Revisão: Anéis

Def. Um anel é uma tripla $(R,+,\cdot)$ em que R é um conjunto não-vazio e $+,\cdot : R\times R \to R$ são op. binárias satisfazendo:

(i) $(R,+)$ é um grupo abeliano,

(ii) $r\cdot(s+t) = r\cdot s + r\cdot t$, $(r+s)\cdot t = r\cdot t + s\cdot t$, $\forall r,s,t \in R$,

(iii) $r\cdot(s\cdot t) = (r\cdot s)\cdot t$, $\forall r,s,t \in R$.

(iv) Se existe $1 \in R$ t.q. $1\cdot r = r\cdot 1 = r$, $\forall r \in R$, então dizemos que R é um anel com 1 ou anel unitário.

(v) Se R for anel com 1 e para todo $0 \neq d \in R$ existe $d^{-1} \in R$ t.q. $d\cdot d^{-1} = d^{-1}\cdot d = 1$, então R é denominado anel de divisão (division ring, ou skew-field).

Def. Um subconjunto $\emptyset \neq S \subseteq R$ é denominado um subanel se S for anel, com as operações de R.

Def (1) Um ideal (ideal bilateral) $I \subseteq R$ é um subconjunto tal que

(i) $x - y \in I$, $\forall x, y \in I$,

(ii) $rx, xr \in I$, $\forall r \in R$, $\forall x \in I$.

(2) Um ideal à esquerda é um subconj. $I \subseteq R$ tq.

(i) $x - y \in I$, $\forall x, y \in I$,

(ii) $rx \in I$, $\forall x \in I$, $\forall r \in R$.

(3) Da mesma forma, define-se ideal à direita.

Def. Sejam R e S anéis. Um homomorfismo de anéis é um mapa $f: R \to S$ tal que

$$f(r+s) = f(r) + f(s), \quad f(r \cdot s) = f(r) f(s), \quad \forall r, s \in R.$$

Def. Um R-módulo à esquerda é um grupo abeliano $(M, +)$ munido de um mapa $R \times M \to M$ satisfazendo:

(i) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$, $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$, $\forall r_1, r_2 \in R$, $\forall m \in M$,

(ii) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$, $\forall r \in R$, $m_1, m_2 \in M$,

(iii) Se $1 \in R$, então $1 \cdot m = m$, $\forall m \in M$.

Obs. Da mesma forma, define-se módulo à direita.

Def. Um submódulo é um subgrupo $N \subseteq M$ tal que $RN \subseteq N$.

Exemplo. Seja R um anel. Então o produto de R torna R um R-módulo à esquerda. Denota-se tal módulo por ${}_R R$.

Um subconj. $I \subseteq {}_R R$ é submódulo se e só se I é um ideal à esquerda de R.

Def. Sejam M e N R-módulos. Um homomorfismo de R-módulos (ou função R-linear) é um mapa $f: M \to N$ tal que

(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$, $\forall m_1, m_2 \in M$,

(ii) $f(r.m) = r \cdot f(m)$, $\forall r \in R$, $\forall m \in M$.

Obs. M e N são isomorfos se existe um isomorfismo de R-módulos $f: M \to N$, isto é, se existe um hom. de R-módulos $f: M \to N$ que é injetor e sobrejetor. Denota-se $M \cong N$.

Def. Um R-módulo M é dito ser irredutível se $RM \neq 0$ e se seus únicos submódulos são 0 e M.

Obs. Se $f: M \to N$ é um hom. de R-mód., então $\operatorname{Ker} f \subseteq M$ e $f(M) \subseteq N$ são submódulos.

Notação. Denota-se $\operatorname{Hom}_R(M,N) = \{f: M \to N \text{ hom. de } R\text{-mod}\}$, e $\operatorname{End}_R(M) := \operatorname{Hom}_R(M,M)$. O conj. $\operatorname{Hom}_R(M,N)$ é um grupo abeliano com a soma:

$$(f+g)(m) := f(m) + g(m).$$

Além disso, $\operatorname{End}_R(M)$ é um anel, em que o produto é dado por composição de funções.

Teorema (Lema de Schur). Seja M um R-módulo irredutível. Então $\operatorname{End}_R(M)$ é um anel de divisão.

Prova. Seja $0 \neq f \in \operatorname{End}_R(M)$. Então $\operatorname{Ker} f \neq M$, e $\operatorname{Ker} f \subseteq M$ é um submódulo. Como M é irredutível, vale que $\operatorname{Ker} f = 0$. Agora $f(M) \neq 0$ (pois $f \neq 0$) e $f(M) \subseteq M$ é um submódulo. Segue que $f(M) = M$. Daí f é bijetor, e portanto, invertível. $\square$

Def. Um módulo M é completamente redutível se para todo submódulo $N \subseteq M$, existe submódulo $N' \subseteq M$ tal que $M = N \oplus N'$.

Def. Um módulo M é semissimples se $M = \sum M_\alpha$, em que M_α são submódulos irredutíveis.

Def. Um R-módulo M é artiniano se satisfaz uma das seguintes condições equivalentes:

(i) Toda sequência decrescente de submódulos
$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$$
estaciona, isto é, existe m tal que $M_m = M_n$, $\forall n > m$.

(ii) Toda família não vazia de submódulos de M admite elemento minimal.

Proposição. Seja M um R-módulo artiniano. Então M é semissimples $\iff$ M é completamente redutível.

Dem. $(\Leftarrow)$ Evidente.

$(\Rightarrow)$ Seja $N \subseteq M$ um R-submódulo. Considere
$$\mathcal{F} = \left\{ \{N\} \cup \{L_i\}_{i \in J} \,/\, L_i \text{ são submod. irr, e } N + \sum L_i \text{ é soma direta} \right\}$$

$\mathcal{F}$ é não vazia pois contém $\{N\}$. Usando Lema de Zorn, existe um elemento maximal de $\mathcal{F}$, chame de $\{N\} \cup \{L_i\}$. Seja $M' = N + \sum' L_i$. Temos que $M = \sum M_\alpha$, com M_α irredutível. Além disso,

$$M_\alpha \cap M' \subseteq M_\alpha \Rightarrow \begin{array}{l} M_\alpha \cap M' = 0 \\ \text{ou} \\ M_\alpha \cap M' = M_\alpha \Rightarrow M_\alpha \subseteq M'. \end{array}$$

Assumindo que $M' \neq M$, então tem que existir algum $M_\alpha \not\subseteq M'$, ou seja, $M_\alpha \cap M' = 0$. Mas daí $M' + M_\alpha$ é soma direta, contradizendo a maximalidade de $\{N\} \cup \{L_i\}$. Daí $M = N \oplus \sum L_i$. Então $N' := \sum L_i$ é tal que $M = N \oplus N'$, portanto M é completamente red. $\square$

Obs. Não precisa da condição "artiniano" na prop. anterior.

Representações e FG-módulos

Def. Seja $\mathbb{F}$ um corpo. Uma $\mathbb{F}$-álgebra é um anel $(A, +, \cdot)$, que também é um $\mathbb{F}$-esp. vetorial, e de modo que

$$\alpha(a \cdot b) = (\alpha a) \cdot b = a \cdot (\alpha b), \ \forall \alpha \in \mathbb{F}, \forall a, b \in A.$$

Seja G um grupo e considere o espaço $\mathbb{F}G$, que é o $\mathbb{F}$-esp. vetorial com base $\{e_g \mid g \in G\}$. Então $\mathbb{F}G$ admite um produto se definirmos

$$e_g \cdot e_h = e_{gh}.$$

Dado uma representação $\rho: G \to GL(V)$, então V admite estrutura de $\mathbb{F}G$-módulo se definirmos

$$\left(\sum_{g \in G} \alpha_g e_g\right) \cdot v = \sum_{g \in G} \alpha_g \rho_g(v), \quad v \in V.$$

Reciprocamente, dado um $\mathbb{F}G$-módulo V, obtemos uma representação $\rho: G \to GL(V)$ via

$$\rho(g) \cdot v = e_g \cdot v, \quad \forall g \in G, \forall v \in V.$$

Anéis Semissimples

Def. Um anel R é artiniano se ${}_R R$ é um R-mód. artiniano, isto é, se R toda família não vazia de ideais à esquerda de R admite elemento minimal.

Obs. (1) Se R é artiniano e $B \subseteq R$ é um ideal, então B é artiniano.

(2) Se A é uma álg. com 1 de dim $< \infty$, então A é artiniano.

Dados $I, J \subseteq R$, define-se $I \cdot J = \{\sum \pm xy \mid x \in I, y \in J\}$.
Se I e J são ideais (à esquerda, à direita), então também será o produto $I \cdot J$.
Define-se $I^1 = I$, e $I^n = I^{n-1} \cdot I$, $\forall n > 1$.

Def. Seja R um anel.

(i) R é dito ser *simples* se $R^2 \neq 0$ e seus únicos ideais são 0 e R,

(ii) R é dito ser *semiprimo* se para todo ideal $0 \neq I \subseteq R$, vale que $I^2 \neq 0$,

(iii) R é dito ser *primo* se dados ideais $0 \neq I, J \subseteq R$, vale que $I \cdot J \neq 0$,

(iv) R é dito ser *semissimples* se ${}_R R$ é semissimples,

(v) R é dito ser *completamente redutível* se ${}_R R$ é completamente redutível.

Observação. R simples $\Rightarrow$ R primo $\Rightarrow$ R semiprimo.

Def. Seja R um anel. Um elemento $e \in R$ é dito ser *idempotente* se $e^2 = e$.

Obs. Se e é idempotente e $1 \in R$, então $1 - e$ é idempotente.

Lema. Sejam R semiprimo e $0 \neq I \subseteq R$ um ideal minimal à esquerda. Então, existe $e \in I$, com $e^2 = e$, tal que $I = Re$.

Dem. Como R é semiprimo, $I^2 \neq 0$. Daí, existe $a \in I$ tal que $Ia \neq 0$. Mas $I \cdot a \subseteq I$ é um ideal não nulo, e portanto $I \cdot a = I$. Então, um elemento $e \in I$ tal que $ea = a$. Temos que

$$e^2 a = e\,ea = ea \Rightarrow (e^2 - e)a = 0.$$

Seja

$$\mathrm{Ann}_I^{\ell}\, a = \{x \in I \mid xa = 0\}.$$

Então $\mathrm{Ann}_I^{\ell}\, a \subseteq I$ é um ideal à esquerda. Como $e \notin \mathrm{Ann}_I^{\ell}\, a$, segue que $\mathrm{Ann}_I^{\ell}\, a = 0$. Mas $e^2 - e \in \mathrm{Ann}_I^{\ell}\, a$. Ou seja, $e^2 - e = 0$, e portanto, $e^2 = e$. Temos que

$$0 \neq Re \subseteq I \Rightarrow I = Re. \qquad \square$$

Exemplo. Seja $R = M_n(\mathbb{F})$ (ex. R é simples). Temos que

$$\left\{ \begin{pmatrix} 0 & \cdots & 0 & * & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & * & 0 & \cdots & 0 \end{pmatrix} \right\} =: L_j \text{ são ideais minimais à esquerda.}$$

↳ j-ésima coluna

$L_j = M_n(\mathbb{F}) \cdot e_{jj}$. Além disso, $e_{jj}^2 = e_{jj}$. Temos

$$M_n(\mathbb{F}) = M_n(\mathbb{F}) \cdot e_{11} \oplus \cdots \oplus M_n(\mathbb{F}) \cdot e_{nn}.$$

Poderíamos também escrever $L_1 = M_n(\mathbb{F}) e_{11} = M_n(\mathbb{F})(e_{11} + e_{21})$
$(e_{11} + e_{21})^2 = e_{11} + e_{21}$. Poderíamos tb. trocar

$$L_1 \cong L_1' = M_n(\mathbb{F}) \cdot (e_{11} + e_{12}) =$$

$$= \left\{ \begin{pmatrix} a_1 & a_1 & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ a_n & a_n & 0 & \cdots & 0 \end{pmatrix} \right\}.$$