Aplicações p/ álgebra de grupo

O último resultado que vimos e provamos foi:

Teorema da Densidade. Sejam R um anel, M um R-módulo irredutível e $D = \mathrm{End}_R M$. Então, dados $v_1, \dots, v_m \in M$ que são D-linearmente independentes e $w_1, \dots, w_m \in M$, existe $r \in R$ de modo que $r v_i = w_i$, para todo $i = 1, 2, \dots, m$.

Seja R anel simples e artiniano. Então R tem ideal à esquerda minimal da forma Re. Temos que

$$D = \mathrm{End}_R(Re) \cong eRe.$$

Temos que Re é um D-módulo à direita. Daí, a multiplicação pela esquerda por um elemento de $r \in R$ é um homomorfismo de D-módulos $Re \to Re$. Então temos homomorfismo de anéis

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

Como R é simples, segue que $R \to \mathrm{End}_{eRe}(Re)$ é injetiva.

Teorema. Seja R anel simples e artiniano. Então existem $n \in \mathbb{N}$ e anel de divisão D de modo que $R \cong M_n(D)$. O número n e a classe de isomorfismo de $\mathcal{I}$ são unicamente determinados por $\mathcal{R}$.

Demonstração. Vimos que temos homomorfismo injetor de anéis $\mathcal{R} \longrightarrow \mathrm{End}_{eRe}(Re)$. Basta então mostrarmos que $\dim_{eRe} Re < \infty$.

Assuma, por absurdo, que $\dim_{eRe} Re = \infty$. Então existem $v_1, v_2, \ldots \in Re$ sequência infinita de elementos eRe-l.i. Considere

$$\mathrm{Ann}_{\mathcal{R}}\{v_1\} \supsetneq \mathrm{Ann}_{\mathcal{R}}\{v_1, v_2\} \supsetneq \cdots,$$

em que $\mathrm{Ann}_{\mathcal{R}} V = \{r \in \mathcal{R} \mid rv = 0, \forall v \in V\}$. Temos que cada $\mathrm{Ann}_{\mathcal{R}} V$ é ideal à esquerda de $\mathcal{R}$. Do Teorema da Densidade, as inclusões são próprias. Isso contradiz a condição de $\mathcal{R}$ ser artiniano. Daí $\dim_{eRe} Re = n < \infty$. Portanto, novamente do Teorema da Densidade, vale que $\mathcal{R} \to \mathrm{End}_{eRe}(Re)$ é sobrejetivo. Além disso, $\mathrm{End}_{eRe}(Re) \cong M_n(eRe)$, e portanto, $\mathcal{R} \cong M_n(eRe)$.

A unicidade do n segue do Teorema de Jordan-Hölder.

$\square$

Seja G um grupo finito e $\mathbb{F}$ um corpo, com $\operatorname{char}\mathbb{F}=0$ ou $\operatorname{char}\mathbb{F}\nmid |G|$. Então, por Teorema de Maschke, ~~segue~~ segue que $\mathbb{F}G$ é completamente redutível.

Daí, temos que existem anéis de divisão $D_1,\dots,D_s$ de modo que

$$\mathbb{F}G \cong M_{n_1}(D_1)\oplus\cdots\oplus M_{n_s}(D_s).$$

Agora, assuma que $\mathbb{F}$ é algebricamente fechado. Neste caso, se D é $\mathbb{F}$-álgebra de divisão e $\dim_{\mathbb{F}} D<\infty$, então $D=\mathbb{F}$. Então,

$$\mathbb{F}G \cong M_{m_1}(\mathbb{F})\oplus\cdots\oplus M_{m_t}(\mathbb{F}).$$

Def. Um conjunto completo de $\mathbb{F}G$-módulos irredutíveis é um conjunto $\{V_i\}$ tal que $V_i\not\cong V_j$, se $i\neq j$, e para todo $\mathbb{F}G$-módulo irredutível V, existe V_i tal que $V\cong V_i$.

Teorema. Sejam G grupo finito e $\mathbb{F}$ corpo alg. fechado, com $\operatorname{char}\mathbb{F}=0$ ou $\operatorname{char}\mathbb{F}\nmid|G|$. Então o $\mathbb{F}G$-módulo regular contém um conjunto completo de $\mathbb{F}G$-módulos irredutíveis. Se V é um $\mathbb{F}G$-módulo irredutível, então $\mathbb{F}G$ contém $\dim_{\mathbb{F}} V$ cópias de V. Além disso, se $\{V_i\}_{i=1}^{s}$ é um conjunto completo de $\mathbb{F}G$-módulos irredutíveis, então

$$|G| = \sum_{i=1}^{s} (\dim_{\mathbb{F}} V_i)^2 .$$

$\square$

Teorema. Seja G um grupo finito e $\mathbb{F}$ um corpo algebricamente fechado, com $\operatorname{char} \mathbb{F} = 0$ ou $\operatorname{char} \mathbb{F} \nmid |G|$. Então G é abeliano se e só se todo $\mathbb{F}G$-módulo irredutível possui $\mathbb{F}$-dimensão igual a 1. Neste caso, um conjunto completo de $\mathbb{F}G$-módulo irredutíveis possui $|G|$ elementos. $\square$

Se $\mathbb{F}G \cong M_{n_1}(\mathbb{F}) \oplus \cdots \oplus M_{n_s}(\mathbb{F})$, então

$$Z(\mathbb{F}G) \cong Z(M_{n_1}(\mathbb{F})) \oplus \cdots \oplus Z(M_{n_s}(\mathbb{F})) \cong \mathbb{F} \oplus \cdots \oplus \mathbb{F}.$$

Além disso, um conjunto completo de $\mathbb{F}G$-módulos irredutíveis possui s elementos, nessa notação. Além disso,

$$s = \dim_{\mathbb{F}} Z(\mathbb{F}G).$$

Agora, sejam $\mathcal{C}_1, \ldots, \mathcal{C}_r$ as classes de conjugação de G: $g_1, g_2 \in \mathcal{C}_i \iff \exists g \in G$ t.q. $g^{-1} g_2 g = g_1$.

Para cada $\mathcal{C}_i$, defina
$$C_i = \sum_{g \in \mathcal{C}_i} e_g \in \mathbb{F}G.$$

Proposição. Os elementos $C_1, \dots, C_r$ formam uma base para $Z(\mathbb{F}G)$.

Demonstração. Os $C_1, \dots, C_r$ são l.i., pois cada elemento é soma de alguns e_g distintos. Dado $h \in G$, temos
$$e_h C_i e_h^{-1} = \sum_{g \in \mathcal{C}_i} e_{hgh^{-1}} = \sum_{g \in \mathcal{C}_i} e_g = C_i,$$
e portanto, $C_i \in Z(\mathbb{F}G)$.

Agora, seja $z = \sum_{g \in G} \alpha_g e_g \in Z(\mathbb{F}G)$. Daí, dado $h \in G$, vale que
$$\sum_{g \in G} \alpha_g e_g = z = e_h z e_h^{-1} = \sum_{g \in G} \alpha_g e_{hgh^{-1}} = \sum_{g \in G} \alpha_{h^{-1}gh} e_g.$$
Assim, obtemos que $\alpha_g = \alpha_{h^{-1}gh}$, $\forall h \in G$. Isso significa que os α_g são constantes quando $g \in \mathcal{C}_i$, para cada $\mathcal{C}_i$. Daí z é combinação linear dos $C_1, \dots, C_r$. $\square$

Teorema. Sejam G grupo finito e $\mathbb{F}$ corpo alg. fechado, com $\operatorname{char}\mathbb{F} = 0$ ou $\operatorname{char}\mathbb{F} \nmid |G|$. Sejam r a quantidade de classes de conjugação de G, e s a quantidade de elementos de um conjunto completo de $\mathbb{F}G$-módulos irredutíveis. Então $r = s = \dim_{\mathbb{F}} Z(\mathbb{F}G)$. $\square$

Def. Seja A um anel. Um elemento $a \in A$ é dito ser nilpotente se existe $n \in \mathbb{N}$ tal que $a^n = 0$.

O anel A é dito ser nilpotente se existe $n \in \mathbb{N}$ tal que $A^n = 0$.

Teorema. Seja A uma $\overline{\mathbb{F}}$-álgebra de dimensão finita, em que $\overline{\mathbb{F}}$ é um corpo algebricamente fechado. Se A admite uma base de elementos nilpotentes, então A é nilpotente.

Demonstração. Assuma que existe $0 \neq I \subseteq A$ ideal bilateral com $I^2 = 0$. Então $\overline{\mathbb{F}}I$ é ideal bilateral e $(\overline{\mathbb{F}}I)^2 = 0$. Então $A/\overline{\mathbb{F}}I$ possui uma base formada por elementos nilpotentes, pois é imagem homomórfica de A. Temos que $\dim_{\overline{\mathbb{F}}} A/(\overline{\mathbb{F}}I) < \dim_{\overline{\mathbb{F}}} A$, então, por indução, segue que $A/\overline{\mathbb{F}}I$ é nilpotente.

Daí, como $(\overline{\mathbb{F}}I)^2=0$, segue que $\mathcal{A}$ é nilpotente.

Assuma então que $\mathcal{A}$ é uma álgebra semiprima, isto é, $0\neq I\subseteq \mathcal{A}$ ideal bilateral implica $I^2\neq 0$. Além disso, como $\dim_{\overline{\mathbb{F}}}\mathcal{A}<\infty$, segue que $\mathcal{A}$ é artiniano em relação aos ideais mínimais à esquerda que são também $\overline{\mathbb{F}}$-subespaços vetoriais. Repetindo a teoria de anéis semissimples para $\overline{\mathbb{F}}$-álgebras, obtemos que

$$\mathcal{A}\cong M_{n_1}(\overline{\mathbb{F}})\oplus\cdots\oplus M_{n_s}(\overline{\mathbb{F}})\subseteq M_n(\overline{\mathbb{F}}).$$

Um elemento nilpotente possui traço zero. Como $\mathcal{A}$ possui uma base formada por elementos nilpotentes e tr é linear, segue que todo elemento de $\mathcal{A}$ possui traço nulo. Mas $e_{11}\in\mathcal{A}$ e $\operatorname{tr} e_{11}\neq 0$, uma contradição. $\square$

Observação. Não precisa da hipótese de $\mathbb{F}$ ser alg. fechado no teorema anterior. De fato, $\mathcal{A}$ é uma $\mathbb{F}$-álg. admitindo base formada por elementos nilpotentes, então $\overline{\mathcal{A}}=\mathcal{A}\otimes_{\mathbb{F}}\overline{\mathbb{F}}$ também possui $\overline{\mathbb{F}}$-base formada por elementos nilpotentes. Do teorema, $\overline{\mathcal{A}}$ é nilpotente, e portanto $\mathcal{A}$ também é.

Teorema. Seja $\mathbb{F}$ um corpo de característica $p>0$ e G um grupo com $|G|=p^m$. Seja

$$J = \operatorname{Span}\{e_g - e_1 \mid g \in G\} \subseteq \mathbb{F}G.$$

Então J é um ideal bilateral que é nilpotente, e $\mathbb{F}G/J \cong \mathbb{F}$. Se M é um $\mathbb{F}G$-módulo irredutível, então $\dim_{\mathbb{F}} M = 1$ e $e_g m = m$, $\forall g \in G$, $\forall m \in M$.

Demonstração. Dado $h \in G$, temos

$$e_h(e_g - e_1) = (e_{hg} - e_1) - (e_h - e_1) \in J,$$

$$(e_g - e_1)e_h = (e_{gh} - e_1) - (e_h - e_1) \in J,$$

ou seja, J é ideal bilateral de $\mathbb{F}G$.

Note que

$$(e_g - e_1)^{p^m} = e_g^{p^m} - e_1^{p^m} = e_{g^{p^m}} - e_1 = e_1 - e_1 = 0.$$

Daí J admite uma base formada por elementos nilpotentes. Do teorema anterior, segue que J é nilpotente.

Note que $\mathbb{F}G = \mathbb{F}e_1 + J$, e daí $\mathbb{F}G/J \cong \mathbb{F}$.

Seja M um $\mathbb{F}G$-módulo irredutível. Então JM é um $\mathbb{F}G$-submódulo de M, e portanto, $JM = 0$ ou $JM = M$.

Se $JM = M$, então $J^m M = M$, $\forall m \in \mathbb{N}$. Mas J é nilpotente, então existe n tal que $J^n = 0$. Isso implica $M = J^n M = 0$, uma contradição. Daí $JM = 0$.

Tome então $g \in G$ e $m \in M$. Então

$$e_g \cdot m = (e_g - e_1 + e_1) \cdot m = \underbrace{(e_g - e_1)}_{\in J} \cdot m + e_1 \cdot m$$

$$= e_1 \cdot m = m.$$

Então, a única possibilidade é que $M = \mathbb{F}m$, e portanto, $\dim_{\mathbb{F}} M = 1$. $\square$

Assuma agora que G é um grupo abeliano finito, e seja $\hat{G} = \{\text{hom. de grupos } G \longrightarrow \mathbb{F}^\times\}$. Se $\mathbb{F}$ é adequado, então $\hat{G} \cong G$ (por exemplo, se $\mathbb{F}$ é alg. fechado e $\operatorname{char} \mathbb{F} = 0$, ou $\operatorname{char} \mathbb{F} \nmid |G|$).

Exemplo. Seja $C_3 = \langle \alpha \mid \alpha^3 = 1 \rangle$, e $\xi \in \mathbb{C}$ tal que $\xi \neq \xi^3 = 1$. Então $\mathbb{C}C_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$.

O isomorfismo é feito assim

$$\alpha \in \mathbb{C}C_3 \longmapsto (1, \xi, \xi^2) \in \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}.$$

Denote $\hat{C}_3 = \{\chi_1, \chi_2, \chi_3\}$, então

$$g \in \mathbb{C}C_3 \longmapsto (\chi_1(g), \chi_2(g), \chi_3(g)).$$

Exempl. $\mathbb{Q}C_3 \cong \mathbb{Q} \oplus \mathbb{Q}[\xi]$, $\hat{C}_3^{\mathbb{Q}} = \{1\}$,

$$a(e_\alpha - e_1) + b(e_{\alpha^2} - e_\alpha) + c(e_1 + e_\alpha + e_{\alpha^2}) \longmapsto (c, -a-b+a\xi+b\xi^2) \in \mathbb{Q} \times \mathbb{Q}[\xi].$$

$\mathbb{Q}C_3$ possui duas rep. irred., um de dim. 1 e outro de dim. 2.

Exempl. Seja G grupo abeliano finito e $\mathbb{F} = \overline{\mathbb{F}}$, char $\mathbb{F} = 0$ ou char $\mathbb{F} \nmid |G|$. Seja $\hat{G} = \{\chi_1, \dots, \chi_m\}$. Então um iso. $\mathbb{F}G \longrightarrow \underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{|G| = m \text{ cópias}}$ é dado por

$$g \in \mathbb{F}G \longmapsto (\chi_1(g), \dots, \chi_m(g)) \in \mathbb{F}^m.$$

Além disso, se M é um $\mathbb{F}G$-mód. irredutível, então existe $\chi \in \hat{G}$ tal que

$$e_g m = \chi(g) m, \ \forall g \in G, \forall m \in M.$$

Além disso, os ideais minimais são dados por

$$e_\chi = \sum_{g \in G} \chi(g)^{-1} e_g.$$

---||---

Teorema da Densidade. Sejam R um anel, M um R-módulo irredutível e $D = \mathrm{End}_R M$. Então, dados $v_1, \dots, v_m \in M$ que são D-linearmente independentes e $w_1, \dots, w_m \in M$, existe $r \in R$ de modo $rv_i = w_i$, ara todo $i = 1, 2, \dots, m$.

Demonstração. Basta encontrar $r \in R$ tal que

$$rv_1 \neq 0 \quad e \quad rv_2 = \dots = rv_m = 0.$$

Se $v \neq 0$, então $Rv = M$ (*)

De fato: Seja r_i tal que

$$r_i v_i \neq 0 \quad e \quad \text{os demais } r_i v_j = 0, \ \text{se } i \neq j.$$

Daí, $R(r_1 v_1) = M$, então existe $s_1 \in R$ tal que $s_1 r_1 v_1 = w_1$. Então, sejam s_i tq.

$$s_i r_i v_i = w_i.$$

Então, tome $r = s_1 r_1 + \dots + s_m r_m$.

Temos que

$$rv_i = s_1 \underbrace{r_1 v_i}_{=0} + \cdots + s_i r_i v_i + \cdots + s_m \underbrace{r_m v_i}_{=0}$$

$$= w_i, \quad i = 1, \ldots, m.$$

Provemos por indução em m, em que $m=1$ é (*).
Assuma o resultado válido p/ todo conjunto D-l.i. elementos contendo $< m$ elementos.

Seja $I = \mathrm{Ann}_R\{v_2, \ldots, v_{m-1}\}$. Então, sendo

$$W = \{m \in M \mid rm = 0, \forall r \in I\},$$

vale que $W = v_2 D \oplus \cdots \oplus v_{m-1} D$.

Vale que $v_2 D \oplus \cdots \oplus v_{m-1} D \subseteq W$. Seja $v \in M$ tal que $v \notin v_2 D \oplus \cdots \oplus v_{m-1} D$. Daí, da H.I., existe $r \in R$ t.q.

$$rv \neq 0 \text{ e } rv_2 = \cdots = rv_{m-1} = 0.$$

Daí $r \in I$, $rv \neq 0$. Ou seja $v \notin W$.

Se encontrar $r \in I$ tal que $rv_1 \neq 0$ e $rv_n = 0$, então acabou. Vamos assumir então que se $r \in I$ e $rv_n = 0$, então $rv_1 = 0$. Então

$$\begin{aligned} \psi: Iv_n &\longrightarrow Iv_1 \\ xv_n &\longmapsto xv_1 \end{aligned}$$

está bem definido. Mas, vale que

$$0 \neq Iv_n = Iv_1 = M.$$

Daí $\psi \in \mathrm{End}_R M \cong D$, ou seja existe $d \in D$ tal que

$$xv_1 = \psi(xv_n) = xv_n d, \quad \forall x \in I.$$

Então, $x(v_1 - v_n d) = 0$, $\forall x \in I$. Ou seja, $v_1 - v_n d \in W$, uma contradição. $\square$