$ a operar como o seu correspondente $a_\lambda \in \mathfrak{A}_\lambda$. O mesmo se diz de $\mathfrak{S}$. Pelo facto de ser $\Pi\,\mathfrak{T}_\lambda = (o)$ e de o aniquilador $\mathfrak{a}_\lambda$, de M_λ, contido em $\mathfrak{S}$, verificar a inclusão $\mathfrak{a}_\lambda \subseteq \mathfrak{T}_\lambda$, será também

$\Pi\, \mathfrak{a}_\lambda = (o)$. Ora os $\mathbf{M}_\lambda$ são irredutíveis — $\mathfrak{C}(\mathbf{M}_\lambda)$, e, assim, $\mathbf{D} = (o)$, pois $\mathbf{D} \subseteq \Pi\, \mathfrak{a}_\lambda$.

A condição é *suficiente:* Tomemos $\mathfrak{S}$ e suponhamos $\mathbf{D} = (o)$. Em seguida, consideremos um conjunto de módulos $\mathbf{M}_\lambda$ que sejam módulos — $\mathfrak{S}$ quase-simples e tais que $\Pi\, \mathfrak{a}_\lambda = (o)$. A soma directa completa dos $\mathfrak{C}(\mathbf{M}_\lambda)$ é um anel semi-simples que contém uma parte isomorfa de $\mathfrak{S}$, como se vê do modo a seguir. Dado $s \in \mathfrak{S}$, seja $s + \mathfrak{a}_\lambda$ o seu correspondente no homomorfismo $\mathfrak{S} \sim \mathfrak{S}/\mathfrak{a}_\lambda$. Como este anel cociente está contido em $\mathfrak{C}(\mathbf{M}_\lambda)$, define-se, assim, uma correspondência $s \to \alpha_\lambda \in \mathfrak{C}(\mathbf{M}_\lambda)$. Se todos os α_λ forem nulos, ter-se-á $s \in \Pi\, \mathfrak{a}_\lambda$, ou seja $s = o$. A correspondência em questão é um isomorfismo, q. e. d.

Sabemos que, qualquer que seja $\mathfrak{S}$, há sempre módulos — $\mathfrak{S}$ simples, e, portanto, há sempre módulos — $\mathfrak{S}$ quase-simples. Se $\mathbf{M}$ é um tal módulo, a sua característica p é a mesma que a do centro de $\mathfrak{C}(\mathbf{M})$. Admitindo $p \neq o$, para cada $a \in \mathfrak{S}$ e cada $x \in \mathbf{M}$, tem-se $x a \,.\, p = o = x \,.\, p a$, de sorte que $p\mathfrak{S}$ está contido no aniquilador de $\mathbf{M}$. Admitindo $p = o$, se designarmos por T o ideal bilateral de $\mathfrak{S}$ composto dos elementos deste com ordem finita, tem-se, para cada $a \in T$ e cada $x \in \mathbf{M}$, (supondo $n a = o$),

$$x \,.\, n a = o = x a \,.\, 1 + \ldots + x a \,.\, 1 = x a \,.\, n 1, \quad (1 \in \mathfrak{C}(\mathbf{M})),$$

$$x a = x a \cdot \frac{n 1}{n 1} = (x \,.\, n a) \cdot \frac{1}{n 1} = o,$$

o que prova estar T contido no aniquilador de $\mathbf{M}$. Deste modo, se considerarmos a totalidade dos módulos — $\mathfrak{S}$ quase-simples, quaisquer que sejam as hipóteses que, em princípio, possamos formular, é sempre $\mathbf{D} \supseteq T \cap \prod_p p\mathfrak{S}$, onde p se estende a todos os números primos.

É agora interessante a seguinte proposição:

TEOREMA 42: — *Dado um anel $\mathfrak{S}$, a intersecção $\mathbf{D}$, de todos os ideais de $\mathfrak{S}$, que são aniquiladores de módulos — $\mathfrak{S}$ quase-simples, é* $\mathbf{D} = \mathrm{T} \cap \prod_{\mathrm{p}} \mathrm{p}\,\mathfrak{S}$, (GOLDMAN). A demonstração ficará feita, se chegarmos a concluir a inclusão $\mathbf{D} \subseteq T \cap \prod_p p\mathfrak{S}$. Começaremos pelo caso em que existe elemento um $= u \in \mathfrak{S}$. Tomemos, então, um módulo — $\mathfrak{S}$ quase-simples $\mathbf{M}$ e façamos a decomposição $\mathbf{M} = \mathbf{M}' + \mathbf{M}''$, onde $\mathbf{M}'$ é aniquilado por $\mathfrak{S}$ e $\mathbf{M}''$ é a parte de $\mathbf{M}$ para a qual u é operador unitário. Se $\mathfrak{a} \subseteq \mathfrak{S}$ for o aniquilador de $\mathbf{M}$, é também o aniquilador de $\mathbf{M}''$. Vê-se, em seguida, que $\mathbf{M}''$ é quase-simples, provando que é módulo sobre o corpo $\mathfrak{z}$, centro de $\mathfrak{C}(\mathbf{M})$. De facto, dado $C \in \mathfrak{z}$, tem-se

$$x u \,.\, C = x(u + \mathfrak{a}) \,.\, C = x C \,.\, (u + \mathfrak{a}) = x C u \in \mathbf{M}'', \quad (x \in \mathbf{M}).$$

Posto isto, concluímos que a determinação de $\mathbf{D}$, no caso em que existe $u \in \mathfrak{S}$, pode fazer-se considerando ùnicamente os módulos — $\mathfrak{S}$ quase-simples, para os quais u é operador unitário.

Independentemente da existência de u, o anel cociente $\mathfrak{S}/p\mathfrak{S}$, como módulo — $\mathfrak{S}$, é quase-simples, incluindo aqui o caso em que $p\mathfrak{S} = \mathfrak{S}$. Mas, quando $u \in \mathfrak{S}$, podemos afirmar ser sempre $p\mathfrak{S}$ o aniquilador de $\mathfrak{S}/p\mathfrak{S}$. Na hipótese $\mathfrak{S} = p\mathfrak{S}$, a afirmação é trivial; não sendo assim, da relação $(\mathfrak{S}/p\mathfrak{S})\, a = o$, concluímos $\mathfrak{S} a \subseteq p\mathfrak{S}$, e, portanto, $a \in p\mathfrak{S}$. Vê-se, deste modo, que se tem $\mathbf{D} \subseteq \Pi\, p\mathfrak{S}$, quando existe u. Examinemos T. Se for $T = \mathfrak{S}$, é evidentemente $\mathbf{D} \subseteq T$, e, portanto, $\mathbf{D} = T \cap \Pi\, p\mathfrak{S}$. Tendo-se $T \neq \mathfrak{S}$, consideremos $\mathbf{N} = \mathfrak{S}/T$. $\mathbf{N}$ é módulo — $\mathfrak{S}$, sem elementos de ordem finita. Se construirmos um módulo — $\mathfrak{S}$ quase-simples, que tenha precisamente T como aniquilador, a conclusão relativa a $\mathbf{D}$ é a mesma que anteriormente. É o que vai ser levado a efeito nos termos seguintes: constrói-se um módulo $\mathbf{M}$ sobre o corpo K dos números racionais e sobre o anel $\mathfrak{S}$, com T como aniquilador. Então, tratando-se dum módulo — K, $\mathbf{M}$ será quase-simples. $\mathbf{M}$ vai aparecer como caso particular de *produto tensorial de grupos abelianos,* no sentido de H. WHITNEY, [Cfr. «Duke Mathematical Journal», vol. 4, 1938, *Tensor product of abelian groups,* em particular págs. 496-498].

Sejam $\mathfrak{L} = \{x, x', \ldots, x_1, x_2, \ldots, x_i, z, \ldots\}$, $\mathbf{N} = \{y, y', \ldots, y_1, y_2, \ldots, y_i, v, \ldots\}$ dois grupos abelianos e consideremos o conjunto $\mathfrak{T}$ de elementos da forma

$(x_1 y_1, \ldots, x_n y_n)$, onde n pode tomar qualquer valor finito. Em $\mathfrak{T}$, ponhamos $(x_1 y_1, \ldots, x_n y_n) + (x_{n+1} y_{n+1}, \ldots, x_p y_p) = (x_1 y_1, \ldots, x_p y_p)$ para definição de soma de dois elementos. Depois, tendo em conta que é $(x_1 y_1) + \ldots + (x_n y_n) = (x_1 y_1, \ldots, x_n y_n)$, escrevamos, para um elemento $a \in \mathfrak{T}$, $a = \Sigma x_i y_i$. Em $\mathfrak{T}$ introduz-se uma relação de equivalência, considerando como equivalentes dois elementos que possam deduzir-se um do outro por operações repetidas dos tipos que vão indicar-se, efectuadas em qualquer dos sentidos:

$$\ldots + x(y + y') + \ldots \sim \ldots + xy + xy' + \ldots$$

$$\ldots + (x + x')y + \ldots \sim \ldots + xy + x'y + \ldots .$$

Claramente que se considera também cada elemento de $\mathfrak{T}$ equivalente a si próprio. Os elementos de $\mathfrak{T}$ ficam divididos em classes formando um conjunto $\mathfrak{Q} = \mathfrak{L} \circ \mathbf{N}$, que se diz produto tensorial de $\mathfrak{L}$ por $\mathbf{N}$. O conjunto $\mathfrak{Q}$ é um grupo abeliano para a definição de soma que vamos dar. Em primeiro lugar, sendo $\alpha \in \mathfrak{Q}$, escreveremos $\alpha = \Sigma x_i . y_i$, se $a = \Sigma x_i y_i$ for um elemento da classe α. Depois, poremos $\alpha + \beta = \Sigma x_i . y_i + \Sigma x'_j . y'_j = \Sigma z_k . v_k$, se $\beta = \Sigma x'_j . y'_j$ e se $\Sigma x_i y_i + \Sigma x'_j y'_j = \Sigma z_k v_k$. Importa que esta definição de soma seja independente dos representantes das classes, o que é imediato. A soma é evidentemente associativa. Quanto ao elemento um de $\mathfrak{Q}$, observemos que, sendo $x . o = (x + x - x) . o = x . o + x . o + (-x) . o = x . (o + o) + (-x) . o = x . o + (-x) . o = (x - x) . o = o . o$, e também $o . y = o . o$, é, quaisquer que sejam x e y, $x . y + o . o = x . y + x . o = x . (y + o) = x . y$, de sorte que o referido elemento é $x . o = o . y = o . o$. Finalmente, o inverso dum elemento $\alpha \in \mathfrak{Q}$ obtém-se tendo em conta as relações $(-x + x) . y = (-x) . y + x . y = o . o$, $-(x . y) = (-x) . y$, ou também $-(x . y) = x . (-y)$. O grupo $\mathfrak{Q}$, acabado de formar, é abeliano, como vamos ver. Tem-se, sucessivamente: $(x + x') . (y + y') = (x + x') . y + (x + x') . y' = x . y + x' . y + x . y' + x' . y = x . (y + y') + x' . (y + y') = x . y + x . y' + x' . y + x' . y'$, e, portanto, $x' . y + x . y' = x . y' + x' . y$, como se deseja.

Posto isto, consideremos o corpo K dos números racionais, o anel $\mathfrak{S}$ com elemento um e o ideal T. Depois, o anel cociente $\mathbf{N} = \mathfrak{S}/T$, e, em seguida, o produto tensorial $K \circ \mathbf{N} = \mathbf{M}$. Para cada $k \in K$, poremos $k(\Sigma k_i . \overline{n}_i) = \Sigma k k_i . \overline{n}_i$, $(k_i \in K, \overline{n}_i \in \mathbf{N})$. Para cada $a \in \mathfrak{S}$, poremos $(\Sigma k_i . \overline{n}_i) a = \Sigma k_i . \overline{n}_i a$, entendendo $\overline{n}_i a$ como $(n_i + T) a = n_i a + T$, onde $n_i \in \mathfrak{S}$ é representante da classe $\overline{n}_i$. Procuremos os elementos $b \in \mathfrak{S}$ que aniquilam $\mathbf{M}$. Em particular, esses elementos aniquilam $1 . \overline{u}$, sendo, portanto, $(1 . \overline{u}) b = 1 . \overline{u} b = 1 . \overline{b} = 1 . \overline{o}$, o que implica $\overline{b} = o$, $b + T = o$, ou seja $b \in T$. Por outro lado, qualquer elemento $t \in T$ aniquila $\mathbf{M}$. A hipótese em que existe $u \in \mathfrak{S}$ fica assim completamente tratada.

Resta estudar o caso em que $\mathfrak{S}$ não tem elemento um. Para isso, «mergulhemos» $\mathfrak{S}$ num anel $\mathfrak{S}^*$ com elemento um, como se indicou no Cap. XIV, § 6. Então, todo o módulo $-\mathfrak{S}^*$ é módulo $-\mathfrak{S}$. Inversamente, se $\mathbf{M}$ é módulo $-\mathfrak{S}$, tomemos o elemento um $= [1, o] \in \mathfrak{S}^*$, e, para cada $x \in \mathbf{M}$, ponhamos $x . [1, o] = x$. $\mathbf{M}$ fica transformado num módulo $-\mathfrak{S}^*$, pois, dado $[n, a] \in \mathfrak{S}^*$, ($n$ inteiro, $a \in \mathfrak{S}$), deverá ter-se $[n, a] = [o, a] + n[1, o]$, $x . [n, a] = x . [o, a] + n x . [1, o] = x a + n x$. Nestas condições, observando ainda que os módulos $-\mathfrak{S}$ quase-simples são igualmente módulos $-\mathfrak{S}^*$ quase-simples, e reciprocamente, segue-se que $\mathbf{D} \subseteqq \mathbf{D}^* = T^* \cap \Pi p \mathfrak{S}^*$, onde as notações são imediatas. Ora, supondo $[n, a] \in T^*$ e $m[n, a] = o$, com $m \neq o$, vê-se que $[mn, ma] = [o, o] = o$, o que implica $n = o$, $[n, a] = [o, a] = a \in T$, $T^* = T$. De modo análogo, supondo $[n, a] \in \Pi p \mathfrak{S}^*$, tem-se $[n, a] = [p_1 n_1, p_1 a_1] = [p_2 n_2, p_2 a_2] = \ldots$, o que implica $n = p_1 n_1 = p_2 n_2 = \ldots$, ou seja $n = o$. Virá $[n, a] = [o, a] = [o, p_1 a_1] = [o, p_2 a_2] = \ldots$, isto é, $[n, a] = [o, a] \in \Pi p \mathfrak{S}$. Mas, sendo $\mathbf{D}^* = T^* \cap \Pi p \mathfrak{S}^* = T \cap \Pi p \mathfrak{S}$, conclui-se $\mathbf{D}^* \subseteqq \mathfrak{S}$, e, consequentemente, $\mathbf{D}^* \subseteqq \mathbf{D}$, ou seja $\mathbf{D}^* = \mathbf{D}$, o que demonstra o teorema.

Uma segunda caracterização abstracta dos sub-anéis dos anéis simples é esta:

TEOREMA 43: — *É condição necessária e suficiente, para que* $\mathbf{S}$ *possa «mergulhar-se» num anel sèmi-simples* $\mathbf{T}$, *que não haja em* $\mathbf{S}$ *elementos diferentes de zero com uma ordem igual ao quadrado dum número primo.* Vamos ver com efeito, que a condição expressa no teorema é equivalente à condição $\mathbf{D} = (o)$. Se a condição do enunciado tem lugar, tomemos $a \in \mathbf{D}$. Supondo $a \neq o$ e $n \neq o, 1$ a ordem de a;

tomemos um número primo $p \neq 1$, factor de n. Das relações $na = o$, $n = pt$, tira-se $pta = o$. De facto de ser $a \in p\mathrm{S}$, conclui-se $a = pb$, para um certo $b \in \mathrm{S}$, e, portanto, conclui-se $p^2 tb = o$. Como tb não pode ter a ordem p^2, será $ptb = ta = o$, o que leva ao absurdo de a ordem de a não ser pt, como se supôs. Será $a = o$, $\mathrm{D} = (o)$. Inversamente, admitindo que é $\mathrm{D} = (o)$, tomemos $a \in \mathrm{S}$ tal que $p^2 a = o$. Se $\pi \neq p$ for outro número primo, da relação $\alpha p + \beta \pi = 1$, na qual α e β são inteiros, tira-se $\alpha p^2 + \beta \pi p = p$, de sorte que $\beta \pi p a = pa$. Visto que π é qualquer número primo, concluímos $pa \in \Pi p\mathrm{S}$. Como é também $a \in T$, ter-se-á $a \in \mathrm{D}$, ou seja $a = o$. O teorema está demonstrado.

8) **Os anéis comutativos e as somas sub-directas** — Seja S um anel comutativo de característica finita q. Se q não é uma potência dum número primo, vamos provar que S é soma directa dum número finito de anéis (ideais) cujas características são precisamente as diferentes potências de números primos que entram na decomposição de q. Escrevamos, com efeito, $q = n_1 n_2$, onde n_1 e n_2 são primos entre si. Existem inteiros α e β tais que $\alpha n_1 + \beta n_2 = 1$. Então, para cada $a \in \mathrm{S}$, tem-se $a = \alpha n_1 a + \beta n_2 a = b + c$, onde $b = \alpha n_1 a$, $c = \beta n_2 a$. O elemento $b \in \mathrm{S}$ é anulado por n_2 e c é anulado por n_1. Como os conjuntos dos elementos de S anulados por n_1 ou por n_2 são ideais $\mathfrak{a}_1$ e $\mathfrak{a}_2$, respectivamente, conclui-se $\mathrm{S} = (\mathfrak{a}_1, \mathfrak{a}_2)$. Esta soma é directa, visto que, supondo $d \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, será $n_1 d = n_2 d = o$, e, admitindo que ρ é o menor inteiro que anula d, n_1 e n_2 possuem ρ como factor comum. Isso exige $\rho = 1$, e, portanto, $d = o$. Assim, $\mathrm{S} = \mathfrak{a}_1 + \mathfrak{a}_2$. A aplicação repetida do raciocínio demonstra a afirmação, visto que todo o ideal de $\mathfrak{a}_i$, $(i = 1, 2)$, é ideal de S.

Podemos dar os dois enunciados a seguir:

TEOREMA 44: — *Um anel comutativo, de característica finita* q, *é soma directa de sub-anéis (ideais) cujas características são as potências de números primos que entram na decomposição de* q.

COROLÁRIO 2: — *Um anel comutativo sub-directamente irredutível tem a característica igual a zero ou igual a uma potência dum número primo.*

OBSERVAÇÃO: — As duas afirmações anteriores são válidas para anéis não comutativos.

No Cap. XVIII, § 3, demonstrámos [teor. 6] um resultado de BIRKHOFF, segundo o qual todo o anel se pode representar como soma sub-directa de anéis sub-directamente irredutíveis. Embora seja evidente que tal representação não é única, vamos dar alguns exemplos interessantes desse facto, tomados no caso comutativo. Se I é o anel dos inteiros, os ideais (2), (5), (11), ..., ou os ideais (3), (7), (13), ..., gerados por números primos alternados, têm uma intersecção nula. Assim, I é isomorfo duma soma sub-directa de corpos $I/(2)$, $I/(5)$, ..., ou de corpos $I/(3)$, $I/(7)$, ..., não havendo entre os primeiros isomorfos dos segundos, pois as respectivas características são diferentes. Se considerarmos, anàlogamente, os ideais (2^3), (5^3), ..., assim como (3^3), (7^3), ..., reconhece-se que I é isomorfo duma soma sub-directa de anéis $I/(2^3)$, ..., ou de anéis $I/(3^3)$, ..., os quais, embora não sejam corpos, são sub-directamente irredutíveis, como se vê pelas ligeiras considerações que vão seguir-se.

Para darmos um exemplo de anel comutativo nas condições do teorema 7, do Cap. XVIII, tomemos ainda I, assim como um número primo p e um inteiro $\alpha \geqq 3$. Pondo $S = I/(p^\alpha)$, reconhece-se imediatamente a existência de divisores de zero. Vê-se que é $D = (p)$ e $J = (p^{\alpha-1})$, [18, pág. 384]. A relação $I/(p) \simeq (I/(p^\alpha))/((p)/(p^\alpha)) = S/D$ mostra que este anel cociente é corpo. A condição 4), do referido teorema 7, é igualmente verificada. Na verdade, ponhamos $d_1 = kp + (p^\alpha)$, onde k não admite o factor $p^{\alpha-2}$. Então, escrevendo $k = qp^\gamma$, $(\gamma < \alpha - 2)$, q não tem o factor p, existindo inteiros x e y tais que $xq + yp = 1$. Desta relação tira-se $xkp^2 p^{\alpha-(\gamma+3)} + yp^\alpha = p^{\alpha-1}$, pelo que, pondo $k' = xp^{\alpha-(\gamma+3)}$, $d_2 = k'p + (p^\alpha)$, vem $d_1 d_2 = p^{\alpha-1} + (p^\alpha)$.

Pois que a respectiva demonstração assenta sobre a hipótese de haver em S elementos que não são divisores de zero, as propriedades 1), 2), 3) e 4), a que o teorema 7 alude, podem não ser realizadas e o anel ser sub-directamente irredutível. Tomemos, por ex., o anel $I[x]$ dos polinómios inteiros, depois o anel $S = I[x]/(8, x^2)$. O sub-

-anel $\mathbf{T} = \{\bar{o}, \overline{2x}, \overline{4x}, \overline{6x}\}$, formado pelas classes associadas de representantes $o, 2x, 4x, 6x$, só tem divisores de zero. É $D = \mathbf{T}$, e o aniquilador de D é o próprio $\mathbf{T}$, gerado por $j = \overline{2x}$. Como, porém, $\mathbf{T}/D$ é composto do único elemento zero, falha a propriedade 3). Entretanto, $\mathbf{T}$ é sub-directamente irredutível, pois que a intersecção de todos os ideais diferentes de zero é o ideal $\{\bar{o}, \overline{4x}\} \neq (o)$. Neste exemplo é aplicável o teorema 8 do Cap. XVIII. De facto, aqui é $a\,\mathbf{T} = (o)$, qualquer que seja $a \in \mathbf{T}$; pondo $p = 2$, $k = 2$, vê-se que $2^2 a = o$; e, sendo $J = \{\bar{o}, \overline{4x}\}$, para cada $b \in J$, é $2b = o$, enquanto que, supondo $c \notin J$, é $2c \neq o$.

Um segundo exemplo, dentro do mesmo teorema 8, é o seguinte. Consideremos um número primo $p > 1$, depois o anel $\mathfrak{A} = \{kp\}$, formado pelos múltiplos de p. Supondo $\alpha > 1$, o anel cociente $\mathfrak{A}/(p^\alpha) = \mathbf{S}$, composto dos elementos $\{(p^\alpha), p + (p^\alpha), \ldots, p^\alpha - p + (p^\alpha)\}$, só contém divisores de zero. Se $\bar{a} = a + (p^\alpha) \in \mathbf{S}$ é tal que $\bar{a}\,\mathbf{S} = (o)$, ter-se-á, em particular, $(a + (p^\alpha))(p + (p^\alpha)) = o$, de sorte que, sendo $ap \in (p^\alpha)$, a contém $p^{\alpha-1}$ em factor. Inversamente, se a contém $p^{\alpha-1}$ em factor, é $\bar{a}\,\mathbf{S} = (o)$. Como $p\bar{a} = o$, vê-se que aqui os únicos elementos para os quais $\bar{a}\,\mathbf{S} = (o)$ são os elementos de $J = (j) = (\overline{p^{\alpha-1}})$. Um elemento qualquer de $\mathbf{S}$ tem a forma $\bar{a} = k_o p^{\alpha-1} + k_1 p^{\alpha-2} + \ldots + k_{\alpha-2}\,p + (p^\alpha)$, onde os k_i verificam as relações $o \leqq k_i \leqq p - 1$. Para que $\bar{a} \notin J$ é necessário e basta que um k_i, com $i \neq o$, seja $\neq o$. Supondo $k_{\alpha-\lambda} = k' \neq o$, $(\lambda > 1)$, o último k da expressão de $\bar{a} \notin J$, determinemos o inteiro ρ por forma que se tenha $\rho k' = \beta p + 1$, onde β é inteiro. É claro que se pode supor sempre $\rho < p$. Então, vê-se que é

$$\bar{a}(\rho p^{\alpha-\lambda} + (p^\alpha)) = (k' \rho p^{\alpha-1} + (p^\alpha)) = p^{\alpha-1} + (p^\alpha),$$

existindo assim $\bar{b} = \rho p^{\alpha-\lambda} + (p)$, por forma que se tenha $\bar{a}\bar{b} = j$, como afirma o teorema 8 invocado.

Embora as considerações do próximo § digam ainda respeito a anéis comutativos, terminaremos este número com a demonstração do

TEOREMA 45: — *Num anel sub-directamente irredutível* $\mathbf{S}$, *nas condições do teorema 7, do Cap. XVIII, a condição de mínimo para os ideais de* $\mathbf{S}$ *arrasta a nilpotência de cada divisor de zero,* [18, pág. 386]. Seja d um divisor de zero, suposto não nilpotente. A condição de mínimo leva a concluir que, na cadeia $(d) \supseteqq (d^2) \supseteqq \ldots$, se tem $(d^\sigma) = (d^{\sigma+1})$, para um certo inteiro σ mínimo. Como será, então, $d^\sigma = s d^{\sigma+1} + m d^{\sigma+1}$, onde $s \in \mathbf{S}$ e m é inteiro, para $a \in \mathbf{S}$, que não seja divisor de zero, vale $d^\sigma[a - d(sa + ma)] = o$, de sorte que, tendo-se, por hipótese, $d^\sigma \neq o$, é $d_1 = a - d(sa + ma)$ um divisor de zero. Resulta daí $j d_1 = j a = o$, o que contradiz a hipótese de a não ser divisor de zero.

N. H. McCoy dá ainda, em [18, pág. 386], um exemplo de anel que mostra ser essencial a condição de mínimo na afirmação do teorema anterior.

9) **Sobre os anéis — p** — Conforme N. H. McCoy e D. Montgomery, diz-se que $\mathfrak{S} \neq (o)$ é um *anel* — p, se for, para cada $x \in \mathfrak{S}$,

$$x^p = x, \qquad px = o, \qquad (p = \text{número primo}).$$

No caso particular em que, para cada $a \in \mathfrak{S}$, se tem $a^2 = a$, o anel — 2 diz-se um *anel de* Boole. Como, de $(a + b)(a + b) = a + b = a^2 + ab + ba + b^2$, se tira $ab + ba = o$, tem-se, em particular, $aa + aa = a^2 + a^2 = a + a = 2a = o$, de sorte que $ab = -ba = ba$. Deste modo, todo o anel de Boole é comutativo e a simples condição $x^2 = x$ implica $2x = o$.

Como num anel de Boole não há nilpotentes não nulos, o lema 2 do Cap. XVIII é aplicável sob a forma seguinte:

TEOREMA 46: — *Um anel de* Boole *sub-directamente irredutível é um corpo isomorfo do corpo* $\mathrm{I}/(2)$, *onde* I *se supõe o anel dos inteiros.*

Tem-se também, [27, teor. 6]:

TEOREMA 47 (Stone): — *É condição necessária e suficiente, para que* $\mathfrak{S}$ *seja um anel de* Boole, *que* $\mathfrak{S}$ *seja isomorfo duma soma sub-directa de corpos* $\mathrm{I}/(2)$.

Passando aos anéis — p, em geral, vamos igualmente provar:

TEOREMA 48: — *Todo o anel* — p *é comutativo,* [22, pág. 525]. Tomemos $a, b \in \mathfrak{S}$ e ponhamos

$$(a+b)^p = a^p + P(a^{p-1}b) + P(a^{p-2}b^2) + \dots + \\ + P(a\,b^{p-1}) + b^p, \tag{2}$$

onde $P(a^{p-k}b^k)$ significa o conjunto das parcelas em que a aparece $p-k$ vezes e b aparece k vezes. Em particular, tem-se $P(a^{p-1}b) = a^{p-1}b + a^{p-2}b\,a + \dots + a\,b\,a^{p-2} + b\,a^{p-1}$. Das igualdades $(a+b)^p = a+b$, $a^p = a$, $b^p = b$, e de (2), concluímos agora $P(a^{p-1}b) + P(a^{p-2}b^2) + \dots + P(a\,b^{p-1}) = o$. Como a e b são quaisquer, podemos substituir b, sucessivamente, por $2b, 3b, \dots, (p-1)b$, na igualdade anterior. Chega-se ao sistema

$$k\,P(a^{p-1}b) + k^2 P(a^{p-2}b^2) + \dots + \\ + k^{p-1} P(a\,b^{p-1}) = o, \tag{3}$$

no qual $k = 1, 2, \dots, p-1$. O determinante Δ, de (3), no qual os PP se consideram incógnitas, é diferente de zero. Representando por $\Delta_1, \Delta_2, \dots, \Delta_{p-1}$ os complementos algébricos dos elementos da 1.ª coluna, multiplicando por Δ_k a equação (3) e fazendo a soma estendida ao índice k, obtém-se a relação

$$\Sigma\, k\, \Delta_k\, P(a^{p-1}b) = o, \qquad \text{ou} \qquad \Delta\, P(a^{p-1}b) = o.$$

Concluímos $P(a^{p-1}b) = o$, assim como $a\,P(a^{p-1}b) - P(a^{p-1}b)\,a = a^p b - b\,a^p = a\,b - b\,a = o$, pois que Δ é um produto de números primos inferiores a p.

Um anel — p sub-directamente irredutível é um corpo de característica p, [lema 2, Cap. XVIII], de sorte que vale o

TEOREMA 49 (MCCOY-MONTGOMERY): — *É condição necessária e suficiente, para que* $\mathfrak{S}$ *seja um anel* — p, *que* $\mathfrak{S}$ *seja isomorfo duma soma sub-directa de corpos* I/(p).

10) **Sobre anéis regulares** — O objectivo deste § é dar um teorema de representação relativo a anéis regulares, aplicando ainda o teorema de BIRKHOFF do Cap. XVIII, § 3. Nos termos que se encontram em [22, págs. 524 e 525], começaremos por três lemas.

LEMA 9: — *Todo o idempotente* e *dum anel* $\mathfrak{S}$, *sem elementos nilpotentes diferentes de zero, pertence ao centro de* $\mathfrak{S}$. De facto, para cada $a \in \mathfrak{S}$, é $(e\,a\,e - e\,a)^2 = (e\,a\,e - a\,e)^2 = o$. Nas condições da hipótese, ter-se-á $e\,a\,e = e\,a = a\,e$, de sorte que e comuta com cada a.

LEMA 10: — *É condição necessária e suficiente, para que um anel regular* $\mathfrak{S}$ *não tenha nilpotentes diferentes de zero, que, para cada* $\mathrm{a} \in \mathfrak{S}$, *exista* $\mathrm{x} \in \mathfrak{S}$ *tal que* $\mathrm{a}^2\mathrm{x} = \mathrm{a}$. Se os nilpotentes não existem, da igualdade $a\,x\,a = a \neq o$ conclui-se que o idempotente $a\,x \neq o$ pertence ao centro de $\mathfrak{S}$. Será $a\,a\,x = a^2 x = a$. Inversamente, dado $a \neq o$, da relação $a^2 x = a$, tira-se $a^3 x^2 = a^2 x$, depois $a^4 x^3 = a^3 x^2 = a$, etc., pelo que a não pode ser nilpotente.

LEMA 11: — *Um anel* $\mathfrak{S}$ *sub-directamente irredutível, e sem nilpotentes diferentes de zero, não pode ter idempotentes diferentes de zero e do elemento um (se este existe).* No caso de $\mathfrak{S}$ ser comutativo, o lema 2, § 3, Cap. XVIII, contém a afirmação, visto que $\mathfrak{S}$ será, então, um corpo. Dum modo geral, porém, tomemos $x \in \mathfrak{S}$ e ponhamos $x = (x - e\,x) + e\,x$, onde e se supõe idempotente $\neq o, 1$. Em face do lema 9, e pertencerá ao centro de $\mathfrak{S}$, de sorte que a decomposição anterior mostra ser $\mathfrak{S} = (\mathfrak{a}_1, \mathfrak{a}_2)$ a soma de dois ideais bilaterais não nulos, respectivamente formados pelos elementos das formas $x - e\,x$ e $e\,x$. Ora, sendo $\mathfrak{a}_1 \cap \mathfrak{a}_2 = (o)$, a soma em questão é directa, contra a hipótese de $\mathfrak{S}$ ser sub-directamente irredutível.

TEOREMA 50: — *Um anel regular* $\mathfrak{S} \neq (\mathrm{o})$, *sub-directamente irredutível, sem nilpotentes diferentes de zero, é um anel de divisão.* Tomemos $o \neq a \in \mathfrak{S}$. Supondo $a\,x\,a = a$, o idempotente $a\,x$, em face do lema 11, só pode ser o elemento um. O mesmo se diz do elemento $x\,a$. E as relações $a\,x = 1$, $x\,a = 1$ mostram que $\mathfrak{S}$ é um anel cujos elementos possuem inverso. O teorema está provado.

Podemos agora formular o teorema de representação de que falámos no começo do §.

TEOREMA 51: — *É condição necessária e suficiente, para que um anel regular $\mathfrak{S}$ seja isomorfo duma soma sub-directa de anéis de divisão, que $\mathfrak{S}$ não tenha nilpotentes diferentes de zero.* É imediato que a condição é necessária. Inversamente, se $\mathfrak{S}$ não tem nilpotentes não nulos, representemo-lo, conforme o teorema de BIRKHOFF, por uma soma sub-directa de anéis sub-directamente irredutíveis, os quais, como imagens homomorfas dum anel regular, são anéis regulares e não têm elementos nilpotentes $\neq o$, como resulta do lema 10. Então, pelo teorema anterior, reduzem-se a anéis de divisão, como se afirmou.

O teorema anterior tem uma aplicação especial no estudo dos anéis $\mathfrak{S}$ que verificam a condição seguinte: para cada $a \in \mathfrak{S}$, existe um inteiro $n(a) > 1$, função de a, tal que $a^{n(a)} = a$. Tem lugar, a tal respeito, esta importante afirmação:

TEOREMA 52 (JACOBSON-KAPLANSKY): — *É comutativo todo o anel $\mathfrak{S}$ para o qual, dado $o \neq a \in \mathfrak{S}$, existe um inteiro $n(a) > 1$, função de a, verificando a igualdade $a^{n(a)} = a$,* [28, pág. 702]. A demonstração reduz-se, conforme A. FORSYTHE e N. H. MCCOY, por via do teorema 51, ao caso dos anéis de divisão. De facto, a propriedade $a^{n(a)} = a$, com $n(a) > 1$, garante que $\mathfrak{S}$ é um anel regular sem nilpotentes diferentes de zero. O teorema 51 estabelece a representação de $\mathfrak{S}$ como soma sub-directa de anéis de divisão. Para estes últimos, a propriedade $a^{n(a)} = a$ é igualmente válida; e, por isso, se eles forem comutativos, o mesmo se pode afirmar quanto a $\mathfrak{S}$.

Seja $\mathfrak{D}$, então, um anel de divisão com a propriedade em causa. Dado $o \neq a \in \mathfrak{D}$, tem-se $a^n = a$, $a^n_\cdot a^{n-1} = a, \ldots$, $a^n_\cdot a^{n-1}_{\cdot\cdot\cdot} a^{n-1} = a$, ou seja $a^{(\sigma-1)(n-1)+n} = a$, qualquer que seja o inteiro $\sigma \geq o$. Supondo $o \neq b \in \mathfrak{D}$, com $b^m = b$, tem-se anàlogamente $b^{\rho(m-1)+1} = b$, de sorte que, escrevendo $\lambda = (n-1)(m-1)+1$, é $a^\lambda = a$, $b^\lambda = b$. Como b é qualquer, façamos $b = r\,a$, onde r é um inteiro positivo arbitrário. Ter-se-á $r^\lambda a^\lambda = r\,a$, ou seja $(r^\lambda - r)\,a = o$. Daqui se conclui que todo o elemento $a \in \mathfrak{D}$ tem uma ordem finita. Se $\omega(a) = \omega$ for essa ordem, o número

$r(r^{\lambda-1} - 1)$ é divisível por ω. Fazendo r sucessivamente igual aos números primos $p > 1$, o facto de $p^{\lambda-1} - 1$ não admitir p como factor leva-nos a concluir que ω se decompõe em números primos, todos diferentes. Ponhamos, por ex., $\omega = p_1 p_2 \ldots p$. Como se tem $p_1 \ldots p_s a = o$, vê-se que $c = p_2 \ldots p_s a$ tem a ordem p_1. Em $\mathfrak{D}$ há, deste modo, elementos não nulos com uma ordem igual a um certo número primo. Esses elementos constituem um ideal bilateral, que será, pois, igual a $\mathfrak{D}$. Assim, vale o

TEOREMA 53: — *Um anel de divisão $\mathfrak{D}$, tal que $o \neq a \in \mathfrak{D}$, (a qualquer), verifica uma equação da forma $a^{n(a)} = a$, $(n(a) > 1)$, tem uma característica igual a um número primo.*

O resto da demonstração do teorema de JACOBSON-KAPLANSKY é diferido para o Capítulo XXI, onde partiremos do resultado anterior. Aqui, observaremos ainda o que vai dizer-se. Os raciocínios feitos sobre $\mathfrak{D}$, aplicados a um anel qualquer com a propriedade $a^{n(a)} = a$, levam à afirmação seguinte:

TEOREMA 54: — *É condição necessária e suficiente, para que num anel $\mathfrak{S}$ valha a propriedade $a^{n(a)} = a$, com $n(a) > 1$, que $\mathfrak{S}$ seja uma soma directa discreta de ideais bilaterais com a mesma propriedade e com uma característica igual a um número primo.*

11) **Sub-módulo — G** — Os raciocínios de B. BROWN e N. H. MCCOY, constantes de [11] e [16], podem aplicar-se à teoria dos módulos e levar a resultados interessantes, que vamos salientar desenvolvidamente.

Neste §, $\mathfrak{M}$ é um módulo — $\mathfrak{S}$ e todos os sub-módulos serão sub-módulos — $\mathfrak{S}$. Os elementos de $\mathfrak{M}$ serão representados por $x, y, z, \ldots$ e os de $\mathfrak{S}$ por $A, B, \ldots, R, S, T, \ldots$, $A', B', \ldots, R', \ldots$.

Dado $x \in \mathfrak{M}$, façamos-lhe corresponder o sub-módulo $(x\mathfrak{S}, t\mathfrak{S})$, no qual $t \in \mathfrak{M}$ é um elemento fixo, independente de x. Em geral, $x \notin (x\mathfrak{S}, t\mathfrak{S})$. Quando for $x \in (x\mathfrak{S}, t\mathfrak{S})$, diz-se que x é *regular*. Um sub-módulo composto de elementos regulares diz-se regular.

Por analogia com a exposição de [25, § 2], serão enunciadas as proposições a seguir, por vezes sem demonstração.

TEOREMA 55: — *Se* $\mathrm{x}-\mathrm{y}$ *é regular e* $\mathrm{y} \in (x\mathfrak{S}, \mathrm{t}\mathfrak{S})$, x *é regular*. Por hipótese, existem $R, T \in \mathfrak{S}$ tais que $x-y=(x-y)R+tT$ e tem-se igualmente $y=xR'+ + tT'$. Então, $x=x(R'+R-R'R)+t(T'+T- - T'R) \in (x\mathfrak{S}, t\mathfrak{S})$, q. e. d.

COROLÁRIO 3: — *A soma de dois sub-módulos regulares é um sub-módulo regular.*

Chamaremos *sub-módulo* — G, de $\mathfrak{M}$, e representá-lo-emos por $\mathfrak{Q}$ [o corolário a seguir mostra que $\mathfrak{Q}$ é módulo — $\mathfrak{S}$], o conjunto dos elementos $x \in \mathfrak{M}$, tais que todo o elemento $y \in \}mx + x\mathfrak{S}\{$ é regular. Bem entendido que m se supõe inteiro, de sorte que $\}mx+x\mathfrak{S}\{$ é o sub-módulo gerado por x.

COROLÁRIO 4: — *$\mathfrak{Q}$ é sub-módulo regular, igual ao conjunto unido de todos os sub-módulos regulares.*

COROLÁRIO 5: — *No homomorfismo* $\mathfrak{M} \sim \mathfrak{M}/\mathfrak{Q} = \overline{\mathfrak{M}}$, *se* $\mathrm{x} \in \mathfrak{M}$ *é regular, o seu correspondente* $\overline{\mathrm{x}} \in \overline{\mathfrak{M}}$ *é regular, e recìprocamente.* A demonstração exige, evidentemente, que, em $\overline{\mathfrak{M}}$, se utilize $\overline{t}$, correspondente de t, para a definição de regularidade.

COROLÁRIO 6: — *No homomorfismo* $\mathfrak{M} \sim \overline{\mathfrak{M}}$, *do corolário anterior, um sub-módulo regular tem um sub-módulo regular como correspondente, e recìprocamente.*

COROLÁRIO 7: — *O módulo diferença* $\mathfrak{M}/\mathfrak{Q}$ *não tem sub-módulo regular.*

É evidente que, supondo $\mathfrak{T} = \}\alpha, \beta, \gamma, \ldots, \rho, \sigma, \ldots, \alpha', \beta', \ldots, \rho', \ldots\{$ um anel anti-isomorfo de $\mathfrak{S}$ e escrevendo $xA = \alpha x$, onde A e α se correspondem no anti-isomorfismo, se define o mesmo sub-módulo — G.

TEOREMA 56: — *Dado um sub-módulo* $\mathfrak{N}$, *de* $\mathfrak{M}$, *o sub-módulo* — G, *de* $\mathfrak{N}$ *é* $\mathfrak{N} \cap \mathfrak{Q}$.

Não obstante poder ter-se $t \notin \mathfrak{N}$, a demonstração não oferece dúvidas. No caso particular de se ter $t = o$, libertar-nos-emos adiante de algumas dificuldades.

COROLÁRIO 8: — *O sub-módulo* — G, *de* $\mathfrak{Q}$, *é igual a* $\mathfrak{Q}$.

As considerações de B. BROWN e de N. H. MCCOY, desenvolvidas em [16] e expostas em [27, § 5], também aqui têm um carácter mais geral, delas se extraindo as proposições anteriores, convenientemente formuladas.

A actual definição de regularidade será a que vem a seguir: imaginemos um processo de construção dum sub-módulo $\mathfrak{N}(x)$, correspondente de $x \in \mathfrak{M}$, tal que, sendo $\mathfrak{M} \sim \overline{\mathfrak{M}}$ um homomorfismo — $\mathfrak{S}$, no qual $x \to \overline{x}$, é simultâneamente $\mathfrak{N}(x) \to \overline{\mathfrak{N}(x)} = \mathfrak{N}(\overline{x})$. Diz-se, então, que $x \in \mathfrak{M}$ é um elemento do *sub-módulo* — F [veremos adiante que se trata dum sub-módulo — $\mathfrak{S}$], de $\mathfrak{M}$, se, para cada $y \in \}mx + x\mathfrak{S}\{$, for $y \in \mathfrak{N}(y)$. A propriedade $x \in \mathfrak{N}(x)$ caracteriza x como *regular;* e um sub-módulo composto de elementos regulares diz-se regular.

Representaremos por $\mathfrak{F}$ o sub-módulo — F. Em $\mathfrak{F}$ estão contidos todos os sub-módulos regulares e todos os elementos de $\mathfrak{F}$ são regulares.

Visto que $\mathfrak{N}(x)$ é um sub-módulo — $\mathfrak{S}$, $\mathfrak{N}(o)$ está nessas condições. Então $o \in \mathfrak{N}(o)$ é sempre realizado, e, por isso, o é regular, e o sub-módulo (o) é regular. Pelo menos, tem-se $(o) \subseteq \mathfrak{F}$. É fácil dar dois casos limites na definição de $\mathfrak{F}$. Suponhamos, primeiramente, $\mathfrak{N}(x) = (o)$, qualquer que seja x. Vê-se que é $\mathfrak{F} = (o)$. Em segundo lugar, tomemos $\mathfrak{N}(x) = \}mx + x\mathfrak{S}\{$. Vê-se que é $\mathfrak{F} = \mathfrak{M}$.

Das proposições que, acerca de $\mathfrak{F}$, vamos enunciar, nenhuma demonstração será dada. Os raciocínios a fazer serão sempre os de B. BROWN e N. H. MCCOY, como já se referiu, [cfr. 27, § 5].

TEOREMA 57: — *Num módulo* $\mathfrak{M} \neq \mathfrak{F}$, *o sub-módulo* $\mathfrak{N}(x)$, *suposto* x *não regular, pode sempre mergulhar-se num sub-módulo* $\mathfrak{L}$ *tal que* $\mathfrak{M}/\mathfrak{L}$ *é sub-directamente irredutível e tem um sub-módulo* — F *igual a zero.*

TEOREMA 58: — *Supondo* $\mathfrak{L}$ *um sub-módulo de* $\mathfrak{M}$ *tal que* $\mathfrak{M}/\mathfrak{L}$ *possui um sub-módulo* — F *nulo, tem-se* $\mathfrak{F} \subseteq \mathfrak{L}$.

Teorema 59: — *Suposto* $\mathfrak{F} \neq \mathfrak{M}$, *é válida a igualdade* $\mathfrak{F} = \Pi \mathfrak{L}$, *onde* $\mathfrak{L}$ *percorre todos os sub-módulos de* $\mathfrak{M}$ *nas condições seguintes:* 1) $\mathfrak{M}/\mathfrak{L}$ *é sub-directamente irredutível;* 2) $\mathfrak{M}/\mathfrak{L}$ *tem um sub-módulo* — F *nulo.*

Corolário 9: — $\mathfrak{F}$ *é um sub-módulo* — $\mathfrak{S}$.

Corolário 10: — $\mathfrak{F}$ *é o conjunto unido de todos os sub-módulos regulares.*

Teorema 60: — *É condição necessária e suficiente, para que se tenha* $\mathfrak{M} = \mathfrak{F}$, *que não exista* $\mathfrak{L} \neq \mathfrak{M}$ *para o qual:* 1) $\mathfrak{M}/\mathfrak{L}$ *seja sub-directamente irredutível;* 2) $\mathfrak{M}/\mathfrak{L}$ *tenha um sub-módulo* — F *nulo.*

Teorema 61: — *O módulo diferença* $\mathfrak{M}/\mathfrak{F}$ *tem um sub-módulo* — F *nulo.*

Teorema 62: — *É condição necessária e suficiente, para que no módulo* $\mathfrak{M}$ *se tenha* $\mathfrak{F} = (\mathrm{o})$, *que* $\mathfrak{M}$ *seja isomorfo duma soma sub-directa de módulos sub-directamente irredutíveis, cada um dos quais com um sub-módulo* — F *nulo.*

A caracterização dos módulos sub-directamente irredutíveis com um sub-módulo — F nulo pode fazer-se, de resto, por via do seguinte

Teorema 63: — *Um módulo* $\mathfrak{M} \neq (\mathrm{o})$ *sub-directamente irredutível tem um sub-módulo* — F *nulo, se e só se o seu sub-módulo mínimo* $\mathrm{J} \neq (\mathrm{o})$ *contiver um elemento* $\mathrm{x} \neq \mathrm{o}$ *tal que* $\mathfrak{N}(\mathrm{x}) = (\mathrm{o})$.

A aplicação do teorema anterior ao caso em que a regularidade de x se define pela propriedade $x \in (x\mathfrak{S}, t\mathfrak{S})$, aludida no começo do §, mostra não existir módulo sub-directamente irredutível com sub-módulo — G nulo, a não ser que se tenha $t\mathfrak{S} = (o)$. No que vai seguir-se, suporemos, efectivamente, $t\mathfrak{S} = (o)$ e designaremos por sub-módulo — G_1 o respectivo sub-módulo — G.

Teorema 64: — *Um módulo* $\mathfrak{M} \neq (o)$ *sub-directamente irredutível tem um sub-módulo* — G_1 *nulo, se e só se o seu sub-módulo mínimo* $\mathrm{J} \neq (\mathrm{o})$ *contiver um elemento* $\mathrm{x}_0 \neq \mathrm{o}$ *tal que* $\mathrm{x}_0 \mathfrak{S} = (\mathrm{o})$. Então, o sub-módulo mínimo tem a forma

$J = \}m x_0\{$ e é $J\mathfrak{S} = (o)$. São válidas certas proposições referidas a propósito do caso em que $\mathfrak{S}$ se supôs comutativo, [§ 4].

Teorema 65: — *Seja* $\mathrm{M} \neq (\mathrm{o})$ *um módulo* — $\mathfrak{S}$ *sub-directamente irredutível, com um sub-módulo* — G_1 *igual a zero; então:* 1) *o sub-módulo* — $\mathfrak{S}$ *mínimo,* $\mathrm{J} \neq (\mathrm{o})$, *é finito e tem uma característica igual a um número primo* p; 2) *admitindo que* $\mathrm{o} \neq \mathrm{x} \in \mathrm{M}$ *é tal que* $\mathrm{x}\mathfrak{S} = (\mathrm{o})$, *existem um número primo fixo (característica de* J) *e um inteiro* ρ, *função de* x, *por forma que* $\mathrm{p}^{\rho}\mathrm{x} = \mathrm{o}$; 3) *é condição necessária e suficiente, para que* $\mathrm{y} \in \mathrm{J}$, *que tenham lugar as duas relações* $\mathrm{y}\mathfrak{S} = (\mathrm{o})$, $\mathrm{p}\mathrm{y} = \mathrm{o}$; 4) *para cada* x *tal que* $\mathrm{o} \neq \mathrm{x} \in \mathrm{M}$, $\mathrm{x}\mathfrak{S} \neq (\mathrm{o})$, *existe* $\mathrm{A} \in \mathfrak{S}$ *verificando a relação* $\mathrm{x}\mathrm{A} = \mathrm{x}_0$.

Teorema 66: — *Dado um módulo* $\mathrm{M} \neq (\mathrm{o})$, *suposto módulo* — $\mathfrak{S}$, *é suficiente, para que* M *seja sub-directamente irredutível e tenha um sub-módulo* — G_1 *igual a zero, que* M *possua as propriedades seguintes:* 1) *exista um sub-módulo da forma* $\mathrm{J} = \}\mathrm{m}\,\mathrm{x}_0\{ \neq (\mathrm{o})$, *tal que* $\mathrm{J}\mathfrak{S} = (\mathrm{o})$; 2) *para cada* $\mathrm{o} \neq \mathrm{x} \in \mathrm{M}$, *tal que* $\mathrm{x}\mathfrak{S} = (\mathrm{o})$, *existam um número primo fixo* p *e um inteiro* ρ *tais que* $\mathrm{p}^{\rho}\mathrm{x} = \mathrm{o}$; 3) *sempre que* $\mathrm{x}\mathfrak{S} = (\mathrm{o})$, $\mathrm{p}\mathrm{x} = \mathrm{o}$, *e apenas nesse caso, seja* $\mathrm{x} \in \mathrm{J}$; 4) *supondo* $\mathrm{x}\mathfrak{S} \neq (\mathrm{o})$, *exista* $\mathrm{A} \in \mathfrak{S}$ *tal que* $\mathrm{x}\mathrm{A} = \mathrm{x}_0$.

Estudado o caso em que o sub-módulo — G_1, que designaremos por $\mathfrak{Q}_1$, é nulo, será necessário passar à hipótese $\mathfrak{Q}_1 \neq (o)$. A condição de suficiência expressa no teorema 22 é também válida, isto é: as quatro propriedades referidas no teorema 22 são suficientes para que M seja sub-directamente irredutível e tenha $\mathfrak{Q}_1 \neq (o)$, ainda mesmo que $\mathfrak{S}$ não seja comutativo. Bem entendido que $\mathfrak{S}/\Delta$ se considera anel de divisão.

Todavia, as condições necessárias expressas nos teoremas 18 e 21 só em parte têm aqui lugar.

12) **Sobre os anéis sub-directamente irredutíveis** — Na ordem de ideias que vimos desenvolvendo, em correlação com [27, § 5], tomemos, num anel $\mathfrak{S}$ qualquer, a seguinte definição de regularidade — F: x é regular — F, se e só se $x \in ((x\mathfrak{S}, \mathfrak{S}x\mathfrak{S}), (\mathfrak{S}x, \mathfrak{S}x\mathfrak{S}))$. Vale, então, o enunciado a seguir, demonstrável ainda pelo processo de N. H.

McCoy, indicado em [27, § 3, teor. 8] e já referido, de novo, nos teoremas 13 a 17, do § 4.

Teorema 67: — *É necessário e basta, para que um anel arbitrário* $\mathfrak{S}$ *seja sub-directamente irredutível e tenha um radical* — F *nulo, que tenham lugar em* $\mathfrak{S}$ *as seguintes propriedades:* 1) *existe um número primo determinado* p *tal que, supondo* $a\mathfrak{S} = \mathfrak{S}a = (o)$, *pode determinar-se um inteiro* k, *função de* $a \in \mathfrak{S}$, *por forma que* $p^k a = o$; 2) *existe um ideal bilateral principal* $J = (x_o) \neq (o)$ *tal que, para cada* $a \in J$, *e apenas para os elementos de* J, *se tem* $a\mathfrak{S} = \mathfrak{S}a = (o)$, $p\,a = o$; 3) *supondo* $a\mathfrak{S} \neq (o)$, $\mathfrak{S}a\mathfrak{S} = (o)$, *existe* $b \in \mathfrak{S}$ *tal que* $a\,b = x_o$; 4) *supondo* $\mathfrak{S}a \neq (o)$, $\mathfrak{S}a\mathfrak{S} = (o)$, *existe* $b \in \mathfrak{S}$ *tal que* $b\,a = x_o$; 5) *supondo* $\mathfrak{S}a\mathfrak{S} \neq (o)$, *existem elementos* $p_i, q_i \in \mathfrak{S}$ *para os quais* $x_o = \Sigma\, p_i\, a\, q_i$.

PUBLICAÇÕES DO CENTRO DE ESTUDOS DE MATEMÁTICA
DA FACULDADE DE CIÊNCIAS DO PORTO
N.º 34

TRÊS LIÇÕES SOBRE A TEORIA GERAL DOS ANÉIS

(APLICAÇÕES E COMPLEMENTOS, I)

POR
A. ALMEIDA COSTA

PUBLICAÇÃO SUBSIDIADA PELO INSTITUTO DE ALTA CULTURA
1 9 5 4