Universidade Estadual de Campinas
IMECC

Dissertação de Mestrado

Teoria de Kummer sobre Anéis Comutativos

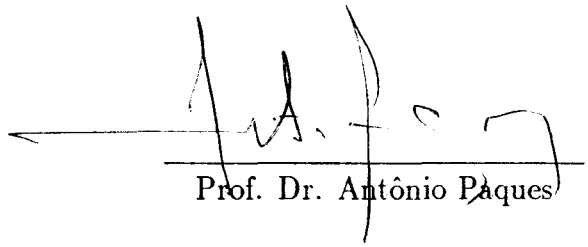
Aluna: Angela Marta Pereira das Dores Savioli
Orientador: Prof. Dr. Antonio Paques

Dezembro de 1993

Teoria de Kummer sobre Anéis Comutativos

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pela Sra. *Angela Marta Pereira das Dores Savioli* e aprovada pela Comissão Julgadora.

Campinas 21, de dezembro de 1993.



Prof. Dr. Antônio Paques

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do Título de Mestre em Matemática.

Dedico este trabalho aos meus pais.

Agradecimentos

- Ao Prof. Antonio Paques, que muito mais do que orientador, é um exemplo de profissional e pessoa.
- Aos professores do IMECC pelo apoio e colaboração.
- Aos professores de Rio Claro: Nativi, João Ivo e Henrique.
- Ao pessoal da secretaria de pós-graduação.
- Ao CNPq, pelo apoio financeiro.
- À Universidade Estadual de Londrina - UEL - pelo grande apoio.
- À *turma* do predinho, pelos momentos de descontração.
- Ao Túlio pela ajuda.
- À *irmã* Ana Claudia e aos mais que amigos: Pedro, Ademir e Jefferson.
- Aos meus pais, Marilanda e José, e à minha irmã Júlia Luciana.
- Ao meu esposo Paulino.
- A todos aqueles que de alguma forma colaboraram para esta dissertação.
- A Deus, por tudo.

Obrigada,

Angela Marta.

Índice

Introdução

A Teoria de Kummer clássica, sobre extensões abelianas de corpos contendo raízes da unidade, foi formalmente estendida e generalizada, para anéis comutativos, por Harrison em 1965, em seu trabalho "Abelian extensions of commutative rings" publicado no Memoirs nº 52 da American Mathematical Society, às páginas 66 a 79. Nesse trabalho, Harrison dá a construção formal do grupo $T(G,R)$ das classes de G-isomorfismo das extensões abelianas finitas de um anel comutativo R, com mesmo grupo de Galois G.

Dados dois elementos quaisquer $[S_1]$ e $[S_2]$ de $T(G,R)$, o elemento produto é a classe representada pela R-subálgebra $(S_1 \otimes_R S_2)^{\delta G}$ de $S_1 \otimes S_2$ invariante pela ação do subgrupo $\delta G = \{(\sigma^{-1},\sigma) \mid \sigma \in G\}$ do grupo abeliano finito $G \times G$. Evidentemente $(S_1 \otimes S_2)^{\delta G}$ é uma nova extensão abeliana de R, construída a partir das extensões S_1 e S_2, com grupo de Galois $G \times G/\delta G$ naturalmente isomorfo a G. O elemento neutro de $T(G,R)$ é representado pela extensão abeliana $E_G(R) = \oplus_{\sigma \in G} R e_\sigma$, onde os e_σ são idempotentes ortogonais dois a dois e de soma 1, e a ação de G sobre $E_G(R)$ é dada pela permutação dos e_σ induzida pela multiplicação de G; isto é, $\sigma(e_\tau) = e_{\sigma\tau}$, $\sigma, \tau \in G$. Para cada $[S]$ de $T(G,R)$, o seu inverso $[S]^{-1}$ é representado pela própria extensão S, com a ação de G dada por $\sigma : s \mapsto \sigma^{-1}(s)$, $s \in S$ $\sigma \in G$.

O principal teorema do trabalho de Harrison é o seguinte:

> "Sejam R um anel comutativo cujos únicos idempotentes são 0 e 1. Então existe uma correspondência biunívoca entre as extensões abelianas finitas de R e os subgrupos finitos de $T(\mathbb{Q}/\mathbb{Z}, R)$, onde $T(\mathbb{Q}/\mathbb{Z}, R)$ denota o limite direto dos grupos $T(\mathbb{Z}/n\mathbb{Z}, R)$, para todo inteiro $n \geq 1$."

Para extensões abelianas finitas, com mesmo grupo de Galois G, o resul-

tado acima pode ser reescrito na seguinte forma:

> "Sejam R um anel comutativo, cujos únicos idempotentes são 0 e 1 e G um grupo abeliano finito. Então existe uma correspondência biunívoca entre as extensões abelianas de R, com grupo de Galois G, e os subgrupos finitos de $T(G,R)$."

Se, por exemplo, a ordem de G é n (respectivamente p primo) e R é um corpo de característica 0 contendo uma raiz n-ésima da unidade (respectivamente de característica p), então $T(G,R) \simeq R^*/R^{*n}$ (respectivamente $R^+/\{r - r^p \mid r \in R\}$).

Este exemplo mostra que a teoria desenvolvida por Harrison não somente estende as teorias (aditiva e multiplicativa) de Kummer, como também as unifica em uma única linguagem.

Na realidade, Harrison pretendia mais. O seu objetivo foi o de tentar desenvolver uma teoria da qual pudesse derivar todas as teorias até então conhecidas no estudo das extensões abelianas de um corpo. Ele obteve sucesso nas teorias clássicas (aditiva e multiplicativa) de Kummer, mas ainda não é claro como utilizar a sua teoria para derivar a teoria de corpos de classes.

De qualquer forma, o trabalho de Harrison apresenta um novo enfoque para o estudo de extensões abelianas finitas de um corpo qualquer ou, mais geralmente, de um anel comutativo.

A idéia da construção de Harrison do grupo $T(G,R)$ não é de todo original; na realidade ela remonta aos trabalhos de Hasse ("Die Multiplikationsgruppe der abelschen Körper mit. fester Galoisgruppe", Abh. Math. Sem. Univ. Hamburg **16** (1949), 29-40), no caso em que $R = K$ é um corpo. Enquanto na teoria de Hasse as extensões galoisianas são corpos, na teoria de Harrison as extensões galoisianas não são necessariamente corpos. Por exemplo, a extensão trivial $E_G(K)$ nunca é corpo, exceto se $G = \{1\}$. Ape-

sar disso, mesmo na teoria de Hasse, esta nova noção de extensão galoisiana (introduzida formalmente pela primeira vez na literatura por Auslander e Goldman, no trabalho "The Brauer group of a commutative ring", Transactions AMS **97** (1960), 367-409) oferece muito mais vantagens que a noção clássica, principalmente devido às propriedades funtoriais do grupo $T(G,R)$. Além disso, é sempre possível traduzir os resultados desta nova teoria na linguagem clássica usando a noção de "KernKörper" de Hasse, a qual significa, em algum sentido, o maior corpo contido em uma extensão galoisiana de K.

Esta dissertação é composta de cinco seções nas quais abordamos, pela ordem, as noções de álgebras separáveis, extensões galoisianas, extensões abelianas e grupo de Harrison, módulos projetivos de posto 1 e grupo de Picard e a Teoria (multiplicativa) de Kummer propriamente dita.

Nenhuma das primeiras quatro seções trata as noções que aborda de forma totalmente abrangente. A nossa preocupação, em todas elas, foi a de procurar apresentar apenas um elenco de resultados minimamente necessário ao desenvolvimento da Teoria de Kummer para anéis, abordada na seção 5.

Em todas as seções, a noção de produto tensorial é fartamente utilizada como ferramenta básica. Essa noção e suas propriedades são assumidas conhecidas sem menção a qualquer referência bibliográfica.

Para conforto do leitor listamos, no final de cada seção, as referências bibliográficas utilizadas na mesma.

1 Álgebras Separáveis

Nosso objetivo nesta seção será o de obtermos uma definição da noção de separabilidade para anéis e apresentarmos alguns exemplos e resultados que nos serão úteis nas seções posteriores.

Consideremos inicialmente k um corpo e $f \in k[\mathrm{x}]$ um polinômio mônico e irredutível. É dito que f é *separável* sobre k se f não tem raízes múltiplas em algum corpo de raízes de f sobre k.

Dada uma extensão qualquer F de k, sejam $p_1, \cdots, p_r \in F[\mathrm{x}]$ os fatores irredutíveis distintos de f em $F[\mathrm{x}]$, isto é, $f = p_1^{n_1} \cdots p_r^{n_r}$ em $F[\mathrm{x}]$, $n_i \geq 1, 1 \leq i \leq r$. Como os ideais $(p_i^{n_i})$, $1 \leq i \leq r$, são comaximais em $F[\mathrm{x}]$, obtemos

$$F \otimes_k \frac{k[\mathrm{x}]}{(f)} \simeq \frac{F[\mathrm{x}]}{(p_1^{n_1})} \oplus \cdots \oplus \frac{F[\mathrm{x}]}{(p_r^{n_r})}$$

Se temos f separável sobre k, então $n_i = 1$ para todo $1 \leq i \leq r$ e, por conseguinte,

$$F \otimes_k \frac{k[\mathrm{x}]}{(f)} \simeq \frac{F[\mathrm{x}]}{(p_1)} \oplus \cdots \oplus \frac{F[\mathrm{x}]}{(p_r)}$$

onde o segundo membro é uma soma direta de corpos. Disto segue que $F \otimes_k k[\mathrm{x}]/(f)$ não possue elementos *nilpotentes* não nulos (isto é, elementos não nulos λ tais que $\lambda^m = 0$ para algum m inteiro $m > 1$).

Reciprocamente, suponhamos que para toda extensão F de k, $F \otimes_k k[\mathrm{x}]/(f)$ não possue elementos nilpotentes não nulos e consideremos N um corpo de raízes de f sobre k. Então

$$f = (\mathrm{x} - x_1)^{r_1} \cdots (\mathrm{x} - x_n)^{r_n} \text{ em } N[\mathrm{x}] ,$$

onde $x_1, \cdots, x_n$ são todas as raízes distintas de f em N, e

$$N \otimes_k \frac{k[\mathrm{x}]}{(f)} \simeq \frac{N[\mathrm{x}]}{(\mathrm{x} - x_1)^{r_1}} \oplus \cdots \oplus \frac{N[\mathrm{x}]}{(\mathrm{x} - x_n)^{r_n}} .$$

Por hipótese $N \otimes_k k[\mathsf{x}]/(f)$ não possue elementos nilpotentes não nulos, logo, o mesmo ocorre com cada quociente $N[\mathsf{x}]/(\mathsf{x} - x_i)^{r_i}$ e assim $r_i = 1$ para todo $1 \leq i \leq n$. Portanto, f é separável sobre k.

A discussão acima pode ser sintetizada na seguinte proposição:

Proposição 1.1: *Sejam k um corpo e $f \in k[\mathsf{x}]$ um polinômio mônico e irredutível. Então f é separável sobre k se, e somente se, para toda extensão F de k, $F \otimes_k k[\mathsf{x}]/(f)$ não possue elementos nilpotentes não nulos.*

Uma extensão algébrica L de k é dita *separável* sobre k se o polinômio mínimo $m(\alpha, k) \in k[\mathsf{x}]$ de cada elemento $\alpha \in L$ é separável sobre k.

Teorema 1.2: *Seja L uma extensão finita de k. As seguintes condições são equivalentes:*

i. L é uma extensão separável de k.

ii. Para toda extensão F de k, $F \otimes_k L$ não possue elementos nilpotentes não nulos.

Demonstração:

(i) $\Longrightarrow$ (ii) Sabemos que toda extensão finita e separável L de k é da forma $k[\mathsf{x}]/(f)$ para algum polinômio mônico, irredutível e separável $f \in k[\mathsf{x}]$. Pela Proposição 1.1 temos o resultado.

(ii) $\Longrightarrow$ (i) Suponhamos, por absurdo, que L não é separável sobre k. Então $\mathrm{car}(k) = p > 0$ e existe L tal que $m(\alpha, k) = \mathsf{x}^{np} + a_{n-1}\,\mathsf{x}^{(n-1)p} + \cdots + a_1\mathsf{x}^p + a_0$. Consideremos

$$F = k(a_0^{\frac{1}{p}}, \cdots, a_{n-1}^{\frac{1}{p}}) \quad \text{e}$$

$$\beta = 1 \otimes \alpha^n + a_{n-1}^{\frac{1}{p}}(1 \otimes \alpha^{n-1}) + \cdots + a_1^{\frac{1}{p}}(1 \otimes \alpha) + a_0^{\frac{1}{p}}(1 \otimes 1) \in F \otimes_k L\ .$$

Como $\partial m(\alpha, k) = np > n$, vê-se imediatamente que $1, \alpha, \cdots, \alpha^n$ são linearmente independentes sobre k e por conseguinte $1 \otimes 1, 1 \otimes \alpha, \cdots, 1 \otimes \alpha^n$ são linearmente independentes sobre F. Como consequência temos $\beta \neq 0$. Contudo $\beta^p = 0$ e assim temos uma contradição . Logo L é separável sobre k. ■

Consideremos L uma extensão finita de k e seja

$$L_{\text{sep}} = \{\alpha \in L; m(\alpha, k) \text{ é separável sobre } k\} .$$

Sabemos da teoria de corpos que L_{sep} é um subcorpo de L que contém k e é, por construção, a maior extensão separável de k contida em L.

Além disso:

(i) L é puramente inseparável sobre L_{sep}, isto é, $L = L_{\text{sep}}$ se $\text{car}(k) = 0$ e $m(\alpha, L_{\text{sep}}) = (\mathsf{x} - \alpha)^{p^e}$ em $L[\mathsf{x}]$, com $e \geq 0$, para todo $\alpha \in L$, se $\text{car}(k) = p > 0$.

(ii) se $\text{car}(k) = p$ então $[L : L_{\text{sep}}] = p^e$, $e \geq 0$, e toda raiz de qualquer polinômio irredutível $f \in k[\mathsf{x}]$ em L tem multiplicidade exatamente igual a $[L : L_{\text{sep}}]$.

(iii) para toda extensão normal N de k contendo L, existem exatamente $n = [L_{\text{sep}} : k]$ k-imersões de L em N (onde $[L_{\text{sep}} : k]$ é o grau de separabilidade de $L \mid k$).

Dada uma extensão finita $L = k(\alpha_1, \cdots, \alpha_l)$ de k sempre existe uma extensão normal finita N de k contendo L; considere, por exemplo, N igual a um corpo de raízes do polinômio $\prod_{i=1}^{l} m(\alpha_i, k) \in k[\mathsf{x}]$. Sejam $\sigma_1, \cdots, \sigma_n$ as k-imersões distintas de L em N e x um elemento qualquer de L. Definimos, então, o *traço* de x como sendo o elemento $\text{tr}(x) \in N$ dado por

$$\text{tr}(x) = [L : L_{\text{sep}}] \sum_{i=1}^{n} \sigma_i(x) .$$

Afirmamos que $\mathrm{tr}(x) \in k$.

De fato, se L é inseparável sobre k então $\mathrm{car}(k) = p, [L : L_{\mathrm{sep}}] = p^e$, $e > 0$ e, portanto

$$\mathrm{tr}(x) = p^e \sum_{i=1}^{n} \sigma_i(x) = 0 \in k .$$

Agora, se considerarmos L separável sobre k, então $[L : L_{\mathrm{sep}}] = 1$ e $\mathrm{tr}(x) = \sum_{i=1}^{n} \sigma_i(x)$. Por outro lado, se $[k(x) : k] = r$ e $[L : k(x)] = s$, existem r k-imersões $\tau_1, \cdots, \tau_r$ de $k(x)$ em N e s $k(x)$-imersões $\varphi_1, \cdots, \varphi_s$ de L em N. Além disso, cada τ_i se estende a um k-automorfismo $\tilde{\tau}_i$ de N. Então as $r.s = n = [L : k]$ aplicações $\tilde{\tau}_i\varphi_j$, $1 \leq i \leq r$, $1 \leq j \leq s$, são as n k-imersões de L em N. Portanto

$$\mathrm{tr}(x) = \sum_{i=1}^{n} \sigma_i(x) = \sum_{i=1}^{r}\sum_{j=1}^{s} \tilde{\tau}_i\varphi_j(x) = s\sum_{i=1}^{r} \tilde{\tau}_i(x) = s\sum_{i=1}^{r} \tau_i(x) .$$

Mas $m(x,k) \in k[\mathsf{x}]$ e

$$m(x,k) = \prod_{i=1}^{r}(\mathsf{x} - \tau_i(x)) = \mathsf{x}^r - (\sum_{i=1}^{r} \tau_i(x))\mathsf{x}^{r-1} + \cdots + (-1)^r \prod_{i=1}^{r} \tau_i(x) ,$$

o que assegura, em particular, que $\sum_{i=1}^{r} \tau_i(x) \in k$. Portanto $\mathrm{tr}(x) \in k$.

Sabemos que quaisquer dois corpos de raízes de um mesmo polinômio $f \in k[\mathsf{x}]$ são sempre isomorfos; logo pode ser facilmente verificado que a definição de $\mathrm{tr}(x)$ acima dada independe do corpo de raízes N considerado. Assim, temos definido uma aplicação $\mathrm{tr} : L \longrightarrow k$, obviamente k-linear, chamada forma *traço* de L sobre k.

Teorema 1.3: *Sejam $k \subseteq L \subseteq N$ e $tr : L \longrightarrow k$ conforme considerados acima. São equivalentes:*

i. L é extensão separável de k.

ii. $tr \neq 0$.

iii. Para toda base $\{x_i; 1 \leq i \leq m\}$ *de* L *sobre* k *existem elementos* $x_i' \in L, 1 \leq i \leq m$, *tais que* $\sum_{i=1}^{m} x_i x_i' = 1$ *e* $ax_i' = \sum_{j=1}^{m} \lambda_{ji} x_j'$, *com* $\lambda_{ji} \in k$, *sempre que* $ax_i = \sum_{j=1}^{m} \lambda_{ij} x_j$, *para todo* $a \in L$.

Demonstração:

(i) $\Longrightarrow$ (ii) L é uma extensão separável de k, logo $[L : L_{\text{sep}}] = 1$. Então se $\sigma_1, \cdots, \sigma_n$ são as $n = [L : k]$ k-imersões de L em N temos $\text{tr} = \sum_{i=1}^{n} \sigma_i$. Assim, como os σ_i, $i = 1, \cdots, n$, são linearmente independentes sobre N segue que $\text{tr} = \sum_{i=1}^{n} \sigma_i \neq 0$.

(ii) $\Longrightarrow$ (i) Suponhamos, por absurdo, que L é inseparável sobre k. Então $\text{car}(k) = p > 0$ e $[L : L_{\text{sep}}] = p^e$, $e \geq 1$, donde segue que $\text{tr} = 0$, o que é uma contradição.

(ii) $\Longrightarrow$ (iii) Consideremos a aplicação k-linear

$$T : L \longrightarrow L^* = \text{Hom}_k(L; k) \ .$$

dada por $T(x)(y) = \text{tr}(xy)$, para quaisquer $x, y \in L$. Como $\text{tr} \neq 0$, temos facilmente que T é um isomorfismo de k-espaços vetoriais. Sejam $\{x_1, \cdots, x_m\} \subset L$ e $\{f_1, \cdots, f_m\} \subset L^*$ bases duais. Logo existe uma base $\{y_1, \cdots, y_m\}$ de L sobre k tal que $T(y_i) = f_i$, pois T é sobrejetora, e por consequência $\text{tr}(x_i y_j) = f_j(x_i) = \delta_{ij}$. Claramente $x = \sum_{i=1}^{m} x_i y_i \neq 0$, pois, caso contrário, teríamos

$$[L : k] = m = \sum_{i=1}^{m} \text{tr}(x_i y_i) = \text{tr}(\sum_{i=1}^{m} x_i y_i) = \text{tr}(0) = 0 \ ,$$

o que é um absurdo. Então, tomando $x_i' = x^{-1} y_i$ obtemos $\sum_{i=1}^{m} x_i x_i' = 1$. Sejam $a \in L, ax_i = \sum_{l=1}^{m} \lambda_{il} x_l$, com $\lambda_{il} \in k$ e $ay_i = \sum_{l=1}^{m} \lambda_{il} y_l$. De

$$\text{tr}((ax_i)y_j) = \text{tr}(x_i(ay_j)) \ ,$$

obtemos

$$\sum_{l=1}^{m} \lambda_{il} \mathrm{tr}(x_l y_j) = \sum_{l=1}^{m} \lambda'_{jl} \mathrm{tr}(x_i y_l)$$

e consequentemente $\lambda_{ij} = \lambda'_{ji}$.

Então se $ax_i = \sum_{j=1}^{m} \lambda_{ij} x_j$ tem-se sempre que

$$ax'_i = x^{-1} a y_i = x^{-1} \sum_{j=1}^{m} \lambda_{ji} y_j = \sum_{j=1}^{m} \lambda_{ji} x^{-1} y_j = \sum_{j=1}^{m} \lambda_{ji} x'_j \ .$$

(iii) $\Longrightarrow$ (i) Sejam $E \supseteq k$ uma extensão de k, $A = L \otimes_k E$ e $N = \mathrm{nil}(A) = \{x \in A; x \text{ é nilpotente } \}$. Claramente A é uma k-álgebra comutativa e $N \subset A$ é um ideal de A. Para mostrarmos que $N = 0$, verifiquemos primeiramente que N é um somando direto de A como A-módulo. Notemos que N e A são E-espaços vetoriais de dimensão finita e portanto existe um E-subespaço M de A tal que $A = N \oplus M$. Seja $\pi : A \to N$ a projeção canônica de A em N, isto é, $\pi(A) = N$, $\pi \mid_N = id$ e $\pi((1 \otimes b)x) = (1 \otimes b)\pi(x)$, para todo $b \in E$. Seja $\pi' : A \to A$ a aplicação k-linear definida por

$$\pi'(x) = \sum_{i=1}^{m} (x'_i \otimes 1)\pi((x_i \otimes 1)x) \ , \text{ para todo } x \in A \ .$$

Claramente $\pi'(A) \subseteq N$. Além disso, para todo $y \in N$ temos

$$\begin{aligned} \pi'(y) &= \sum_{i=1}^{m} (x'_i \otimes 1)\pi((x_i \otimes 1)y) = \sum_{i=1}^{m} (x'_i \otimes 1)(x_i \otimes 1)y \\ &= \sum_{i=1}^{m} (x'_i x_i \otimes 1)y = (1 \otimes 1)y = y \ , \end{aligned}$$

ou seja, $N = \pi'(A)$ e $\pi' \mid_N = id$.

De

$$\begin{aligned} (a \otimes b) \left(\sum_{i=1}^{m} (x'_i \otimes 1)\pi(x_i \otimes 1) \right) &= \sum_{i=1}^{m} (ax'_i \otimes b)\pi(x_i \otimes 1) \\ = \sum_{i=1}^{m} \sum_{j=1}^{m} (\lambda_{ji} x'_j \otimes b)\pi(x_i \otimes 1) &= \sum_{i=1}^{m} \sum_{j=1}^{m} (\lambda_{ji} x'_j \otimes 1)\pi(x_i \otimes b) \end{aligned}$$

$$= \sum_{j=1}^{m}\sum_{i=1}^{m} \lambda_{ij}x_i' \otimes 1\pi(x_j \otimes b) = \sum_{i=1}^{m}(x_i' \otimes 1)\pi(\sum_{j=1}^{m}(\lambda_{ij}x_j \otimes b))$$
$$= \sum_{i=1}^{m}(x_i' \otimes 1)\pi(ax_i \otimes b) = (\sum_{i=1}^{m}(x_i' \otimes 1)\pi(x_i \otimes 1))(a \otimes b) ,$$

para todo $a \otimes b \in A$, concluímos, então, que π' é A-linear. Portanto $A = N \oplus N'$ como A-módulo, onde $N' = \ker \pi' \subseteq A$. Então, se $1 = x + x'$, com $x \in N$ e $x' \in N'$, temos $x = x^2 + xx'$. Como $xx' \in N \cap N' = \{0\}$, segue que $x = x^2$ e por conseguinte $x = 0$ pois x é nilpotente. Consequentemente $1 = x' \in N'$ ou seja, $N' = A$ e $N = \{0\}$. Segue-se agora do Teorema 1.2 que L é separável sobre k. ■

Seja novamente L uma extensão finita de k e denotemos por L^e a k-ágebra (chamada a *álgebra envolvente de* L) $L \otimes_k L$. É claro que L é um L^e-módulo via a ação

$$(a \otimes b)x = a\ x\ b = a\ b\ x\ ,\quad a, b, x \in L$$

e que a aplicação $\mu : L^e \to L$, dada por

$$\mu\left(\sum_{i=1}^{n} a_i \otimes b_i\right) = \sum_{i=1}^{n} a_i b_i$$

é L^e-linear e sobrejetora. Portanto, denotando o núcleo de μ por $J(L)$, temos a seguinte sequência exata de L^e-módulos

$$0 \longrightarrow J(L) \longrightarrow L^e \xrightarrow{\mu} L \longrightarrow 0 .$$

Observemos que $J(L)$ é um ideal de L^e gerado por $\{a \otimes 1 - 1 \otimes a; a \in L\}$, pois para todo $a \in L$, $\mu(a \otimes 1 - 1 \otimes a) = 0$. Reciprocamente, se $\sum_{i=1}^{n} a_i \otimes b_i \in J(L)$ então $\sum_{i=1}^{n} a_i b_i = 0$ e

$$\sum_{i=1}^{n} a_i \otimes b_i = \sum_{i=1}^{n}(1 \otimes b_i)(a_i \otimes 1 - 1 \otimes a_i) .$$

Teorema 1.4: *Sejam $k \subseteq L$, $\mu : L^e \longrightarrow L$ e $J(L)$ como acima. São equivalentes:*

i. L *é extensão separável de* k.

ii. Existe $e \in L^e$ *tal que* $\mu(e) = 1$ *e* $J(L)e = 0$.

iii. A sequência exata

$$0 \longrightarrow J(L) \longrightarrow L^e \xrightarrow{\mu} L \longrightarrow 0$$

cinde.

Demonstração:

(i) $\Longrightarrow$ (ii) Pelo Teorema 1.3 existe uma base $\{x_1, \cdots, x_m\}$ de L sobre k e elementos $x_i' \in L$, $1 \leq i \leq m$, tais que $\sum_{i=1}^m x_i x_i' = 1$ e $ax_i' = \sum_{j=1}^m \lambda_{ji} x_j'$, com $\lambda_{ji} \in k$, sempre que $ax_i = \sum_{j=1}^m \lambda_{ij} x_j$, para todo $a \in L$. Consideremos

$$e = \sum_{i=1}^m x_i \otimes x_i' \in L^e$$

Claramente $\mu(e) = 1$ e, para todo $a \in L$, se $ax_i = \sum_{j=1}^m \lambda_{ij} x_j$, com $\lambda_{ij} \in L$, temos

$$\begin{aligned}(a \otimes 1)e &= \sum_{i=1}^m ax_i \otimes x_i' = \sum_{i=1}^m \sum_{j=1}^m \lambda_{ij} x_j \otimes x_i' \\ &= \sum_{j=1}^m \sum_{i=1}^m \lambda_{ji} x_i \otimes x_j' = \sum_{i=1}^m x_i \otimes \sum_{j=1}^m \lambda_{ji} x_j' \\ &= \sum_{i=1}^m x_i \otimes ax_i' = (1 \otimes a)e \ ,\end{aligned}$$

ou seja, $J(L)e = 0$.

(ii) $\Longrightarrow$ (i) Seja $e = \sum_{i=1}^{n} x_i \otimes x_i' \in L^e$ verificando $\mu(e) = 1$ e $J(L)e = 0$. Podemos supor sem perda de generalidade que $\{x_1, \cdots, x_n\}$ é uma base de L sobre k. Como $\mu(e) = 1$ temos $\sum_{i=1}^{n} x_i x_i' = 1$ e de $J(L)e = 0$ temos, para todo $a \in L$, $(1 \otimes a)e = (a \otimes 1)e$. (*) Então se $ax_i = \sum_{j=1}^{n} \lambda_{ij} x_j$, segue-se que

$$\begin{aligned}\sum_{i=1}^{n} x_i \otimes ax_i' &\overset{*}{=} \sum_{i=1}^{n} ax_i \otimes x_i' \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \lambda_{ij} x_j \otimes x_i' = \sum_{j=1}^{n}\sum_{i=1}^{n} \lambda_{ji} x_i \otimes x_j' \\ &= \sum_{i=1}^{n} x_i \otimes \sum_{j=1}^{n} \lambda_{ji} x_j'\end{aligned}$$

e consequentemente

$$\sum_{i=1}^{n} 1 \otimes (ax_i' - \sum_{j=1}^{n} \lambda_{ji} x_j')(x_i \otimes 1) = 0 \ .$$

Como $\{x_1, \cdots, x_n\}$ é base de L sobre k então $\{x_1 \otimes 1, \cdots, x_n \otimes 1\}$ é base de L^e sobre $L \simeq 1 \otimes L$ e, portanto, $1 \otimes (ax_i' - \sum_{j=1}^{n} \lambda_{ji} x_j') = 0$, para todo $1 \leq i \leq n$. Portanto,

$$ax_i' - \sum_{j=1}^{n} \lambda_{ji} x_j' = \mu\left(1 \otimes (ax_i' - \sum_{j=1}^{n} \lambda_{ji} x_j')\right) = \mu(0) = 0 \ ,$$

para todo $1 \leq i \leq n$.

(ii) $\Longrightarrow$ (iii) Definimos a seguinte aplicação:

$$\begin{aligned}\nu : \quad & L \to L^e \\ & x \mapsto (x \otimes 1)e = (1 \otimes x)e \ ,\end{aligned}$$

para qualquer $x \in L$. É claro que $\nu(x + y) = \nu(x) + \nu(y)$ e $\mu \circ \nu = \mathrm{id}_L$. Mais ainda,

$$\begin{aligned}\nu((a \otimes b)x) &= \nu(abx) = (abx \otimes 1)e = (a \otimes 1)(x \otimes 1)(b \otimes 1)e \\ &= (a \otimes 1)(x \otimes 1)(1 \otimes b)e = (a \otimes 1)(1 \otimes b)(x \otimes 1)e \\ &= (a \otimes b)(x \otimes 1)e = (a \otimes b)\nu(x) \ ,\end{aligned}$$

para todo $a, b, x \in L$. Logo ν é um homomorfismo de L^e-módulos. Portanto a sequência exata

$$0 \longrightarrow J(L) \longrightarrow L^e \xrightarrow{\mu} L \longrightarrow 0$$

cinde.

(iii) $\Longrightarrow$ (ii) Por hipótese a sequência exata

$$0 \longrightarrow J(L) \longrightarrow L^e \xrightarrow{\mu} L \longrightarrow 0$$

cinde. Logo existe um homomorfismo de L^e-módulos $\nu : L \longrightarrow L^e$ tal que $\mu \circ \nu = \mathrm{id}_L$. Seja $e = \nu(1)$. Então

$$\mu(e) = \mu(\nu(1)) = \mu \circ \nu(1) = 1 \quad \text{e}$$

$$\begin{aligned} (a \otimes 1)e &= (a \otimes 1)\nu(1) = \nu((a \otimes 1).1) = \nu(a.1.1) = \nu(a) \\ &= \nu((1 \otimes a).1) = (1 \otimes a)\nu(1) = (1 \otimes a)e \end{aligned}$$

para todo $a \in L$, ou seja,

$$((a \otimes 1) - (1 \otimes a))\, e = 0$$

para todo $a \in L$, o que prova que $J(L)e = 0$. ■

A afirmação (iii) do Teorema 1.4 sugere-nos uma nova caracterização de separabilidade via noção de módulo projetivo. A noção de módulo projetivo será usada fortemente nas seções seguintes. Por essa razão, abrimos um parênteses em nossa exposição para acrescentarmos aqui o teorema-definição seguinte.

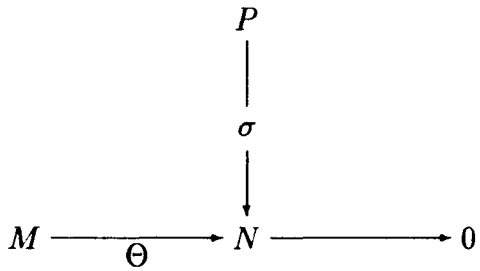
É bem conhecido que todo módulo sobre um anel R é imagem homomórfica de um R-módulo livre. Ou seja, se M é um R-módulo então existe um R-módulo livre L e um epimorfismo de R-módulos $L \to M \to 0$. Os

R-módulos projetivos são exatamente aqueles R-módulos M para os quais a sequência exata $L \to M \to 0$ cinde. Os módulos projetivos são, na realidade, a generalização para anéis da noção de subespaço vetorial.

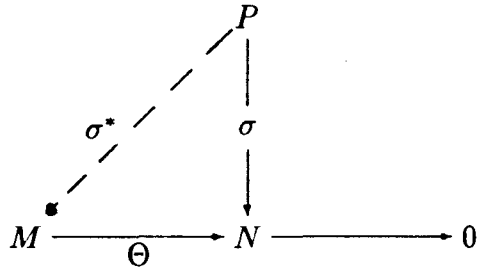
Teorema 1.5: *Seja P um R-módulo. As seguintes afirmações são equivalentes:*

i. *P é um somando direto de um R-módulo livre.*

ii. *Dado o diagrama*



de R-módulos, onde Θ é sobrejetiva, existe um homomorfismo de R-módulos $\sigma^* : P \to M$ tal que o diagrama



é comutativo.

iii. *Se $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ é uma sequência exata de R-módulos então a sequência de R-módulos*

$$0 \to Hom_R(P, L) \xrightarrow{\alpha^*} Hom_R(P, M) \xrightarrow{\beta^*} Hom_R(P, N) \to 0$$

é exata.

iv. *Toda sequência exata de R-módulos $M \xrightarrow{\rho} P \to 0$ cinde.*

v. *Existem conjuntos não vazios* $\{p_\lambda \mid \lambda \in \Lambda\}$ *em* P *e* $\{f_\lambda \mid \lambda \in \Lambda\}$ *em* $P^* = Hom_R(P, R)$ *tais que, para todo* $p \in P$, $f_\lambda(p) = 0$, *exceto para um número finito de índices* $\lambda \in \Lambda$, *e* $p = \sum_{\lambda \in \Lambda} f_\lambda(p) p_\lambda$.

Demonstração:

(i) $\Longrightarrow$ (ii) Seja por hipótese o diagrama dado

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \sigma & & \\ M & \xrightarrow[\Theta]{} & N & \longrightarrow & 0 \end{array}$$

onde a linha $M \xrightarrow{\Theta} N \to 0$ é exata.

Como P é somando direto de um R-módulo livre F ($F = P \oplus Q$, por (i)), seja $\pi : F \to P$ a projeção canônica.

Sejam $B = \{b_\lambda \mid \lambda \in \Lambda\}$ base de F e $\{m_\lambda \mid \lambda \in \Lambda\} \subset M$ tal que

$$\Theta(m_\lambda) = (\sigma \circ \pi)(b_\lambda) \ , \ \forall \lambda \in \Lambda \ .$$

Como B é R-livre a aplicação

$$\begin{aligned} B &\to M \\ b_\lambda &\mapsto m_\lambda \end{aligned}$$

induz um único homomorfismo de R-módulos

$$\begin{aligned} \tau : \quad F &\to M \\ b_\lambda &\mapsto m_\lambda \ . \end{aligned}$$

Basta tomar $\sigma^* = \tau\,|_P$.

(ii) $\Longrightarrow$ (iii) Consideremos a sequência exata $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ e provemos que

$$0 \to \mathrm{Hom}_R(P,L) \xrightarrow{\alpha^*} \mathrm{Hom}_R(P,M) \xrightarrow{\beta^*} \mathrm{Hom}_R(P,N) \to 0$$

é exata.

Se $f \in \ker \alpha^*$ então $\alpha^*(f) = 0$. Como $\alpha^* = \alpha \circ f$, então $\alpha \circ f = 0$, o que implica que $\alpha(f(p)) = 0$, para todo $p \in P$. Então $f(p) = 0$, para todo $p \in P$. Assim $f = 0$.

Seja $h \in \mathrm{Hom}(P,N)$. Logo temos por (ii) que existe um R-homomorfismo $h^* : P \to M$ tal que $\beta^*(h^*) = \beta \circ h^* = h$. Portanto β^* é sobrejetora.

Seja $g \in \mathrm{Im}\ \alpha^*$. Logo existe $f \in \mathrm{Hom}_R(P,L)$ tal que $g = \alpha^*(f) = \alpha \circ f$. Então

$$\begin{aligned} \beta^*(g) &= \beta \circ g = \beta \circ (\alpha \circ f) \\ &= (\beta \circ \alpha) \circ f = 0 \circ f = 0\,, \end{aligned}$$

o que implica que $g \in \ker \beta^*$. Logo $\mathrm{Im}\alpha^* \subseteq \ker \beta^*$.

Agora seja $g \in \ker \beta^*$. Então $\beta \circ g = \beta^*(g) = 0$, o que implica que $\beta(g(p)) = 0$, para todo $p \in P$ e assim $g(p) \in \ker \beta = \mathrm{Im}\ \alpha$, para todo $p \in P$. Então existe $l_p \in L$ tal que $g(p) = \alpha(l_p)$, para todo $p \in P$.

Definimos, para todo $p \in P$

$$\begin{aligned} f: \quad & P \to L \\ & p \mapsto l_p\,. \end{aligned}$$

Claramente f está bem definida e é um homomorfismo de R-módulos.

Logo $f \in \mathrm{Hom}_R(P,L)$ e para todo $p \in P$ temos

$$\alpha^*(f)(p) = (\alpha \circ f)(p) = \alpha(f(p)) = \alpha(l_p) = g(p)\,.$$

Assim, $\alpha^*(f) = g$. Portanto $\ker \beta^* \subseteq \mathrm{Im}\alpha^*$.

(iii) $\Longrightarrow$ (iv) Seja $M \xrightarrow{\rho} P \to 0$ exata.

Então

$$0 \to \ker \rho \xhookrightarrow{i} M \xrightarrow{\rho} P \to 0$$

é exata. Indiquemos $\ker \rho$ por K. Assim, por (iii), a sequência

$$0 \to \mathrm{Hom}_R(P, K) \xrightarrow{i^*} \mathrm{Hom}_R(P, M) \xrightarrow{\rho^*} \mathrm{Hom}_R(P, P) \to 0$$

é exata.

Seja $\mathrm{id}_P \in \mathrm{Hom}_R(P, P)$. Como a sequência é exata temos que ρ^* é sobrejetora. Logo existe $\delta \in \mathrm{Hom}_R(P, M)$ tal que

$$\rho^*(\delta) = \mathrm{id}_P$$

o que implica que

$$\rho \circ \delta = \mathrm{id}_P \ .$$

Portanto a sequência $M \xrightarrow{\rho} P \to 0$ cinde e consequentemente $M \simeq P \oplus \ker \rho$.

(iv) $\Longrightarrow$ (v) Seja $\{p_\lambda \mid \lambda \in \Lambda\}$ um conjunto de geradores de P. Seja também F o R-módulo livre com base $B = \{b_\lambda \mid \lambda \in \Lambda\}$. Como B é um conjunto R-livre a aplicação

$$B \to P$$

$$b_\lambda \mapsto p_\lambda$$

induz um homomorfismo de R-módulos

$$\rho: \quad F \to P$$

$$b_\lambda \mapsto p_\lambda$$

para todo $\lambda \in \Lambda$. Claramente ρ é sobrejetora. Então temos

$$F \xrightarrow{\rho} P \to 0 \quad \text{exata} \ .$$

Por (iv) existe um homomorfismo de R-módulos $\delta : P \to F$ tal que $\rho o \delta = \mathrm{id}_P$. Como $F = \oplus_{\lambda \in \Lambda} Rb_\lambda$, seja $\pi_\lambda : F \to R$ a projeção canônica dada por

$$\pi_\lambda \left(\sum_{\text{finita}} r_\lambda b_\lambda \right) = r_\lambda \quad \text{para todo } \lambda \in \Lambda .$$

Seja $f_\lambda = \pi_\lambda \circ \delta$ para todo $\lambda \in \Lambda$. Claramente $f_\lambda \in P^*$ para todo $\lambda \in \Lambda$ e para todo $p \in P$.

$$f_\lambda(p) = \pi_\lambda \circ \delta(p) = \pi_\lambda (\delta(p)) = \pi_\lambda \left(\sum_{\text{finita}} r_\lambda b_\lambda \right) = r_\lambda .$$

Disto segue que $f_\lambda(p) = 0$ exceto num número finito de $\lambda \in \Lambda$. Para qualquer $p \in P$

$$\begin{aligned} p &= \mathrm{id}_P(p) = \rho \circ \delta(p) = \rho \left(\sum_{\text{finita}} r_\lambda b_\lambda \right) \\ &= \sum_{\text{finita}} r_\lambda \rho(b_\lambda) = \sum_{\text{finita}} r_\lambda p_\lambda = \sum_{\lambda \in \Lambda} f_\lambda(p) p_\lambda . \end{aligned}$$

(v) $\Longrightarrow$ (i) Seja F o R-módulo livre com base $\{b_\lambda \mid \lambda \in \Lambda\}$ e

$$\begin{aligned} \rho : \quad & F \to P \\ & b_\lambda \mapsto p_\lambda \end{aligned}$$

conforme obtido no passo anterior da demonstração. Claramente ρ é sobrejetora e

$$F \xrightarrow{\rho} P \to 0 \quad \text{é exata.}$$

Seja $\delta : P \to F$ dado por

$$\delta(p) = \delta \left(\sum_{\lambda \in \Lambda} f_\lambda(p) p_\lambda \right) = \sum_{\lambda \in \Lambda} f_\lambda(p) b_\lambda .$$

A aplicação δ está claramente bem definida e é um homomorfismo de R-módulos. Além disso, $\rho \circ \delta = \mathrm{id}_P$. Logo

$$F \xrightarrow{\rho} P \to 0$$

cinde e $F \simeq P \oplus \ker \rho$.

Assim P é somando direto de um R-módulo livre. ■

Dos Teoremas 1.4 e 1.5 decorre agora o seguinte teorema.

Teorema 1.6: *Seja L uma extensão finita de k. Então as afirmações seguintes são equivalentes:*

i. L é extensão separável de k.

ii. L é um L^e-módulo projetivo.

Demonstração: Imediata. ■

Consideremos agora o elemento $e \in L^e$ descrito no Teorema 1.4. Logo e verifica $\mu(e) = 1$ e $J(L)e = 0$. Como $e - 1 \in J(L)$ temos $(e-1)e = 0$ ou seja $e^2 = e$. Portanto este elemento e é idempotente e é chamado idempotente de separabilidade de L. Além disso, como L^e é uma álgebra comutativa, este idempotente de separabilidade e é único. De fato, se $e' \in L^e$ é outro elemento de L^e verificando as mesmas propriedades $\mu(e') = 1$ e $J(L)e' = 0$ então $e - e' \in J(L)$ (pois $\mu(e - e') = 0$) e de $(e - e')e = 0$ e $(e - e')e' = 0$ obtemos

$$e = e^2 = e'e = ee' = e'^2 = e' .$$

Se L é uma extensão finita e separável de k então L pode ser identificada ao quociente $k[x] = k[\mathsf{x}]/(f)$, onde $x = \mathsf{x} + (f)$ e $f = m(x, k)$ é um polinômio separável sobre k. Se f' denota a derivada formal de f então $f'(x) \neq 0$. Sejam

$$f = a_0\mathsf{x}^n + a_1\mathsf{x}^{n-1} + \cdots + a_n \in k[\mathsf{x}] \ , \ \text{com} \ \ a_0 = 1 \ \ \text{e}$$

$$f_l = a_0\mathsf{x}^l + a_1\mathsf{x}^{l-1} + \cdots + a_l \ ,$$

para todo $0 \leq l \leq n$. Então o elemento

$$e = (\frac{1}{f'(x)} \otimes 1)(f_{n-1}(x) \otimes 1 + f_{n-2}(x) \otimes x + \cdots + f_0 \otimes x^{n-1}) \in L^e$$

é um idempotente de separabilidade de L sobre k. Para a verificação desta afirmação ver o exemplo 1.8.e abaixo.

O nosso intuito nos resultados acima apresentados foi o de buscar, utilizando quase que essencialmente a teoria dos corpos e fazendo um mínimo de apelo à teoria de módulos e álgebras, uma definição da noção de separabilidade que melhor se adequasse a uma generalização no contexto de anéis.

Evidentemente, nos Teoremas 1.2, 1.3 e 1.4, nos inspiramos em fatos que são próprios da teoria de álgebras. Assim como na teoria de corpos a noção de separabilidade se baseia na simplicidade de raízes de polinômios, na teoria de álgebras, esta mesma noção se baseia na semisimplicidade de álgebras. O Teorema 1.2 assegura que ambos os enfoques são equivalentes quando colocados no contexto de corpos. Uma k-álgebra A de dimensão finita é dita *semisimples* se A não possue ideais nilpotentes não nulos, o que, no caso de A ser comutativa, equivale a dizer que A não possue elementos nilpotentes não nulos.

Uma k-álgebra A de dimensão finita é dita *separável* se, para todo corpo $E \supset k$, a E-álgebra $E \otimes_k A$ é semisimples. Um teorema análogo ao Teorema 1.4 é também válido para k-álgebras de dimensão finita em geral. Para uma abordagem completa sobre a noção de semisimplicidade e separabilidade no contexto mais geral de álgebras de dimensão finita sobre um corpo k veja [1]. Da mesma forma, as noções e resultados da teoria de corpos não detalhados aqui podem ser vistos em [4].

No que se seguirá R denotará sempre um anel comutativo com unidade. Sejam S uma R-álgebra não necessariamente comutativa e S^0 sua álgebra oposta, isto é, $S^0 = S$ como R-módulos (à esquerda) e $x^0 y^0 = (yx)^0$, para

todo $x, y \in S$. Seja $S^e = S \otimes_R S^0$ a álgebra envolvente de S.

Evidentemente, S é um S^e-módulo (à esquerda) via ação de

$$(a \otimes b^0)x = a\ x\ b\ ,$$

para todo $a, b, x \in S$. Consideremos a aplicação $\mu : S^e \to S$ dada por

$$\mu\left(\sum_{i=1}^{n} a_i \otimes b_i^0\right) = \sum_{i=1}^{n} a_i b_i\ .$$

Esta aplicação é S^e-linear e sobrejetiva. Se denotarmos por $J(S)$ o núcleo de μ, temos a seguinte sequência exata de S^e-módulos

$$0 \longrightarrow J(S) \longrightarrow S^e \xrightarrow{\mu} S \longrightarrow 0\ .$$

Dizemos que S é uma *R-álgebra separável* se S é um S^e-módulo projetivo.

Teorema 1.7: *Sejam R, S, S^e, $\mu : S^e \longrightarrow S$ e $J(S)$ como considerados acima. São equivalentes:*

i. S é $R-$álgebra separável.

ii. A sequência exata de S^e-módulos

$$0 \longrightarrow J(S) \longrightarrow S^e \xrightarrow{\mu} S \longrightarrow 0$$

cinde.

iii. Existe $e \in S^e$ tal que $\mu(e) = 1$ e $J(S)e = 0$.

A demonstração deste teorema segue argumentos análogos aos utilizados na demonstração do Teorema 1.4.

O elemento $e \in S^e$ dado neste Teorema 1.7 é um idempotente, chamado idempotente de separabilidade de S, e não é necessariamente único, como veremos no exemplo 1.8.g considerado abaixo:

Exemplos 1.8:

a) R é uma R-álgebra separável.

$$\mu : R^e \longrightarrow R$$

é um isomorfismo.

b) Seja T um sistema multiplicativo do anel R, isto é, $0 \notin T$, $1 \in T$ e $x.y \in T$ sempre que $x, y \in T$. Consideremos o anel de frações

$$S = T^{-1}R = \left\{ \frac{a}{t} \mid a \in R, t \in T \right\} .$$

É fácil ver que a aplicação

$$\begin{aligned} \mu : \quad & S \otimes_R S^0 \longrightarrow S \\ & \sum_{i=1}^{n} a_i \otimes b_i \mapsto \sum_{i=1}^{n} a_i b_i \end{aligned}$$

é, neste caso, um isomorfismo de S^e-módulos. Portanto $S = T^{-1}R$ é uma R-álgebra separável.

c) Seja $R = \mathbf{Z}$ e $S = \mathbf{Z}/p\mathbf{Z}$ para algum primo p. Claramente

$$\begin{aligned} \mu : \quad & \frac{\mathbf{Z}}{p\mathbf{Z}} \otimes_{\mathbf{Z}} \frac{\mathbf{Z}}{p\mathbf{Z}} \longrightarrow \frac{\mathbf{Z}}{p\mathbf{Z}} \\ & \sum_i \overline{a}_i \otimes \overline{b}_i \longmapsto \sum_i \overline{a}_i \overline{b}_i \end{aligned}$$

é um isomorfismo e portanto $S = \mathbf{Z}/p\mathbf{Z}$ é uma $\mathbf{Z}$-álgebra separável.

d) Seja $R = \mathbf{Z}[\sqrt{-3}]$ e $S = \mathbf{Z}[w]$, com $w^2 + w + 1 = 0$ $(w = \frac{-1+\sqrt{-3}}{2})$. $R \subset S$ e portanto S é uma R-álgebra. Além disso,

$$e = 1 \otimes 1 + 1 \otimes w - w \otimes 1 \in S \otimes_R S$$

é um idempotente de separabilidade de S sobre R. De fato,

$$\mu(e) = 1 + \omega - \omega = 1$$

$$
\begin{aligned}
(1\otimes\omega-\omega\otimes 1)e &= 1\otimes\omega+1\otimes\omega^2-\omega\otimes\omega-\omega\otimes 1-\omega\otimes\omega+\omega^2\otimes 1\\
&= 1\otimes(\omega+\omega^2)-2\omega\otimes\omega-(-\omega+\omega^2)\otimes 1\\
&= 1\otimes -1-2\omega\otimes\omega+(-1\otimes 1-2\omega\otimes 1)\\
&= -2\otimes 1-1\otimes 2\omega^2-2\omega\otimes 1\\
&= -2\otimes 1+(1\otimes 2\omega+2\otimes 1)-2\omega\otimes 1\\
&= 2\omega\otimes 1-2\omega\otimes 1 \;=\; 0
\end{aligned}
$$

Logo $Je=0$.

e) Seja $f\in R[\mathsf{x}]$ um polinômio mônico e $S=R[\mathsf{x}]/(f)=R[x]$, onde $x=\mathsf{x}+(f)$. Denotando por f' a derivada formal de f, se f' é invertível em S então S é uma R-álgebra separável. De fato, sejam

$$f(\mathsf{x})=a_0\mathsf{x}^n+a_1\mathsf{x}^{n-1}+\cdots+a_n\in R[\mathsf{x}]\ .$$

com $a_0=1$ e

$$f_l(\mathsf{x})=a_0\mathsf{x}^l+a_1\mathsf{x}^{l-1}+\cdots+a_l\ ,$$

para todo $0\le l\le n$. O elemento

$$e=\frac{f_{n-1}(x)}{f'(x)}\otimes 1+\frac{f_{n-2}(x)}{f'(x)}\otimes x+\cdots+\frac{f_0(x)}{f'(x)}\otimes x^{n-1}\ \in S\otimes_R S$$

é um idempotente de separabilidade de S sobre R.

Notemos que

$$\mu(e)=\frac{1}{f'(x)}\Big(f_{n-1}(x)+xf_{n-2}(x)+\cdots+x^{n-2}f_1(x)+x^{n-1}f_0(x)\Big)$$

e que $f'(x)=(f_{n-1}(x)+xf_{n-2}(x)+\cdots+x^{n-2}f_1(x)+x^{n-1}f_0(x))$.
Portanto $\mu(e)=1$.

Por outro lado, temos que

$$
\begin{aligned}
(1\otimes x)e \;=\; & \frac{-a_n}{f'(x)}\otimes 1+\frac{f_{n-1}(x)-a_{n-1}}{f'(x)}\otimes x+\cdots+\\
& +\frac{f_1(x)-a_1}{f'(x)}\otimes x^{n-1} \;=\; (x\otimes 1)e
\end{aligned}
$$

Observando que

$$(1 \otimes x^l)e = (1 \otimes x^{l-1})(1 \otimes x)e = (1 \otimes x^{l-1})(x \otimes 1)e = (x \otimes 1)(1 \otimes x^{l-1})e \ ,$$

tem-se por indução que $(1 \otimes x^l)e = (x^l \otimes 1)e$, para todo $l \geq 0$. Logo, para qualquer $z \in R[x]$, temos

$$\begin{aligned} z &= \sum_{l=0}^{n-1} \lambda_l x^l \ , \lambda_l \in R \ \text{ e} \\ (1 \otimes z)e &= \left(1 \otimes \sum_{l=0}^{n-1} \lambda_l x^l\right) e = \sum_{l=0}^{n-1} \lambda_l (1 \otimes x^l)e = \sum_{l=0}^{n-1} \lambda_l (x^l \otimes 1)e \\ &= \left[\left(\sum_{l=0}^{n-1} \lambda_l x^l\right) \otimes 1\right] e = (z \otimes 1)e \ . \end{aligned}$$

Assim $J(S)e = 0$.

f) Seja $S = \mathbb{R} \oplus \mathbb{R}_i \oplus \mathbb{R}_j \oplus \mathbb{R}_k$ a $\mathbb{R}$-álgebra dos quatérnios. O elemento

$$e = \frac{1}{4}(1 \otimes 1 - i \otimes i - j \otimes j - k \otimes k) \in S \otimes_{\mathbb{R}} S^0$$

é um idempotente de separabilidade de S sobre $\mathbb{R}$.

g) Seja $S = M_n(R)$ a álgebra de matrizes $n \times n$ com coeficientes em R. Sejam

$$e_{ij} = \begin{bmatrix} 0 & \cdots & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{bmatrix} \ , 1 \leq i,j \leq n \ .$$

as matrizes elementares de S, onde evidentemente o único elemento não nulo da matriz reside na linha i, coluna j. O elemento

$$e_j = \sum_{i=1}^{n} e_{ij} \otimes e_{ji}$$

para $1 \leq j \leq n$ é um idempotente de separabilidade de S sobre R.

h) Seja G um grupo finito de ordem n, com n sendo uma unidade de R. Então o anel de grupo $R[G]$ é uma R-álgebra separável, pois se tomarmos

$$e = \frac{1}{n}\sum_{\sigma} \sigma \otimes \sigma^{-1} \text{ em } [R[G]]^e ,$$

temos $\mu(e) = 1$ e, para todo $\tau \in G$,

$$(\tau \otimes 1)e = \frac{1}{n}\sum_{\sigma} \tau\sigma \otimes \sigma^{-1} = \frac{1}{n}\sum_{\rho} \rho \otimes \rho^{-1}\tau = (1 \otimes \tau)e ,$$

ou seja, $Je = 0$.

Observamos que na definição de extensão separável de um corpo k assim como na de k-álgebra separável assumimos a hipótese de dimensão finita. Esta hipótese é completamente omitida na definição de álgebra separável sobre um anel comutativo R. Ocorre mesmo que existem R-álgebras separáveis que não são sequer finitamente geradas como R-módulos, como bem mostra o exemplo 1.8.b.

Contudo, pode ser verificado que se S é uma R-álgebra separável conforme definido acima - isto é, S é um S^e-módulo projetivo - e R é um corpo, então necessariamente S é de dimensão finita sobre R (veja, por exemplo, Proposição III.3.2 de [3]).

Para uma abordagem ampla da teoria de álgebras separáveis sobre anéis recomendamos [2] e [3].

Concluiremos esta seção com uma generalização do exemplo 1.8.g, necessária ao que se segue. Vimos no exemplo 1.8.g, que a R-álgebra $A = M_{n\times n}(R)$ das matrizes $n \times n$ a coeficientes em R é R-separável. Observamos dois fatos adicionais:

(a) A é isomorfa à R-álgebra $\mathrm{Hom}_R(L, L)$ dos R- endomorfismos de um R-módulo livre L de posto n.

(b) A, e por conseguinte $\mathrm{Hom}_R(L,L)$, é uma R-álgebra *central*, isto é, o centro

$$C(A) = \{a \in A \mid ab = ba, \text{ para todo } \ b \in A\}$$

de A é igual a R.

Ambos os fatos acima mencionados são de verificação elementar e omitimos suas demonstrações.

Recordemos também que um R-módulo M é dito *fiel* se a aplicação natural

$$\begin{aligned} R &\to \mathrm{Hom}_R(M,M) \\ r &\mapsto f_r : m \mapsto rm \end{aligned}$$

é injetiva. Obviamente, todo R-módulo livre é fiel.

O teorema seguinte é a generalização acima referida.

Teorema 1.9: *Seja P um R-módulo projetivo, finitamente gerado e fiel. Então a R-álgebra $A = Hom_R(P,P)$ é central e separável.*

Para a demonstração deste teorema necessitamos de alguns resultados preliminares.

Seja P um R-módulo projetivo e finitamente gerado. Logo, pelo Teorema 1.5, existem elementos $p_i \in P$ e $f_i \in P^* = \mathrm{Hom}_R(P,R)$, $1 \leq i \leq n$, tais que $p = \sum_{i=1}^n f_i(p)p_i$, para todo $p \in P$. Disto decorre que $P = \mathrm{tr}(P)P$, onde $\mathrm{tr}(P)$ é o ideal de R formado pelos elementos da forma $f(p)$, para todo $p \in P$ e $f \in P^*$. Logo, existe $a \in \mathrm{tr}(P)$ tal que $(1-a)P = 0$. De fato, de $P = \mathrm{tr}(P)P$ temos $p_i = \sum_{j=1}^n a_{ij}p_j$, onde $a_{ij} = f_j(p_i)$, $i = 1, \cdots, n$. Disto

segue que $\sum_{j=1}^{n}(\delta_{ij} - a_{ij})p_j = 0$, $1 \leq i \leq n$, ou ainda

$$(\delta_{ij} - a_{ij})_{1\leq i,j\leq n} \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} .$$

Multiplicando esta última igualdade pela adjunta clássica da matriz $(\delta_{ij} - a_{ij})$ obtemos $\det(\delta_{ij} - a_{ij})p_i = 0$, para todo $1 \leq i \leq n$. Desde que $\det A = 1 - a$, para algum $a \in \mathrm{tr}(P)$, temos $(1 - a)P = 0$.

Se assumimos agora que P é também fiel então de $(1 - a)P = 0$ decorre que $1 = a \in \mathrm{tr}(P)$ e portanto $\mathrm{tr}(P) = R$.

Com isto mostramos o seguinte lema:

Lema 1.10: *Se P é um R-módulo projetivo, finitamente gerado e fiel então $tr(P) = R$.*

Demonstração do Teorema 1.9:

Do Lema 1.10 segue-se que existem elementos

$$x_1, \cdots, x_m \in P \quad \text{e} \quad g_1, \cdots, g_m \in P^*$$
$$\text{tais que} \qquad \sum_{j=1}^{m} g_j(x_j) = 1 .$$

Do Teorema 1.5 segue-se que existem elementos $p_i \in P$ e $f_i \in P^*$, $1 \leq i \leq n$, tais que $p = \sum_{i=1}^{n} f_i(p)p_i$, para todo $p \in P$. Definimos

$$E_{ij}\ , F_{ji} \in A = \mathrm{Hom}_R(P, P) \quad \text{por}$$
$$E_{ij}(p) = g_j(p)p_i \quad \text{e} \quad F_{ji}(p) = f_i(p)x_j$$

para todo $p \in P$, $1 \leq i \leq n$, $1 \leq j \leq m$.

Seja $e = \sum_{i,j} E_{ij} \otimes F^{\circ}_{ji} \in A \otimes_R A^{\circ}$. Mostremos que e é um idempotente

de separabilidade de A. De fato,

$$\begin{aligned}\mu(e)(p) &= \sum_{i,j} E_{ij}F_{ji}(p) = \sum_{i,j} E_{ij}\left(f_i(p)x_j\right) = \sum_{i,j} f_i(p)E_{ij}(x_j) \\ &= \sum_{i,j} f_i(p)g_j(x_j)p_i = \sum_i \left(\sum_j g_j(x_j)\right) f_i(p)p_i = \sum_{i=1} f_i(p)p_i \\ &= p\,,\end{aligned}$$

para todo $p \in P$. Portanto $\mu(e) = \mathrm{id}_P = 1_A$.

Para mostrar que $(f \otimes 1_A^o)e = (1_A \otimes f^0)\epsilon$, para todo $f \in A$, é suficiente verificarmos esta igualdade para um conjunto de geradores de A como R-módulo. Tal conjunto é

$$\{D_{kl} \,:\, 1 \leq k, l \leq n\}$$

onde $D_{kl}(p) = f_l(p)p_k$, para todo $p \in P$. De fato, se $f \in A$ e $f(p_k) = \sum_{l=1}^n c_{kl}p_l$ então

$$f(p) = f\left(\sum_{k=1}^n f_k(p)p_k\right) = \sum_{k=1}^n f_k(p)f(p_k) = \sum_{k,l} c_{kl}f_k(p)p_l = \sum_{k,l} c_{kl}D_{lk}(p)\,,$$

para todo $p \in P$; ou seja $f = \sum_{k,l} c_{kl}D_{lk}$.

Vejamos agora que $(D_{kl} \otimes 1_A^o)e = (1_A \otimes D_{kl}^o)e$. Observemos inicialmente que

$$(D_{kl} \otimes 1_A^o)\epsilon = (D_{kl} \otimes 1_A^o)\left(\sum_{i,j} E_{ij} \otimes F_{ji}^o\right) = \sum_{i,j} D_{kl}E_{ij} \otimes F_{ji}^o$$

e que

$$\begin{aligned}D_{kl}E_{ij}(p) &= D_{kl}(g_j(p)p_i) = f_l(g_j(p)p_i)p_k = g_j(p)f_l(p_i)p_k \\ &= f_l(p_i)g_j(p)p_k = f_l(p_i)E_{kj}(p) = r_{il}E_{kj}(p)\,,\end{aligned}$$

com $r_{il} = f_l(p_i) \in R$, para todo $p \in P$; ou seja $D_{kl}E_{ij} = r_{il}E_{kj}$. Então

$$(D_{kl} \otimes 1_A^o)\,e = \sum_{i,j} r_{il}E_{kj} \otimes F_{ji}^o = \sum_{i,j} E_{kj} \otimes r_{il}F_{ji}^o$$

Mas

$$\sum_i r_{il}F_{ji}(p) = \sum_i f_l(p_i)f_i(p)x_j = f_l\left(\sum_i f_i(p)p_i\right)x_j$$
$$= f_l(p)x_j = F_{jl}(p) ,$$

para todo $p \in P$; ou seja $\sum_i r_{il}F_{ji} = F_{jl}$.

Portanto $(D_{kl} \otimes 1_A^o)\, e = \sum_j E_{kj} \otimes F_{jl}^o$.

Por outro lado,

$$(1_A \otimes D_{kl}^o)\, e = \sum_{i,j} E_{ij} \otimes D_{kl}^o F_{ji}^o = \sum_{i,j} E_{ij} \otimes (F_{ji}D_{kl})^o \ .$$

Por raciocínio análogo ao que vimos acima, verifica-se que $F_{ji}D_{kl} = r_{ki}F_{jl}$ com $r_{ki} = f_i(p_l) \in R$. Então

$$(1_A \otimes D_{kl}^o)\, e = \sum_{i,j} E_{ij} \otimes r_{ki}F_{jl}^o = \sum_{i,j} r_{ki}E_{ij} \otimes F_{jl}^o$$
$$= \sum_j \left(\sum_i r_{ki}E_{ij}\right) \otimes F_{jl}^o \ .$$

Novamente, por raciocínio análogo ao visto acima, obtemos $\sum_i r_{ki}E_{ij} = E_{kj}$ e, portanto

$$(1_A \otimes D_{kl}^o)\, e = \sum_j E_{kj} \otimes F_{jl}^o = (D_{kl} \otimes 1_A^o)\, e \ .$$

Finalmente mostremos que A é central. Antes vejamos que $C(A) = eA$. De fato, para todo $f, g \in A$ temos

$$(ef)g = (1_A \otimes g^o)(ef) = [(1_A \otimes g^o)e]\, f = [(g \otimes 1_A^o)e]\, f$$
$$= (g \otimes 1_A^o)(ef) = g(ef)$$

e portanto $ef \in C(A)$. Isto mostra que $eA \subset C(A)$. Reciprocamente, para todo $f \in C(A)$ temos

$$ef = \left(\sum_{i,j} E_{ij} \otimes F_{ji}^o\right) f = \sum_{i,j} E_{ij}\ f\ F_{ji}$$

e portanto $\epsilon f \in C(A)$. Isto mostra que $\epsilon A \subset C(A)$. Reciprocamente, para todo $f \in C(A)$ temos

$$\begin{aligned} \epsilon f &= \left(\sum_{i,j} E_{ij} \otimes F_{ji}^{o}\right) f = \sum_{i,j} E_{ij}\, f\, F_{ji} \\ &= \left(\sum_{i,j} E_{ij} F_{ji}\right) f = \mu(\epsilon) f = 1_A f = f \end{aligned}$$

e portanto $C(A) = \epsilon A$.

Vejamos agora que $\epsilon A = R1_A$. Claramente, $R1_A \subset C(A) = \epsilon A$. Reciprocamente, para todo $D_{kl} \in A$ temos

$$\epsilon D_{kl} = \left(\sum_{i,j} E_{ij} \otimes F_{ji}^{o}\right) D_{kl} = \sum_{i,j} E_{ij} D_{kl} F_{ji} \quad \text{e}$$

$$\begin{aligned} E_{ij} D_{kl} F_{ji}(p) &= E_{ij} D_{kl}(f_i(p) x_j) = f_i(p) E_{ij}\left(D_{kl}(x_j)\right) \\ &= f_i(p) E_{ij}\left(f_l(x_j) p_k\right) = f_i(p) f_l(x_j) E_{ij}(p_k) \\ &= f_i(p) f_l(x_j) g_j(p_k) p_i \end{aligned}$$

donde segue que

$$\begin{aligned} \epsilon D_{kl}(p) &= \sum_{i,j} f_i(p) f_l(x_j) g_j(p_k) p_i = \sum_{j} f_l(x_j) g_j(p_k) \sum_{i} f_i(p) p_i \\ &= \sum_{j} f_l(x_j) g_j(p_k) p = \lambda_{kl} 1_A(p)\,, \end{aligned}$$

para todo $p \in P$, com $\lambda_{kl} = \sum_j f_l(x_j) g_j(p_k) \in R$.

Portanto $\epsilon D_{kl} \in R1_A$ e isto mostra que $\epsilon A \subset R1_A$. Consequentemente, $C(A) = \epsilon A = R1_A$, o que conclui a demonstração do teorema. ■

Referências

[1] Ch.W.Curtis, I.Reiner; Representation Theory of Finite Groups and Associative Algebras, Interscience Pub., New York, 1962.

[3] M.A.Knus, M.Ojanguren; Theórie de la Descente et Algèbre d'Azumaya, Springer Lect. Notes, **389**, 1974.

[4] P.J.McCarthy; Algebraic Extensions of Fields, Blaisdell Pub. Comp., London, 1966.

2 Extensões Galoisianas

Iniciamos esta seção com a definição usual de extensão galoisiana de um corpo. O objetivo é evidenciar, entre as diversas definições equivalentes de extensão galoisiana de um corpo, aquela que seja a mais naturalmente adequada a uma generalização ao contexto de anéis comutativos.

Seja k um corpo e L uma extensão de k. Dizemos que L é uma extensão galoisiana de k se L é uma extensão normal e separável de k. Dada L extensão de k e $G \subseteq \mathrm{Aut}_k L$ definimos a k-álgebra $\Delta(L,G)$ como o L-espaço vetorial com base $\{u_\sigma ; \sigma \in G\}$, munido da multiplicação

$$\left(\sum_{\sigma\in G} a_\sigma u_\sigma\right)\left(\sum_{\tau\in G} b_\tau u_\tau\right) = \sum_{\sigma,\tau\in G} a_\sigma \sigma(b_\tau) u_{\sigma\tau} \ .$$

Consideremos também a k-álgebra $\mathrm{Hom}_k(L,L)$ e o homomorfismo de k-álgebras dado por

$$\begin{aligned} \phi \ : \ \Delta(L,G) &\longrightarrow \mathrm{Hom}_k(L,L) \\ \sum_{\sigma\in G} a_\sigma u_\sigma(x) &\mapsto \phi(\textstyle\sum_{\sigma\in G} a_\sigma u_\sigma) : \mapsto \displaystyle\sum_{\sigma\in G} a_\sigma \sigma(x) \end{aligned}$$

para qualquer $x \in L$.

Teorema 2.1: *Seja k um corpo e L uma extensão de k. Consideremos $G \subseteq Aut_k L$ um subgrupo finito. São equivalentes:*

i. $L^G = k$;

ii. *L é extensão galoisiana de k e $G = Aut_k L$.*

iii. $|G| = \dim_k L$.

iv. $\dim_k L < \infty$ *e* $\phi : \Delta(L,G) \to Hom_k(L,L)$ *é um isomorfismo.*

Demonstração: As três primeiras equivalências constituem resultados conhecidos da teoria de Galois para corpos.Provaremos apenas a equivalência

(iii) $\Leftrightarrow$ (iv).

(iii) $\Longrightarrow$ (iv) Levando em conta a independência linear dos $\sigma \in G$ sobre L, temos que ϕ é injetiva. Por outro lado,

$$\dim_k \Delta(L,G) = \dim_k L.|G| = \dim_k L.\dim_k L = \dim_k \mathrm{Hom}_k(L,L) \ ,$$

donde temos que ϕ é sobrejetiva. Logo ϕ é um isomorfismo de k-álgebras.

(iv) $\Longrightarrow$ (iii) Temos que $\dim_k \Delta(L,G) = \dim_k \mathrm{Hom}_k(L,L)$, pois ϕ é um isomorfismo de k-álgebras. Como $\dim_k L < \infty$, tem-se que $\dim_k L.|G| = (\dim_k L)^2$, ou seja, $|G| = \dim_k L$. ■

Observando atentamente o teorema acima, vemos que algumas das definições de extensões galoisianas sobre corpos não são adequadas para o caso de anéis comutativos.

A definição dada pelo item (iii) não é conveniente para uma generalização sobre anéis, pois as extensões de anéis não são necessariamente módulos livres. A definição dada pelo item (ii) também não é adequada para o caso de extensões de anéis, pois não garante necessariamente a separabilidade, como veremos pelo exemplo abaixo.

Consideremos $R = \mathbf{Z}$ e $S = \mathbf{Z}[\sqrt{2}]$. Então S é uma R-álgebra que contém R como subanel e, considerada como R-módulo, é livre com base $\{1, \sqrt{2}\}$.

Seja $G = \langle\sigma\rangle$ onde $\sigma \in \mathrm{Aut}(S)$ é dado por

$$\sigma(a + b\sqrt{2}) = a - b\sqrt{2} \quad \text{para todo} \quad a, b \in R \ .$$

Notemos que $G \subseteq \mathrm{Aut}_R(S)$ e como $\sigma^2 = id_S$, $|G| = 2 = \dim_R S$. Além disso temos claramente $S^G = R$. Contudo S não é separável sobre R, pois não possui idempotente de separabilidade sobre R, como veremos a seguir.

Suponhamos que $e \in S \otimes_R S$ seja um idempotente de separabilidade de S sobre R. Então $\mu(e) = 1$ e $J(S)e = 0$, onde $\mu : S \otimes_R S \to S$ é o homomorfismo

de $S \otimes_R S$-módulos dado pela multiplicação de S e $J(S) = \ker \mu$. Como S é um R-módulo livre com base $\{1, \sqrt{2}\}$ então $S \otimes_R S$ é um $R-$módulo livre com base $\left\{1 \otimes 1, 1 \otimes \sqrt{2}, \sqrt{2} \otimes 1, \sqrt{2} \otimes \sqrt{2}\right\}$. Então, como $e \in S \otimes_R S$, $e = a1 \otimes 1 + b1 \otimes \sqrt{2} + c\sqrt{2} \otimes 1 + d\sqrt{2} \otimes \sqrt{2}$, com $a, b, c, d \in R$ e do fato de $\mu(e) = 1$ temos $(a + 2d) + (b + c)\sqrt{2} = 1$ donde se tem $a + 2d = 1$ e $b + c = 0$.

Como $J(S)e = 0$ temos em particular $(\sqrt{2} \otimes 1)e = (1 \otimes \sqrt{2})e$ donde se obtém

$$a\ \sqrt{2} \otimes 1 + b\ \sqrt{2} \otimes \sqrt{2} + 2c\ 1 \otimes 1 + 2d\ 1 \otimes \sqrt{2} =$$
$$a\ 1 \otimes \sqrt{2} + 2b\ 1 \otimes 1 + c\ \sqrt{2} \otimes \sqrt{2} + 2d\ \sqrt{2} \otimes 1$$

E desta última igualdade deduzimos que $a = 2d$ e $b = c$. Comparando estas equações com as obtidas anteriormente temos $b = c = 0$, $a = 2d$ e $2a = 1$. Esta última igualdade implica que 2 é invertível em $R = \mathbf{Z}$, o que é absurdo.

No que se segue R sempre denotará um anel comutativo com identidade 1 e o símbolo $\otimes$ significará o produto tensorial sobre R.

Consideremos S uma R-álgebra comutativa com elemento identidade também denotado por 1. Dizemos que S é uma *extensão* de R se S é fiel como R-módulo. Assim, se S é uma extensão de R, existe uma imersão natural $R \to S$ e podemos identificar R com sua imagem $R.1$ em S.

Consideremos S uma extensão de R e G um subgrupo finito de $\mathrm{Aut}_R(S)$. Analogamente à construção vista no início desta seção, seja $\Delta(S : G)$ o S-módulo livre com base $\{u_\sigma \mid \sigma \in G\}$, sobre o qual definimos a multiplicação

$$\left(\sum_{\sigma \in G} a_\sigma u_\sigma\right)\left(\sum_{\tau \in G} b_\tau u_\tau\right) = \sum_{\sigma,\tau \in G} a_\sigma \sigma(b_\tau) u_{\sigma\tau}$$

para todo $a_\sigma, b_\tau \in S$, $\sigma, \tau \in G$.

Consideremos a R-álgebra $\mathrm{Hom}_R(S,S)$ dos R-endomorfismo de S e a aplicação

$$\begin{aligned} \phi \quad &: \quad \Delta(S:G) \longrightarrow \mathrm{Hom}_R(S,S) \\ \sum_{\sigma\in G} a_\sigma u_\sigma \quad &\mapsto \quad \phi\left(\sum_{\sigma\in G} a_\sigma u_\sigma\right) : s \mapsto \sum_{\sigma\in G} a_\sigma \sigma(s) \end{aligned}$$

para qualquer $s \in S$. ϕ é claramente um homomorfismo de S-módulos e também um homomorfismo de R-álgebras.

Seja agora $\nabla(S:G)$ o S-módulo livre com base $\{v_\sigma ; \sigma \in G\}$ sobre o qual definimos a multiplicação

$$\left(\sum_{\sigma\in G} a_\sigma u_\sigma\right)\left(\sum_{\tau\in G} b_\tau u_\tau\right) = \sum_{\sigma,\tau\in G} a_\sigma b_\tau \delta_{\sigma\tau} v_\sigma$$

para quaisquer $a_\sigma, b_\tau \in S$, $\sigma, \tau \in G$. Aqui

$$\delta_{\sigma\tau} = \begin{cases} 1 & \text{se } \sigma = \tau \\ 0 & \text{se } \sigma \neq \tau \ . \end{cases}$$

$\nabla(S:G)$ é claramente uma S-álgebra comutativa com elemento identidade $1 = \sum_{\sigma\in G} v_\sigma$. Observemos que os $v_\sigma, \sigma \in G$, são idempotentes (não nulos) que verificam $v_\sigma v_\tau = 0$ se $\sigma \neq \tau$. Em consequência $\nabla(S:G)$ é isomorfo à S-álgebra

$$\underbrace{S \oplus S \cdots \oplus S}_{|G| \text{vezes}}.$$

Seja a aplicação

$$\begin{aligned} \psi \quad &: \quad S \otimes S \longrightarrow \nabla(S:G) \\ &\sum_{i=1}^{n} a_i \otimes b_i \mapsto \sum_{i=1}^{n} \sum_{\sigma\in G} a_i \sigma(b_i) v_\sigma \ . \end{aligned}$$

Considerando $S \otimes S$ como uma S-álgebra via a ação $s.a \otimes b = (sa) \otimes b$ para quaisquer $a, b, s \in S$, temos que ψ é um homomorfismo de S-álgebras (em

particular de R-álgebras). Agora temos condições de dar a noção de extensão galoisiana de um anel, conforme inicialmente pretendido, considerando-se as equivalências listadas no Teorema 2.1.

Sejam então S extensão de R e $G \subseteq \mathrm{Aut}_R S$ um subgrupo finito. S é dita *extensão galoisiana de R com grupo de Galois G*, se S é um R-módulo projetivo finitamente gerado e ϕ é um isomorfismo de R-álgebras.

O teorema seguinte nos dará outras definições equivalentes de extensões galoisianas.

Teorema 2.2: *Sejam S uma extensão de R e G um subgrupo finito de $Aut_R(S)$. Seja $S^G = \{x \in S; \sigma(x) = x,$ para todo $\sigma \in G\}$. São equivalentes:*

(a) *i.* S *é um R-módulo projetivo finitamente gerado.*

ii. $\phi : \Delta(S:G) \to Hom_R(S,S)$ *é um isomorfismo de R-álgebras.*

(b) *i.* $S^G = R$.

ii. $\psi : S \otimes S \to \nabla(S:G)$ *é um isomorfismo de S-álgebras.*

(c) *i.* $S^G = R$.

ii. existem elementos em $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ *tais que*

$$\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{1,\sigma} = \begin{cases} 1 & se\ \sigma = 1 \\ 0 & se\ \sigma \neq 1, \forall \sigma \in G\ . \end{cases}$$

(d) *i.* $S^G = R$.

ii. para cada $\sigma \neq 1$ *em G e para cada ideal maximal M de S, existe* $x \in S$ *tal que* $\sigma(x) - x \notin M$.

(e) *i.* $S^G = R$.

ii. para cada idempotente não nulo e de S e para cada par $\sigma \neq \tau$ *em G, existe* $x \in S$ *tal que* $\sigma(x)e \neq \tau(x)e$.

iii. S é separável sobre R.

Demonstração:

(a) $\Rightarrow$ (b) Comecemos mostrando que $S^G = R$. Como $G \subseteq \mathrm{Aut}_R(S)$ obviamente temos $R \subseteq S^G$.

Seja $s \in S^G$. Claramente S^G está contido no centro $C(\Delta(S : G))$ de $\Delta(S : G)$ e então $s \in C(\Delta(S : G))$. Assim $\phi(s) \in C(\mathrm{Hom}_R(S, S))$. Como S é um R-módulo projetivo finitamente gerado, então pelo Teorema 1.9 temos que $\mathrm{Hom}_R(S, S)$ é central e separável. Logo $C(\mathrm{Hom}_R(S, S)) \simeq R$ e por conseguinte $C(\Delta(S : G)) = R$ e $s \in R$.

Para provarmos que $\psi : S \otimes S \longrightarrow \nabla(S : G)$ é um isomorfismo de R-álgebras provaremos inicialmente que $\phi(t.S) \subseteq \mathrm{Hom}_R(S, R)$ para $t = \sum_{\sigma \in G} u_\sigma \in \Delta(S : G)$. Com efeito, para todo $a, s \in S$ temos

$$\phi(t.a) = \phi\left[\sum_{\sigma \in G} u_\sigma a u_1\right] = \phi\left[\sum_{\sigma \in G} \sigma(a) u_\sigma\right]$$

e então

$$\phi(t.a)(s) = \sum_{\sigma \in G} \sigma(a)\sigma(s) = \sum_{\sigma \in G} \sigma(as) \in S^G = R\,.$$

Isto prova que $\phi(t.s) \subseteq \mathrm{Hom}_R(S, R)$. Consideremos agora $f \in \mathrm{Hom}_R(S, R) \subseteq \mathrm{Hom}_R(S, S)$ e também $\omega \in \Delta(S : G)$, $\omega = \sum_{\sigma \in G} a_\sigma u_\sigma$, tal que $\phi(\omega) = f$. Então , para todo $s \in S, \phi(\omega)(s) = f(s) \in R$; ou seja, $\sum_{\sigma \in G} a_\sigma \sigma(s) \in R$. Logo, para todo $\rho \in G$,

$$\rho\left(\sum_{\sigma \in G} a_\sigma \sigma(s)\right) = \sum_{\sigma \in G} a_\sigma \sigma(s),$$

o que implica que

$$\sum_{\sigma \in G} \rho(a_\sigma)\rho\sigma(s) = \sum_{\sigma \in G} a_\sigma \sigma(s) = \sum_{\sigma \in G} a_{\rho\sigma} \rho\sigma(s),$$

para todo $s \in S$. Isto acarreta que $\rho(a_\sigma) = a_{\rho\sigma}$, para todo $\rho, \sigma \in G$ o que implica $\rho(a_1) = a_\rho$, para todo $\rho \in G$. Em consequência, $v = \sum_{\sigma \in G} \sigma(a_1) u_\sigma = \left(\sum_{\sigma \in G} u_\sigma\right) a_1 = t.a_1$. Portanto

$$f = \phi(v) = \phi(t.a_1) \in \phi(t.S) \ .$$

Isto nos mostra que $\phi(t.S) = \mathrm{Hom}_R(S, R)$.

Consideremos agora a seguinte sequência de isomorfismos de R-módulos:

$$\begin{array}{lllll} S \otimes S & \stackrel{\phi_1}{\to} & S \otimes t.S & \stackrel{\phi_2}{\to} & S \otimes \mathrm{Hom}_R(S, R) \stackrel{\phi_3}{\to} \\ s \otimes r & \mapsto & s \otimes t.r & \mapsto & s \otimes \phi(t.r) \quad \mapsto \end{array}$$

$$\begin{array}{lllll} \mathrm{Hom}_R(S, S) & \stackrel{\phi_4}{\to} & \Delta(S : G) & \stackrel{\phi_5}{\to} & \nabla(S : G) \\ g_{s \otimes r} & \mapsto & \sum_{\sigma \in G} s\sigma(r) u_\sigma & \mapsto & \sum_{\sigma \in G} s\sigma(r) \omega_\sigma \end{array}$$

onde

$$\begin{aligned} g_{s \otimes r}(s') &= s\phi(t.r)(s') = s\phi\left(\sum_{\sigma \in G} \sigma(r) u_\sigma\right)(s') \\ &= \phi\left(\sum_{\sigma \in G} s\sigma(r) u_\sigma\right)(s') \end{aligned}$$

para qualquer $s' \in S$. Assim temos

$$\psi(s \otimes r) = \sum_{\sigma \in G} s\sigma(r)\omega_\sigma = \phi_5 \circ \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1(s \otimes r),$$

para quaisquer $s, r \in S$, isto é , ψ é um isomorfismo de R-módulos. Já que ψ é um homomorfismo de R-álgebras tem-se o desejado.

b) $\Rightarrow$ c) Para a prova, consideremos $\psi^{-1}(v_1) = \sum_{j=1}^n x_j \otimes y_j \in S \otimes S$. Então $\psi\left(\sum_{j=1}^n x_j \otimes y_j\right) = v_1$, isto é

$$\sum_{\sigma \in G} \left(\sum_{j=1}^n x_j \sigma(y_j)\right) v_\sigma = v_1 \ .$$

Logo

$$\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{1,\sigma}, \forall \sigma \in G \ .$$

c) $\Rightarrow$ d) Suponhamos por absurdo que exista $\sigma \neq 1_G$ em G e que exista um ideal maximal M tal que $s - \sigma(s) \in M$, para todo $s \in S$. Então teremos em particular que $y_j - \sigma(y_j) \in M$ e assim

$$1 = \sum_{j=1}^{n} x_j(y_j - \sigma(y_j)) \in M \ ,$$

o que é absurdo. Logo tem-se o resultado.

d) $\Rightarrow$ c) Consideremos $\sigma \neq 1_G$ em G e $I \subset S$ o ideal gerado por $\{s - \sigma(s) \mid s \in S\}$. Pela hipótese, $I = S$ (pois se $I \subset S$ então existiria $I \subset M \subset S$ com M ideal maximal e isto pela hipótese é um absurdo). Assim existem elementos $x_1, \cdots, x_n, y_1, \ldots, y_n$ em S tais que

$$\sum_{j=1}^{n} x_j(y_j - \sigma(y_j)) = 1 \ .$$

Disto temos

$$\sum_{j=1}^{n} x_j y_j = 1 + \sum_{j=1}^{n} x_j \sigma(y_j) \ .$$

Consideremos $x_{n+1} = -\sum_{j=1}^{n} x_j \sigma(y_j)$ e $y_{n+1} = 1$. Então

$$\begin{aligned} \sum_{j=1}^{n+1} x_j y_j &= \sum_{j=1}^{n} x_j y_j + x_{n+1} y_{n+1} \\ &= 1 + \sum_{j=1}^{n} x_j \sigma(y_j) - \sum_{j=1}^{n} x_j \sigma(y_j) = 1 \end{aligned}$$

e

$$\begin{aligned} \sum_{j=1}^{n+1} x_j \sigma(y_j) &= \sum_{j=1}^{n} x_j \sigma(y_j) + x_{n+1} \sigma(y_{n+1}) \\ &= \sum_{j=1}^{n} x_j \sigma(y_j) - \sum_{j=1}^{n} x_j \sigma(y_j) = 0 \ . \end{aligned}$$

Portanto,

$$\sum_{j=1}^{n+1} x_j \sigma(y_j) = \delta_{1,\sigma} \ .$$

Suponhamos que H e H' sejam subconjuntos quaisquer de G que contém a identidade 1 de G, para os quais existem elementos

$$x_1, \cdots, x_n, y_1, \cdots, y_n, x'_1, \cdots, x'_m, y'_1, \cdots, y'_m \in S$$

tais que para todo $\sigma \in H$ e para todo $\sigma' \in H'$,

$$\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{1,\sigma} \text{ e } \sum_{k=1}^{m} x'_k \sigma'(y'_k) = \delta_{1,\sigma'} \ .$$

Então, para todo $\tau \in H \cup H'$ temos

$$\sum_{j=1}^{n} \sum_{k=1}^{m} x_j x'_k \tau(y_j y'_k) = \left(\sum_{j=1}^{n} x_j \tau(y_j) \right) \left(\sum_{k=1}^{m} x'_k \tau(y'_k) \right) \delta_{1,\tau} \ .$$

Como $G = \cup_{\sigma \neq 1} \{1, \sigma\}$, o resultado segue.

c) $\Rightarrow$ e) Sejam $x_1, \cdots, x_n, y_1, \cdots, y_n$ elementos de S que satisfazem

$$\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{1,\sigma}$$

para qualquer $\sigma \in G$ e consideremos $e = \sum_{j=1}^{n} x_j \otimes y_j$ em $S \otimes S$. Então $\sum_{j=1}^{n} x_j y_j = 1$. Além disso, para todo $s \in S$, $\mathrm{tr}(s) = \sum_{\sigma \in G} \sigma(s) \in S^G = R$ e

$$\begin{aligned} (s \otimes 1)e &= \sum_{j=1}^{n} s x_j \otimes y_j = \sum_{j=1}^{n} \sum_{k=1}^{n} \mathrm{tr}(s x_j y_k) x_k \otimes y_j \\ &= \sum_{k=1}^{n} x_k \otimes \sum_{j=1}^{n} \mathrm{tr}(s y_k x_j) y_j = \sum_{k=1}^{n} x_k \otimes y_k s \\ &= (1 \otimes s)e \ . \end{aligned}$$

Portanto S é separável sobre R. Sejam agora $\sigma, \tau \in G$ e $e \in S$ um idempotente não nulo. Suponhamos que

$$\sigma(s)e = \tau(s)e \text{ para todo } s \in S \ .$$

Assim

$$s\sigma^{-1}(e) = \sigma^{-1}\tau(s)\sigma^{-1}(e), \text{ para todo } s \in S .$$

Logo,

$$\begin{aligned} \sigma^{-1}(e) &= 1.\sigma^{-1}(e) = \sum_{j=1}^{n} x_j y_j \sigma^{-1}(e) \\ &= \sum_{j=1}^{n} x_j \sigma^{-1}\tau(y_j)\sigma^{-1}(e) \\ &= \delta_{1,\sigma^{-1}\tau}\sigma^{-1}(e) . \end{aligned}$$

Como $\sigma^{-1}(e) \neq 0$, então $\sigma^{-1}\tau = 1$ ou $\tau = \sigma$. Portanto se $\sigma \neq \tau$, sempre existe $s \in S$ tal que $\sigma(s)e \neq \tau(s)e$.

e) $\Rightarrow$ c) Consideremos $e = \sum_{j=1}^{n} x_j \otimes y_j$ em $S \otimes S$ o idempotente de separabilidade de S sobre R, isto é, $\mu(e) = \sum_{j=1}^{n} x_j y_j = 1$ e $(s \otimes 1 - 1 \otimes s)e = 0$, para todo $s \in S$. Para todo $\sigma \in G$, seja

$$e_\sigma = \mu((1 \otimes \sigma)(e)) \in S .$$

Como σ é um R-automorfismo de S então $1 \otimes \sigma$ é um S-automorfismo de $S \otimes S$.

Além disso, como S é comutativo, $\mu : S \otimes S \longrightarrow S$ é um homomorfismo de anéis. Logo, para qualquer $\sigma \in G$ temos $e_\sigma^2 = e_\sigma$ e para todo $s \in S$ $se_\sigma = \sigma(s)e_\sigma$.

Assim, por (e.ii), temos que $e_\sigma = 0$ ou $\sigma = 1$ e por conseguinte, para todo $\sigma \in G$,

$$\begin{aligned} \delta_{1,\sigma} &= e_\sigma = \mu((1 \otimes \sigma)(e)) \\ &= \mu\left(\sum_{j=1}^{n} x_j \otimes \sigma(y_j)\right) = \sum_{j=1}^{n} x_j \sigma(y_j) . \end{aligned}$$

c) $\Rightarrow$ a) Sejam $x_1, \cdots, x_n, y_1, \cdots, y_n$ elementos de S tais que

$$\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{1,\sigma}, \forall \sigma \in G \ .$$

Definimos $f_j \in \mathrm{Hom}_R(S, R)$ por

$$f_j(s) = \sum_{\sigma \in G} \sigma(s y_j), \forall s \in S \ .$$

Então para todo $s \in S$,

$$\begin{aligned} \sum_{j=1}^{n} f_j(s) x_j &= \sum_{j=1}^{n} \sum_{\sigma \in G} \sigma(s y_j) x_j \\ &= \sum_{\sigma \in G} \sigma(s) \sum_{j=1}^{n} \sigma(y_j) x_j \\ &= \sum_{\sigma \in G} \delta_{1,\sigma} \sigma(s) = s \ . \end{aligned}$$

Assim S é um R-módulo projetivo finitamente gerado.

Provemos agora que $\phi : \Delta(S : G) \to \mathrm{Hom}_R(S, S)$ é um homomorfismo sobrejetor. Seja $h \in \mathrm{Hom}_R(S, S)$ e consideremos o elemento

$$\omega = \sum_{\sigma \in G} \sum_{j=1}^{n} h(x_j) \sigma(y_j) u_\sigma \in \Delta(S : G) \ .$$

Então, para todo $s \in S$ temos

$$\begin{aligned} \phi(\omega)(s) &= \sum_{\sigma \in G} \sum_{j=1}^{n} h(x_j) \sigma(y_j) \sigma(s) = \sum_{j=1}^{n} h(x_j) \sum_{\sigma \in G} \sigma(y_j s) \\ &= h\left(\sum_{j=1}^{n} x_j \sum_{\sigma \in G} \sigma(y_j s) \right) = h\left[\sum_{\sigma \in G} \left(\sum_{j=1}^{n} x_j \sigma(y_j) \right) \sigma(s) \right] \\ &= h\left(\sum_{\sigma \in G} \delta_{1,\sigma} \sigma(s) \right) = h(s) \ . \end{aligned}$$

Logo $\phi(\omega) = h$.

Para finalizarmos provemos que ϕ é injetor. Consideremos

$$v = \sum_{\sigma \in G} a_\sigma u_\sigma \in \Delta(S : G) \text{ tal que } \phi(v) = 0 \ .$$

Então

$$\phi(v)(s) = 0, \text{ para todo } s \in S \ .$$

Portanto

$$\begin{aligned} 0 &= \sum_{\tau \in G} \sum_{j=1}^{n} \phi(v)(x_j) \ .\tau(y_j) u_\tau \\ &= \sum_{\tau \in G} \sum_{j=1}^{n} \sum_{\sigma \in G} a_\sigma \sigma(x_j) \tau(y_j) u_\tau \\ &= \sum_{\tau \in G} \sum_{\sigma \in G} a_\sigma \sigma \left(\sum_{j=1}^{n} x_j \sigma^{-1} \tau(y_j) \right) u_\tau \\ &= \sum_{\tau \in G} \sum_{\sigma \in G} a_\sigma \delta_{1, \sigma^{-1}\tau} u_\tau = \sum_{\sigma \in G} a_\sigma u_\sigma = v \ . \end{aligned}$$

■

Notemos agora que se S é um corpo então o item (ii) das condições (c) e (d) do Teorema 2.2 são trivialmente satisfeitas. Portanto elas caracterizam generalizações para anéis comutativos da noção clássica de extensão galoisiana finita de um corpo. Também temos que a equivalência dos itens (i) e (ii) da afirmação (b) do Teorema 2.2 é evidente no caso de extensões finitas de corpos. Finalmente observemos que na condição (e) do Teorema 2.2 o item (ii) é obviamente verificado para qualquer corpo, e o item (iii) é uma consequência do item (i) para extensões de corpos. Como vimos pelo exemplo anterior ao Teorema 2.2, isto não ocorre necessariamente para anéis comutativos.

Corolário 2.3: *Sejam S uma extensão galoisiana de R com grupo de Galois G. Então*

(a) Existe um elemento $c \in S$ *tal que* $\mathrm{tr}(c) = \sum_{\sigma \in G} \sigma(c) = 1$.

(b) R *é somando direto de* S *como* R*-módulo.*

(c) Se A *é uma* R*-álgebra comutativa com elemento identidade* 1, *e* G *atua sobre* $A \otimes S$ *via* $\sigma(a \otimes s) = a \otimes \sigma(s)$, *para todo* $s \in S$ *e* $a \in A$, *então* $A \otimes S$ *é uma extensão galoisiana de* A *com grupo de Galois* G.

Demonstração:

(a) Evidentemente $\mathrm{tr} \in \mathrm{Hom}_R(S, R)$ e $\mathrm{tr} = \phi(\sum_{\sigma \in G} u_\sigma)$, onde $\phi : \Delta(S : G) \to \mathrm{Hom}_R(S, S)$ é o isomorfismo dado na afirmação (a) do Teorema 2.2. Seja $t = \sum_{\sigma \in G} u_\sigma \in \Delta(S : G)$. Na prova de (a) $\to$ (b) do Teorema 2.2, demonstramos que $\mathrm{Hom}_R(S, R) = \phi(t.S)$. Portanto, para todo $f \in \mathrm{Hom}_R(S, R)$, existe $s \in S$ tal que $f = \phi(t.s) = \phi(\sum_{\sigma \in G} \sigma(s) u_\sigma)$ e em consequência

$$f(x) = \phi\left(\sum_{\sigma \in G} \sigma(s) u_\sigma\right)(x) = \sum_{\sigma \in G} \sigma(s)\sigma(x) = \sum_{\sigma \in G} \sigma(sx) = \mathrm{tr}(sx),$$

qualquer que seja $x \in S$. Isto mostra que, para todo $f \in \mathrm{Hom}_R(S, R)$, $f = \mathrm{tr}(s-)$ para algum $s \in S$. Por outro lado, S é um R-módulo projetivo finitamente gerado e fiel (pelo Teorema 2.2). Logo existem $x_1, \cdots, x_n \in S$ e $f_1, \cdots, f_n \in \mathrm{Hom}_R(S, R)$ tais que $\sum_{i=1}^n f_i(x_i) = 1$ (pelo Lema 1.10). Então existem $s_1, \cdots, s_n \in S$ tais que

$$f_i = \mathrm{tr}(s_i -) \quad \text{e} \quad 1 = \sum_{i=1}^n f_i(x_i) = \sum_{i=1}^n \mathrm{tr}(s_i x_i)$$
$$= \mathrm{tr}\left(\sum_{i=1}^n s_i x_i\right) = \mathrm{tr}(c)$$

para $c = \sum_{i=1}^n s_i x_i \in S$.

(b) Como, por (a), existe $c \in S$ tal que $\mathrm{tr}(c) = 1$, então a sequência de R-módulos $S \xrightarrow{\mathrm{tr}} R \to 0$ é exata. Definimos $\theta : R \to S$ por $\theta(r) = rc$, qualquer que seja $r \in R$. É claro que θ é um homomorfismo de R-módulos, $\mathrm{tr} \circ \theta = \mathrm{id}_R$ e por conseguinte, tem-se o resultado.

(c) Como, por (b), $S = R \oplus N$ para algum R-módulo N então $A \otimes S = (A \otimes R) \oplus (A \otimes N)$ e podemos identificar A com $A \otimes R$ em $A \otimes S$. Se $x_1, \cdots, x_n, y_1, \cdots, y_n$ são elementos de S que satisfazem

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma}$$

então $1 \otimes x_1, \cdots, 1 \otimes x_n, 1 \otimes y_1, \cdots, 1 \otimes y_n$ são elementos de $A \otimes S$ e

$$\sum_{i=1}^{n} (1 \otimes x_i)(1 \otimes y_i) = 1 \otimes \sum_{i=1}^{n} x_i \sigma(y_i) = 1 \otimes \delta_{1,\sigma} = \delta_{1,\sigma} \ .$$

Em consequência, resta mostrar que $A = (A \otimes S)^G$. Para todo $a \in A$, temos $\sigma(a \otimes 1) = a \otimes \sigma(1) = a \otimes 1$, qualquer que seja $\sigma \in G$ e portanto $A = A \otimes R \subseteq (A \otimes S)^G$.

Por (a), existe $c \in S$ tal que $\mathrm{tr}(c) = 1$. Então

$$\sum_{\sigma \in G} (1 \otimes \sigma)(1 \otimes c) = 1 \otimes 1 \ .$$

Seja agora $z \in (A \otimes S)^G$ e consideremos $1 \otimes c = \sum_{i=1}^{m} a_i \otimes s_i \in A \otimes S$. Logo,

$$z = z.1 \otimes 1 = z \sum_{\sigma \in G} (1 \otimes \sigma)(1 \otimes c) = \sum_{\sigma \in G} (1 \otimes \sigma)(z.1 \otimes c)$$

$$\begin{aligned} z &= \sum_{\sigma \in G} (1 \otimes \sigma)(z.1 \otimes c) = \sum_{\sigma \in G} (1 \otimes \sigma) \left(\sum_{i=1}^{m} a_i \otimes s_i \right) \\ &= \sum_{i=1}^{m} a \otimes \sum_{\sigma \in G} \sigma(s_i) = \sum_{i=1}^{m} a_i \otimes \mathrm{tr}(s_i) \in A \otimes R = A \ . \end{aligned}$$

Isto completa a demonstração do corolário. ■

Exemplos 2.4:

a) Todo anel comutativo R, com elemento identidade, é extensão galoisiana de si mesmo com grupo de Galois $G = \{\mathrm{id}_R\}$.

b) Consideremos R um anel comutativo com elemento identidade, G um grupo finito e $S = \oplus_{\sigma \in G} R e_\sigma$, onde $e_\sigma e_\tau = \delta_{\sigma\tau} e_\sigma, \forall \sigma, \tau \in G$ e $\sum_{\sigma \in G} e_\sigma = 1$. Seja a ação de G sobre S dada por $\sigma(e_\tau) = e_{\sigma\tau}$, para quaisquer $\sigma, \tau \in G$. Então S é uma extensão galoisiana de R com grupo de Galois G. De fato, usaremos o item (c) do Teorema 2.2.

Sejam $x_j = y_j = e_\sigma$, portanto

$$\sum_{\sigma \in G} e_\sigma \tau(e_\sigma) = \sum_{\sigma \in G} e_\sigma e_{\tau\sigma} = \begin{cases} 1 & \text{se } \tau = 1 \\ 0 & \text{se } \tau \neq 1 \end{cases} \text{, para todo } \tau \in G \, .$$

Seja $s \in S^G$. Então $s = \sum_{\sigma \in G} r_\sigma e_\sigma$ e $\tau(s) = s$. para todo $\tau \in G$.

Logo

$$\sum_{\sigma \in G} r_\sigma e_\sigma = \tau \left(\sum_{\sigma \in G} r_\sigma e_\sigma \right) = \sum_{\sigma \in G} r_\sigma e_{\tau\sigma} = \sum_{\sigma \in G} r_{\tau^{-1}\sigma} e_\sigma \, .$$

de onde segue que $r_{\tau^{-1}\sigma} = r_\sigma$, para quaisquer $\sigma, \tau \in G$ e consequentemente $r_\sigma = r_1$, para todo $\sigma \in G$.

Assim $s = \sum_{\sigma \in G} r_1 e_\sigma = r_1 \sum_{\sigma \in G} e_\sigma = r_1 \in R$. Portanto $S^G = R$ e S é uma extensão galoisiana de R com grupo de Galois G.

c) Seja R um anel comutativo com elemento identidade e n um número inteiro ≥ 2 tal que $\frac{1}{n} \in R$. Suponhamos que exista $\varepsilon \in R$ tal que $\varepsilon^n = 1$ e $(1 - \varepsilon^i)$ é uma unidade de R, para todo $i = 1, \cdots, n-1$. Seja $S = R[\mathsf{x}]/(\mathsf{x}^n - a) = R[x]$, com $x = \mathsf{x} + (\mathsf{x}^n - a)$. Seja G um grupo cíclico de ordem n e gerado por σ atuando sobre S via $\sigma(x) = \varepsilon x$ e $\sigma|_R = 1$. É imediato que $S^G = R$. Além disso $\sigma^i(x) - x = (\varepsilon^i - 1)x$ é invertível em S,

para todo $i = 1, \cdots, n-1$. Portanto S é extensão galoisiana de R, com grupo de Galois G (Teorema 2.2.d).

d) Seja R um anel comutativo com elemento identidade tal que $1/2 \in R$. Sejam $b, c \in R$ unidades tais que $(4b^3 - 27c^2) = d^2$, para alguma unidade $d \in R$. Consideremos $S = R[\mathsf{x}]/(\mathsf{x}^3 - b\mathsf{x} - c) = R[x]$, com $x = \mathsf{x} + (\mathsf{x}^3 - b\mathsf{x} - c)$. Seja G um grupo cíclico de ordem 3 cujo gerador σ atua sobre S via

$$\sigma(x) = \frac{3b}{d}x^2 - \frac{9c+d}{2d}x - \frac{2b^2}{d} \text{ e } \sigma|_R = 1 \ .$$

Não é difícil de ver que $S^G = R$ e desde que

$$\left[(x - \sigma(x))(\sigma(x) - \sigma^2(x))(x - \sigma^2(x))\right]^2 =$$
$$= 4b^3 - 27c^2 = d^2 \text{ é uma unidade}$$

de R, então S é uma extensão galoisiana de R, com grupo de Galois G (Teorema 2.2.d).

e) Seja R um anel comutativo com elemento identidade e de característica p primo. Sejam $a \in R$ e $S = R[\mathsf{x}]/(\mathsf{x}^p - \mathsf{x} - a) = R[x]$, com $x = \mathsf{x} + (\mathsf{x}^p - \mathsf{x} - a)$. Consideremos G um grupo cíclico de ordem p, cujo gerador σ atua sobre S via $\sigma(x) = x + 1$.

É fácil ver que $S^G = R$ e desde que

$$\sigma^i(x) - x = x + i - x = i \quad \text{é uma unidade de } R \ ,$$

para todo $i = 1, \cdots, p-1$, então S é uma extensão galoisiana de R com grupo de Galois G (Teorema 2.2.d).

f) Consideremos R um anel comutativo com elemento identidade e tal que $1/2 \in R$. Seja $r \in R$ uma unidade de R. Sejam $T = R[\mathsf{x}]/(\mathsf{x}^2 - r) = R[x]$, com $x = \mathsf{x} + (\mathsf{x}^2 - r)$ e $S = T \times T$. Seja G um grupo cíclico de ordem 4 cujo gerador σ atua sobre S via $\sigma(a + bx, c + dx) = (c - dx, a + bx)$ para quaisquer

$a, b, c, d \in R$. É imediato que $S^G = R$ e desde que

$$\begin{aligned} \sigma(x,0) - (x,0) &= (-x,x) \\ \sigma^2(x,x) - (x,x) &= 2(x,x) \\ \sigma^3(x,0) - (x,0) &= -(x,x) \end{aligned}$$

são unidades de S, então S é extensão galoisiana de R com grupo de Galois G (Teorema 2.2.d).

g) Seja R um anel comutativo com identidade e tal que $1/2 \in R$. Sejam $r, r' \in R$ unidades de R. Sejam $T = R[\mathsf{x}]/(\mathsf{x}^2 - r) = R[x]$, com $x = \mathsf{x} + (\mathsf{x}^2 - r)$, $T' = R[\mathsf{x}]/(\mathsf{x}^2 - r') = R[x']$, com $x' = \mathsf{x} + (\mathsf{x}^2 - r')$. T (resp. T') é claramente uma extensão galoisiana de R com grupo de Galois $H = \langle \sigma; \sigma^2 = 1 \rangle$ (resp. $H' = \langle \tau; \tau^2 = 1 \rangle$), onde $\sigma : x \mapsto -x$ (resp. $\tau : x' \mapsto -x'$). Então $S = T \otimes T'$ é uma extensão galoisiana de R com grupo de Galois $G = H \times H'$ (veja exemplo (h)).

h) Este exemplo generaliza o anterior.

Consideremos T e T' extensões galoisianas de R com grupos de Galois H e H', respectivamente. Então $S = T \otimes T'$ é um extensão galoisiana de R com grupo de Galois $G = H \times H'$ atuando sobre S via $(\sigma, \sigma')(t \otimes t') = \sigma(t) \otimes \sigma'(t')$ para qualquer $t \in T, t' \in T'$, $\sigma \in H$ e $\sigma' \in H'$.

De fato, como T e T' são extensões galoisianas com grupos H e H' respectivamente, existem $a_1, \cdots, a_n, b_1, \cdots, b_n \in T$ e $a'_1, \cdots, a'_m, b'_1, \cdots, b'_m \in T'$ com

$$\sum_{i=1}^{n} a_i \sigma(b_i) = \delta_{1,\sigma} \quad \text{para todo} \quad \sigma \in H$$

e

$$\sum_{j=1}^{m} a'_j \sigma'(b'_j) = \delta_{1,\sigma'} \quad \text{para todo} \quad \sigma' \in H'$$

Sejam $x_{ij} = a_i \otimes a'_j$ e $y_{ij} = b_i \otimes b'_j$, $1 \leq i \leq n$, $1 \leq j \leq m$. Então

$$\begin{aligned}\sum_{i,j} x_{ij}(\sigma,\sigma')(y_{ij}) &= \sum_{i,j}(a_i \otimes a'_j)(\sigma(b_i) \otimes \sigma'(b'_j)) \\ &= \sum_{i,j} a_i\sigma(b_i) \otimes a'_j\sigma'(b'_j) \\ &= \sum_i a_i\sigma(b_i) \otimes \sum_j a'_j\sigma'(b'_j) \;=\; \delta_{1,\sigma} \otimes \delta_{1,\sigma'} \;=\; \delta_{1,(\sigma,\sigma')}\end{aligned}$$

para todo $(\sigma,\sigma') \in H \times H'$. Além disso

$$\begin{aligned}(T \otimes T')^{H\times H'} &= \left((T \otimes T')^{H\times 1}\right)^{1\times H'} \;=\; (T^H \otimes T')^{1\times H'} \\ &= (R \otimes T')^{1\times H'} \;=\; R \otimes (T')^{H'} \;=\; R \otimes R \\ &= R\end{aligned}$$

Terminaremos esta seção enunciando e demonstrando o Teorema Fundamental da Teoria de Galois para anéis comutativos. Para a demonstração desse teorema, necessitamos do lema a seguir.

Sejam $f, g : S \to T$ homomorfismos de anéis. Diz-se que f, g são *fortemente distintos* se para todo idempotente não nulo e de T existe $s \in S$ tal que $f(s)e \neq g(s)e$.

Lema 2.5: *Sejam S uma R-álgebra comutativa com elemento identidade e separável. Seja $f : S \to R$ um homomorfismo de R-álgebras. Então existe um único idempotente $e \in S$ tal que $f(e) = 1$ e se $= f(s)e$ para qualquer $s \in S$. Além disso, se $f_1, \cdots, f_n : S \to R$ são homomorfismos de R-álgebras fortemente distintos dois a dois, então os correspondentes idempotentes $e_1, \cdots, e_n$ em S satisfazem $e_ie_j = 0$, se $i \neq j$ e $f_i(e_j) = \delta_{ij}$, para $i, j = 1, \cdots, n$.*

Demonstração:

Seja $f : S \to R$ um homomorfismo de R-álgebras. Sendo S uma R-álgebra separável existem elementos $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ tais que $\sum_{i=1}^n x_iy_i = 1$

e

$$\sum_{i=1}^{n} sx_i \otimes y_i = \sum_{i=1}^{n} x_i \otimes y_i s, \ \forall s \in S \ .$$

Seja

$$e = \sum_{i=1}^{n} f(x_i) y_i \in S \ .$$

Então

$$\begin{aligned} f(e) &= f\left(\sum_{i=1}^{n} f(x_i)y_i\right) = \sum_{i=1}^{n} f(x_i)f(y_i) \\ &= f\left(\sum_{i=1}^{n} x_i y_i\right) = f(1) = 1 \ . \end{aligned}$$

Agora, para todo $s \in S$, temos

$$\begin{aligned} (f \otimes 1)\left(\sum_{i=1}^{n} sx_i \otimes y_i\right) &= (f \otimes 1)\left(\sum_{i=1}^{n} x_i \otimes y_i s\right) \Rightarrow \\ \sum_{i=1}^{n} f(sx_i) \otimes y_i &= \sum_{i=1}^{n} f(x_i) \otimes y_i s \Rightarrow \\ \sum_{i=1}^{n} 1 \otimes f(sx_i)y_i &= \sum_{i=1}^{n} 1 \otimes f(x_i)y_i s \Rightarrow \\ 1 \otimes \sum_{i=1}^{n} f(s)f(x_i)y_i &= 1 \otimes \sum_{i=1}^{n} f(x_i)y_i s \Rightarrow \\ 1 \otimes f(s)e &= 1 \otimes se \ . \end{aligned}$$

Aplicando a esta igualdade o $S \otimes S$-homomorfismo $\mu : S \otimes S \to S$, induzido pela multiplicação de S, obtemos $f(s)e = se$, para todo $s \in S$. Se fizermos $s = e$, teremos $e = 1e = f(e)e = e^2$. Se e' é outro idempotente de S que verifica $f(e') = 1$ e $f(s)e' = se'$, para todo $s \in S$, então $e' = f(e)e' = ee' = e'e = f(e')e = e$. Assim acabamos a prova da primeira parte do lema.

Sejam agora $f_1, \cdots, f_n : S \to R$ homomorfismos de R-álgebras fortemente distintos dois a dois. Sejam $e_1, \cdots, e_n \in S$ os correspondentes idempotentes

verificando $f_i(e_i) = 1$ e $f_i(s)e_i = se_i$, para todo $s \in S$. Observemos que $e_{ij} = f_i(e_j)$ é um idempotente de R, para $i, j = 1, \cdots, n$ e que

$$f_i(s)e_{ij} = f_i(s)f_i(e_j) = f_i(se_j) = f_i(f_j(s)e_j) = f_j(s)f_i(e_j) = f_j(s)e_{ij},$$

para todo $s \in S$. Como f_i e f_j são fortemente distintos, concluímos que $f_i(e_j) = e_{ij} = 0$, se $i \neq j$. Logo $f_i(e_j) = \delta_{ij}$, para $i, j = 1, \cdots, n$. Finalmente, $e_ie_j = f_j(e_i)e_j = \delta_{ij}e_j = 0$ se $i \neq j$, com o que terminamos a demonstração do lema. ■

Sejam S uma extensão galoisiana de R com grupo de Galois G e $T \subseteq S$ um subanel. Diz-se que T é G-forte se, para todo $\sigma, \tau \in G$

$$\sigma|_T = \tau|_T$$

ou $\sigma|_T, \tau|_T : T \to S$ são fortemente distintos. Observemos que se S não possue idempotentes diferentes de 0 e 1 (por exemplo, S é um corpo) então a condição G-forte é claramente verificada para qualquer subanel de S.

Consideremos agora S extensão galoisiana de R com grupo de Galois G. Seja $H \subseteq G$ um subgrupo de G e $T \subseteq S$ uma R-subálgebra de S. Denotamos

$$\begin{aligned} S^H &= \{s \in S; \sigma(s) = s, \ \forall \sigma \in H\} \text{ e} \\ H_T &= \{\sigma \in G; \sigma(x) = x, \ \forall x \in T\} . \end{aligned}$$

Claramente S^H é uma R-subálgebra de S e H_T é um subgrupo de G. Podemos agora enunciar o Teorema Fundamental da Teoria de Galois, que estabelece uma correspondência bijetiva (que inverte inclusão) entre os subgrupos de G e as R-subálgebras separáveis e G-fortes de S via

$$\begin{aligned} &H \to S^H \quad \text{e} \\ &T \to H_T . \end{aligned}$$

Teorema 2.6 (Teorema Fundamental da Teoria de Galois): *Seja S uma extensão galoisiana de R com grupo de Galois G. Então*

(a) Seja $H \subseteq G$ subgrupo e $T = S^H$. Então T é uma R-álgebra separável e G-forte como subálgebra de S, S é uma extensão galoisiana de T com grupo de Galois H e $H = H_T$.

(b) Sejam T uma R-subálgebra separável e G-forte de S e $H = H_T$. Então $T = S^H$.

(c) Para cada $\sigma \in G$ e para cada R-subálgebra separável e G-forte T de S, $H_{\sigma(T)} = \sigma H_T \sigma^{-1}$. Em consequência, um subgrupo H de G é normal se, e somente se, $\sigma(S^H) = S^H$, para qualquer $\sigma \in G$ e neste caso S^H é uma extensão galoisiana de R com grupo de Galois G/H.

Demonstração:

(a) S é uma extensão galoisiana de R, com grupo de Galois G. Logo pelo item (c) do Teorema 2.2, existem elementos $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ satisfazendo

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma} \quad \text{para todo} \quad \sigma \in G \ .$$

Sendo $H \subseteq G$ subgrupo, então

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma} \quad \text{para todo} \quad \sigma \in H \ .$$

e assim S é uma extensão galoisiana de $S^H = T$, com grupo de Galois H.

Logo temos que S é um T-módulo projetivo e consequentemente $S \otimes S$ é um $T \otimes T$-módulo projetivo. Por outro lado S é uma R-álgebra separável e

portanto um $S \otimes S$-módulo projetivo e concluímos que S é um $T \otimes T$-módulo projetivo. Como S é extensão galoisiana de T então T é um somando direto de S como T-módulo (Corolário 2.3) e consequentemente T é um somando direto de S como $T \otimes T$-módulo. Logo T é um $T \otimes T$-módulo projetivo e assim T é uma R-álgebra separável.

Seja agora

$$H_T = \{\sigma \in G; \sigma(x) = x, \ \forall x \in T\} .$$

Logicamente $H \subset H_T$ e assim $S^{H_T} = S^H = T$.

Vemos também que S é uma extensão galoisiana de T com grupo de Galois H_T. E, pelo Teorema 2.2, temos que $|H_T| = \dim_S S \otimes S = |H|$ (existe um isomorfismo entre $S \otimes S$ e $\nabla(S : H_T)$). Logo $H = H_T$.

Mostremos agora que T é G-forte como subálgebra de S.

Como S é uma extensão galoisiana de T com grupo de Galois H, existe $c \in S$ tal que $\sum_{\rho \in H} \rho(c) = 1$ (Corolário 2.3). Sejam também os elementos $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ tais que

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma} \quad \text{para todo} \quad \sigma \in G .$$

Consideremos

$$x_i' = \sum_{\rho \in H} \rho(x_i c) \quad \text{e} \quad y_i' = \sum_{\rho \in H} \rho(y_i)$$

para cada $i = 1, \cdots, n$.

Observemos que $x_i', y_i' \in S^H = T$ para cada $i = 1, \cdots, n$ e que

$$\sum_{i=1}^{n} x_i' \sigma(y_i') = \begin{cases} 1 & \text{se } \sigma \in H \\ 0 & \text{se } \sigma \notin H, \end{cases} \quad \text{para todo} \quad \sigma \in G .$$

Consideremos agora $\sigma, \tau \in G$ tais que $\sigma|_T \neq \tau|_T$. Então $\tau^{-1}\sigma \notin H$. Se $e \in S$ é um idempotente não nulo tal que $\sigma(t)e = \tau(t)e$, para qualquer $t \in T$

então $\sigma(y_i')e = \tau(y_i')e$ e assim

$$e = \left(\sum_{i=1}^{n} x_i' y_i'\right) e = \sum_{i=1}^{n} x_i'(y_i' e) = \sum_{i=1}^{n} x_i' \tau^{-1}\sigma(y_i')e = 0e = 0$$

e portanto T é G-forte.

(b) Sejam T uma R-subálgebra separável e G-forte de S e $H = H_T$. Claramente $T \subset S^H$. Resta provarmos que $S^H \subset T$.

Pelo Corolário 2.3 temos que $S \otimes S$ é uma extensão galoisiana de $S = S \otimes R$ com grupo G atuando em $S \otimes S$ via a ação

$$\sigma(s \otimes s') = s \otimes \sigma(s') \quad s, s' \in S \quad \text{e } \sigma \in G \ .$$

Definimos uma ação de G sobre $\nabla(S : G)$ dada por

$$\rho(v_\sigma) = v_{\sigma\rho^{-1}} \quad \text{para todo} \quad \rho \in G \ .$$

Como $\psi : S \otimes S \to \nabla(S : G)$ é um isomorfismo de S-álgebras (Teorema 2.2) e

$$\psi(\sigma(x)) = \sigma(\psi(x)), \quad \text{para quaisquer} \quad x \in S \otimes S e \sigma \in G \ ,$$

pode-se ver facilmente que $\nabla(S : G)$ é uma extensão galoisiana de S com grupo de Galois G. Além disso, sendo S um R-módulo projetivo (Teorema 2.2) e $T \subset S^H \subset S$, podemos identificar $S \otimes T$ (respectivamente $S \otimes S^H$) com sua imagem em $S \otimes S^H$ (respectivamente $S \otimes S$). Assim temos

$$S \otimes T \subset S \otimes S^H \subset (S \otimes S)^H,$$

donde segue que

$$\psi(S \otimes T) \subset \psi((S \otimes S)^H) = (\psi(S \otimes S))^H = \nabla(S : G)^H$$

Notemos que se $\nabla(S : G)^H = \psi(S \otimes T)$ então

$$S \otimes S^H \subset (S \otimes S)^H = \psi^{-1}(\nabla(S : G)^H) = S \otimes T$$

e aplicando tr$\otimes$1 temos tr$(S)\otimes S^H \subset$ tr$(S)\otimes T$. Pelo Corolário 2.3, tr$(S) = R$ e consequentemente $S^H = R \otimes S^H \subset R \otimes T = T$.

Assim a prova do item (b) estará completa se mostrarmos que

$$\nabla(S:G)^H \subset \psi(S \otimes T) .$$

Sejam então $\sigma_1, \cdots, \sigma_r \in G$ representantes das respectivas classes laterais distintas de H em G. Sejam $f_i : \nabla(S:G) \to S$, para $i = 1, \cdots, r$, os homomorfismos de S-álgebras dados por

$$f_i\left(\sum_{\sigma \in G} a_\sigma v_\sigma\right) = a_{\sigma_i}$$

e consideremos $f_i|_{\psi(S\otimes T)}$. Então $f_1, \cdots, f_r : \psi(S \otimes T) \to S$ são homomorfismos fortemente distintos dois a dois. De fato, pela escolha dos σ_i, $1 \leq i \leq r$, podemos afirmar que $\sigma_i|_T \neq \sigma_j|_T$ (pois $H = H_T$). Logo, como T é G-forte, para cada idempotente não nulo $e \in S$, existe $t \in T$ tal que $\sigma_i(t)e \neq \sigma_j(t)e$ e por conseguinte temos

$$\begin{aligned} f_i(\psi(1 \otimes t))e &= f_i(\textstyle\sum_{\sigma\in G} \sigma(t)v_\sigma)e \\ &= \sigma_i(t)e \neq \sigma_j(t)e = f_j(\psi(1 \otimes t))e . \end{aligned}$$

Notemos também que T é uma R-álgebra separável e portanto $S \otimes T$ é uma S-álgebra separável. É suficiente observar que se $e_T \in T \otimes T$ é o idempotente de separabilidade de T sobre R então $1 \otimes e_T \in S \otimes (T \otimes T) = (S\otimes T)\otimes_S (S\otimes T)$ é o idempotente de separabilidade de $S\otimes T$ sobre S. Como ψ é um isomorfismo de S-álgebras então $\psi(S \otimes T)$ também é uma S-álgebra separável.

Usando agora o Lema 2.6, existem idempotentes $w_1, \cdots, w_r \in \psi(S \otimes T)$ tais que $f_i(x)w_i = xw_i$, para todo $x \in \psi(S \otimes T)$ e $f_i(w_j) = \delta_{ij}$, para $i, j = 1, \cdots, r$.

Notemos que $w_i \in \nabla(S : G)^H$, para todo $i = 1, \cdots, r$ e para que $\psi(S \otimes T) = \nabla(S : G)^H$ é suficiente provar que $\{w_1, \cdots, w_r\}$ é um sistema de geradores de $\nabla(S : G)^H$ como S-módulo.

Observemos que se $z = \sum_{\sigma \in G} s_\sigma v_\sigma \in \nabla(S, G)^H$ então $\rho(z) = z$, para todo $\rho \in H$ e disto temos

$$\sum_{\sigma \in G} s_\sigma v_{\sigma\rho^{-1}} = \sum_{\sigma \in G} s_\sigma v_\sigma \quad \text{ou} \quad \sum_{\sigma \in G} s_{\sigma\rho} v_\sigma = \sum_{\sigma \in G} s_\sigma v_\sigma$$

donde segue que $s_\sigma = s_{\sigma\tau}$, para quaisquer $\sigma \in G$ e $\rho \in H$. Em particular, $s_{\sigma_i} = s_{\sigma_i\rho}$, para todo $\rho \in H$, $i = 1, \cdots, r$. Então, como $G = \cup_{1 \leq i \leq r} \sigma_i H$, para todo $z \in \nabla(S, G)^H$, temos

$$z = \sum_{\sigma \in G} s_\sigma v_\sigma = \sum_{i=1}^{r} \sum_{\rho \in H} s_{\sigma_i\rho^{-1}} v_{\sigma_i\rho^{-1}} = \sum_{i=1}^{r} s_{\sigma_i} \left(\sum_{\rho \in H} \rho(v_{\sigma_i}) \right)$$

De $f_i(w_j) = \delta_{ij}$ e $w_i \in \nabla(S : G)^H$, $1 \leq i, j \leq r$, obtemos $w_i = \sum_{\rho \in H} \rho(v_{\sigma_i})$ e $z = \sum_{i=1}^{r} s_{\sigma_i} w_i$, para todo $z \in \nabla(S : G)^H$, o que conclui a demonstração de (b).

(c) A partir de (a) e (b) provamos diretamente a primeira parte de (c).

Finalmente, seja H subgrupo normal de G e $T = S^H$. Então $\sigma(T) = T$ para todo $\sigma \in G$. Consideremos $G/H = \{\overline{\sigma}_i;\ 1 \leq i \leq r\}$.

Definimos então $\overline{\sigma}_i : T \to T$ por $\overline{\sigma}_i(x) = \sigma_i(x)$ para todo $x \in T$, $i = 1, \cdots, r$. Logicamente esta ação de σ_i sobre T não depende do representante escolhido. Além disso $T^{G/H} = (S^H)^{G/H} = S^G = R$ e os $x_i', y_i' \in T, i = 1, \cdots, n$, construídos na parte (a), provam que a R-álgebra T e o grupo G/H satisfazem o Teorema 2.2. Logo T é uma extensão galoisiana de R com grupo G/H. ■

Notemos que a hipótese G-forte no Teorema 2.6 é indispensável, como comprova o exemplo seguinte. Seja $S = R_{e_0} \oplus R_{e_1} \oplus R_{e_2} \oplus R_{e_3}$, onde $e_i e_j =$

para quaisquer $i, j = 0, 1, 2, 3$ e $\sum_{i=0}^{3} e_i = 1$. Seja G um grupo cíclico de ordem 4 e gerador σ atuando em S via

$$\sigma(e_i) = e_{i+1}(\text{mod } 4) \ .$$

Seja $T = R(e_0 + e_1) \oplus R(e_2 + e_3)$. É fácil ver que T não é G-forte e $H_T = \{1\} = H_S$.

Referências

[1] S. Chase, D.K. Harrison, A. Rosenberg; Galois theory and Galois cohomology of commutative rings, Memoirs AMS **52** (1965), 15-33.

3 Extensões Abelianas – Grupo de Harrison

Seja R um anel comutativo com elemento identidade. Uma extensão galoisiana finita S de R, com grupo de Galois G, é dita *extensão abeliana* de R se G é abeliano.

A primeira construção formal do grupo $T(G,R)$ das extensões abelianas de R, com mesmo grupo de Galois G, foi feita por Harrison [2] em 1965. Seu objetivo nesse trabalho foi o de apresentar uma Teoria de Kummer para anéis que generalizasse a correspondente teoria clássica conhecida no caso de corpos.

A teoria de Kummer clássica, no contexto de corpos, pode ser resumida no seguinte teorema.

Teorema 3.1: *Seja k um corpo contendo uma raiz n-ésima primitiva da unidade. Então existe uma correspondência 1-1 entre os subgrupos finitos de $k^*/(k^*)^n$ e as extensões abelianas de k, cujo grupo de Galois tem ordem um divisor de n.*

(Para a demonstração deste Teorema, ver, por exemplo, [3], teorema 13, capítulo 2.)

O principal teorema do trabalho desenvolvido por Harrison, traduzido no contexto de extensões abelianas de R com o mesmo grupo de Galois G é o seguinte:

Teorema 3.2: *Sejam R um anel comutativo, cujos únicos idempotentes são 0 e 1, e G um grupo abeliano finito. Então existe uma correspondência 1-1 entre os subgrupos finitos de $T(G,R)$ e as extensões abelianas de R com*

grupo de Galois G.

(Para a demonstração deste Teorema, ver [2], teorema 8)

No caso específico em que R é um corpo contendo uma raiz n-ésima primitiva da unidade, como veremos na seção 5, $T(G,R) \simeq R^*/(R^*)^n$. Nessa mesma seção abordaremos o estudo do grupo $T(G,R)$ no caso em que G é um grupo abeliano finito de ordem n, n é uma unidade de R e R contém uma raiz n-ésima primitiva da unidade.

O isomorfismo $T(G,R) \simeq R^*/(R^*)^n$, nas condições descritas acima, mostra que, de fato, o Teorema 3.2 é uma generalização, no contexto de anéis, do Teorema 3.1. Além disso, o Teorema 3.2 apresenta um novo enfoque no estudo das extensões abelianas de um corpo que permite uma extensão natural ao contexto de anéis comutativos em geral.

Vejamos agora como é construído o grupo $T(G,R)$. Fixados o grupo abeliano finito G e o anel comutativo com elemento identidade R, consideramos o conjunto $T(G,R)$ de todas as classes de isomorfismo das extensões abelianas de R, com grupo de Galois G. Por isomorfismo de extensões abelianas de R entendemos algo mais do que simplesmente um isomorfismo de R-álgebras. Dizemos que duas extensões abelianas, S e S' de R, com mesmo grupo de Galois G, são *isomorfas* ou *G-isomorfas* se existe um isomorfismo de R-álgebras $f : S \to S'$ tal que $f\sigma = \sigma f$, para todo $\sigma \in G$.

Na realidade, na definição acima, podemos exigir menos do que um isomorfismo de R-álgebras que comuta com a ação do grupo G. De fato, é suficiente a existência de um homomorfismo de R-álgebras que comute com a ação do grupo G. Isto é decorrente da seguinte proposição:

Proposição 3.3: *Seja S uma extensão galoisiana de R com grupo de Galois G. Seja A uma extensão de R sobre a qual G atua como grupo de*

automorfismos de R-álgebras e tal que $A^G = R$. *Seja* $f : S \to A$ *um homomorfismo de R-álgebras tal que* $f\sigma = \sigma f$, *para todo* $\sigma \in G$. *Então* f *é um isomorfismo.*

Demonstração:

Pelo Teorema 2.2.c existem elementos $x_i, y_i \in S$, $1 \leq i \leq n$, tais que

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma} \ , \quad \text{para todo} \quad \sigma \in G \ .$$

Consideremos a aplicação traço

$$\begin{aligned} \mathrm{tr} \ : \ S \ &\to S^G = R \ \ (\text{resp. } \mathrm{tr} : \ A \to A^G = R) \\ s &\mapsto \sum_{\sigma \in G} \sigma(s) \ . \end{aligned}$$

Então, dado $a \in A$, temos

$$\begin{aligned} f\left(\sum_{i=1}^{n} x_i \ \mathrm{tr}(f(y_i)a)\right) &= \sum_{i=1}^{n} f(x_i) \ \mathrm{tr}(f(y_i)a) \\ &= \sum_{i=1}^{n} f(x_i) \sum_{\sigma \in G} \sigma(f(y_i)a) \\ &= \sum_{i=1}^{n} f(x_i) \sum_{\sigma \in G} f(\sigma(y_i))\sigma(a) \\ &= \sum_{\sigma \in G} f\left(\sum_{i=1}^{n} x_i \sigma(y_i)\right) \sigma(a) \\ &= \sum_{\sigma \in G} \delta_{1,\sigma} \sigma(a) \\ &= a \end{aligned}$$

o que mostra que f é sobrejetor.

Agora, dado $s \in S$ tal que $f(s) = 0$ temos

$$f(\sigma(y_i s)) = \sigma f(y_i s) = \sigma\left(f(y_i) f(s)\right) = \sigma(0) = 0$$

para todo $\sigma \in G$ e por conseqüinte $\mathrm{tr}(y_i s) = f(\mathrm{tr}(y_i s)) = 0$, para todo $i = 1, \cdots, n$. Logo,

$$0 = \sum_{i=1}^{n} x_i \mathrm{tr}(y_i s) = \sum_{\sigma \in G} \left(\sum_{i=1}^{n} x_i \sigma(y_i) \right) \sigma(s) = \sum_{\sigma \in G} \delta_{1,\sigma} \sigma(s) = s \ ,$$

o que mostra que f é injetor. ■

Retornemos agora ao conjunto $T(G, R)$ das classes de isomorfismo $[S]$ das extensões abelianas S de R com mesmo grupo de Galois G.

No que se seguirá o símbolo $\otimes$ significará sempre o produto tensorial sobre o anel comutativo R.

Sejam $[S], [S'] \in T(G, R)$. Então $S \otimes S'$ é uma extensão abeliana de $R \simeq R \otimes R$ com grupo de Galois $G \times G$ (cf. Exemplo 2.4.h). Denotemos por δG o subgrupo de $G \times G$ consistindo dos elementos da forma (σ^{-1}, σ), $\sigma \in G$. O grupo quociente $G \times G/\delta G$ é obviamente isomorfo a G via o isomorfismo natural $\sigma \mapsto (\sigma, 1) = (1, \sigma) \mathrm{mod}\ \delta G$. Pelo Teorema 2.6, $(S \otimes S')^{\delta G}$ é uma extensão abeliana de R com grupo de Galois $G \simeq G \times G/\delta G$. O grupo G age sobre $(S \otimes S')^{\delta G}$ da seguinte forma

$$\sigma \ : \ \sum_i s_i \otimes s_i' \ \mapsto \ \sum_i \sigma(s_i) \otimes s_i' = \sum_i s_i \otimes \sigma(s_i') \ ,$$

para quaisquer $s_i \in S$, $\forall s_i' \in S'$ e $\forall \sigma \in G$.

Definimos sobre $T(G, R)$ a operação $*$ dada por

$$[S] * [S'] = \left[(S \otimes S')^{\delta G} \right] \ , \quad \text{para todo} \quad [S], [S'] \in T(G, R) \ .$$

Pode-se ver facilmente que a operação $*$ está bem definida; isto é, sua definição independe da escolha dos representantes de classe considerados. A associatividade e a comutatividade da operação $*$ são conseqüências imediatas das correspondentes propriedades do produto tensorial. O elemento

neutro para a operação $*$ é representado pela extensão trivial (veja Exemplo 2.4.b) $E = E_G(R) = \oplus_{\tau \in G} R e_\tau$, onde os $e_\tau, \tau \in G$, são ortogonais dois a dois (isto é, $e_\sigma e_\tau = \delta_{\sigma\tau} e_\tau$, $\sigma, \tau \in G$) e de soma 1, com a ação de G sobre E dada por $\sigma(e_\tau) = e_{\sigma\tau}$, $\sigma, \tau \in G$.

De fato, dado $[S] \in T(G,R)$, notemos que a R-álgebra $S \circledcirc E$ é constituída dos elementos da forma

$$\sum_{\tau \in G} s_\tau \otimes e_\tau \quad \text{e, portanto, se} \quad \sum_{\tau \in G} s_\tau \otimes e_\tau \in (S \otimes E)^{\delta G}$$

temos

$$\begin{aligned} \sum_{\tau \in G} s_\tau \otimes e_\tau &= (\sigma^{-1}, \sigma) \left(\sum_{\tau \in G} s_\tau \otimes e_\tau \right) \\ &= \sum_{\tau \in G} \sigma^{-1}(s_\tau) \otimes \sigma(e_\tau) = \sum_{\tau \in G} \sigma^{-1}(s_\tau) \otimes e_{\sigma\tau} \end{aligned}$$

ou ainda,

$$\sum_{\rho \in G} s_\rho \otimes e_\rho = \sum_{\rho \in G} \sigma^{-1}(s_{\sigma^{-1}\rho}) \otimes e_\rho \, .$$

Da independência linear de $\{1 \otimes e_\rho \mid \rho \in G\}$ sobre $S \simeq S \otimes R$ decorre que $s_\rho = \sigma^{-1}(s_{\sigma^{-1}\rho})$, para todo $\rho \in G$ e portanto $s_\sigma = \sigma^{-1}(s_1)$, para todo $\sigma \in G$. Isto mostra que

$$(S \otimes E)^{\delta G} = \left\{ \sum_{\sigma \in G} \sigma^{-1}(s) \otimes e_\sigma \mid s \in S \right\} \, .$$

Definimos a aplicação

$$\begin{aligned} f \; : \; (S \otimes E)^{\delta G} &\to S \\ \sum_{\sigma \in G} \sigma^{-1}(s) \otimes e_\sigma &\mapsto s \, . \end{aligned}$$

Claramente, f é um isomorfismo de R-álgebras e $f(\sigma, 1) = (\sigma, 1) f$, para todo $\sigma \in G$, donde segue que $[S] * [E] = [S]$.

Finalmente, dado $[S] \in T(G,R)$, o elemento inverso $[S]^{-1}$ é representado pela própria extensão S, com a ação de G dada por $\sigma : s \mapsto \sigma^{-1}(s)$, para todo $\sigma \in G$, $s \in S$. De fato, observemos que a aplicação

$$\begin{aligned} h \ : \ S \otimes S &\to \oplus_{\rho \in G} S e_\rho \\ s \otimes t &\mapsto \sum_{\rho \in G} s\rho(t) e_\rho \ , \end{aligned}$$

onde os $e_\rho, \rho \in G$, são idempotentes ortogonais dois a dois e de soma 1 e ρ é um isomorfismo de S-álgebras (ver Teorema 2.2.b). Além disso, $S \otimes S$ e $\oplus_{\rho \in G} S e_\rho$ são extensões abelianas de R com grupo de Galois $G \times G$ agindo, respectivamente, sobre essas R-álgebras da seguinte forma:

$$\begin{aligned} (\sigma,\tau)(s \otimes t) &= \sigma(s) \otimes \tau^{-1}(t) \quad \text{e} \\ (\sigma,\tau)\left(\sum_{\rho \in G} s_\rho e_\rho\right) &= \sum_{\rho \in G} \sigma(s_\rho) e_{\sigma\tau\rho} \ , \quad \text{para todo} \quad \sigma,\tau \in G \ . \end{aligned}$$

Então

$$\begin{aligned} h((\sigma,\tau)(s \otimes t)) &= h(\sigma(s) \otimes \tau^{-1}(t)) = \sum_{\rho \in G} \sigma(s)\rho\tau^{-1}(t) e_\rho \\ &= \sum_{\delta \in G} \sigma(s)\sigma\delta(t) e_{\sigma\tau\delta} = \sum_{\delta \in G} \sigma(s\delta(t)) e_{\sigma\tau\delta} \\ &= (\sigma,\tau)\left(\sum_{\delta \in G} s\delta(t) e_\delta\right) = (\sigma,\tau) h(s \otimes t) \ , \end{aligned}$$

para quaisquer $\sigma,\tau \in G$, $s,t \in S$.

Disto segue trivialmente que h induz (por restrição à $(S \otimes S)^{\delta G}$) um isomorfismo entre as R-álgebras $(S \otimes S)^{\delta G}$ e $E = \oplus_{\rho \in G} R\ e_\rho = (\oplus_{\rho \in G} S\ e_\rho)^{\delta G}$ tal que

$$h(\sigma,1) = (\sigma,1)h \ , \ \sigma \in G \ .$$

Portanto $T(G,R)$, com a operação $*$ acima definida, é um grupo abeliano.

Na realidade, pode ser visto que a construção acima feita nos dá um funtor $T(-,R)$ da categoria dos grupos abelianos finitos na categoria dos grupos abelianos (ver, por exemplo, [2]). Concluiremos esta seção mostrando que esse funtor é aditivo.

Consideremos os grupos $T(G_i,R)$, $i=1,2$ e as aplicações

$$\begin{aligned}
\varphi \;:\; & T(G_1,R)\times T(G_2,R) \;\to\; T(G_1\times G_2,R)\\
& ([S_1],[S_2]) \;\mapsto\; [S_1\otimes S_2]\;, \quad \text{para todo} \quad [S_i]\in T(G_i,R),\ i=1,2 \quad \text{e}\\
\psi \;:\; & T(G_1\times G_2,R) \;\to\; T(G_1,R)\times T(G_2,R)\\
& [S] \;\mapsto\; ([S^{1\times G_2}],[S^{G_1\times 1}])\;, \quad \text{para todo} \quad [S]\in T(G_1\times G_2,R)\;.
\end{aligned}$$

Pode-se ver facilmente que φ e ψ estão bem definidas e que φ é um homomorfismo de grupos. Além disso

$$\begin{aligned}
\psi\varphi([S_1],[S_2]) &= \psi([S_1\otimes S_2])\\
&= \left([(S_1\otimes S_2)^{1\times G_2}],[(S_1\otimes S_2)^{G_1\times 1}]\right) \quad \text{e,}
\end{aligned}$$

desde que $S_1\otimes S_2$ é uma extensão galoisiana de $S_1\otimes R\simeq S_1$ (resp. $R\otimes S_2\simeq S_2$) com grupo de Galois $G_2\simeq 1\times G_2$ (resp. $G_1\simeq G_1\times 1$) (ver Corolário 2.4.c) obtemos $(S_1\otimes S_2)^{1\times G_2}\simeq S_1$ e $(S_1\otimes S_2)^{G_1\times 1}\simeq S_2$. Evidentemente, esses isomorfismos comutam respectivamente com a ação de G_i, $i=1,2$, donde segue que $\psi\varphi=\mathrm{id}$. Reciprocamente, $\varphi\psi([S])=\varphi([S^{1\times G_2}],[S^{G_1\times 1}])=[S^{1\times G_2}\otimes S^{G_1\times 1}]$. A aplicação

$$\begin{aligned}
\theta \;:\; & S^{1\times G_2}\otimes S^{G_1\times 1} \;\to\; S\\
& s\otimes s' \;\mapsto\; ss'\;, \quad \text{para quaisquer} \quad s\in S^{1\times G_2},\ \text{e}\ s'\in S^{G_1\times 1}\;,
\end{aligned}$$

é claramente um homomorfismo de R-álgebras tal que

$$\theta(\sigma_1,\sigma_2)=(\sigma_1,\sigma_2)\theta\;, \quad \text{para todo} \quad \sigma_i\in G_i\;,\ i=1,2\;.$$

Logo, pela Proposição 3.3, θ é um isomorfismo de R-álgebras, o que mostra que $\varphi\psi = \mathrm{id}$. Portanto $\varphi : T(G_1, R) \times T(G_2, R) \rightarrow T(G_1 \times G_2, R)$ é um isomorfismo de grupos com $\varphi^{-1} = \psi$.

Este último resultado, juntamente com o Teorema Fundamental para grupos abelianos finitos, reduz o estudo do grupo $T(G, R)$ ao contexto de grupos G cíclicos.

Referências

[1] S. Chase, D.K. Harrison, A. Rosenberg, Galois theory and Galois cohomology of commutative rings, Memoirs AMS. **52** (1965), 15-33.

[2] D.K. Harrison, Abelian extensions of commutative rings, Memoirs AMS, **52** (1965), 1-14.

[3] P.J. Mc Carthy. Algebraic Extensions of Fields. Blaisdell Pub. Comp., London, 1966.

4 Módulos Projetivos de Posto 1 – Grupo de Picard

Em toda esta seção R denotará um anel comutativo com elemento identidade. O símbolo $\otimes$ denotará sempre o produto tensorial sobre R.

O posto de um R-módulo projetivo finitamente gerado é uma noção definida localmente. Para sua definição são necessários alguns resultados de natureza local-global. Em todos esses resultados o Lema de Nakayama é de fundamental importância. Por essa razão, iniciamos esta seção com este lema.

Lema 4.1 (Lema de Nakayama): *Seja $I \subset R$ um ideal de R. Sejam M um R-módulo finitamente gerado e N um R-submódulo de M. As seguintes propriedades são equivalentes:*

(a) $I \subset rad(R)$ *$(rad(R) = \cap\{m \subset R; m$ é ideal maximal de $R\})$.*

(b) $1 + I$ *é subgrupo do grupo R^* das unidades de R.*

(c) $IM = M$ *implica que* $M = 0$.

(d) $M = N + IM$ *implica que* $M = N$.

Demonstração:

(a) $\Rightarrow$ (b) Se $x \in I$ então $1 + x \notin m$, para todo ideal maximal m de R e portanto $1 + x \in R^*$.

(b) $\Rightarrow$ (a) Suponhamos que $I \not\subset m$ para algum ideal maximal m de R. Logo $I + m = R$ e portanto $1 = x + y$, com $x \in I$ e $y \in m$. Mas então $y = 1 - x \in R^*$ o que é um absurdo (pois $y \in m$).

(b) $\Rightarrow$ (c) Repetindo o raciocínio utilizado na demonstração do Lema 1.10, podemos assegurar que se $IM = M$, então existe $a \in I$ tal que $(1+a)M = 0$ e disto segue que $M = 0$.

(c) $\Rightarrow$ (d) Notemos que de $M = N + IM$ obtemos

$$\frac{M}{N} = \frac{N+IM}{N} \simeq \frac{IM}{IM \cap N} \simeq I\frac{M}{N}$$

e por (c) temos $M/N = 0$ ou $M = N$.

(d) $\Rightarrow$ (b) Sejam $x \in I$ e $u = 1 + x$. Desde que $1 = u - x$ então $r = r.1 = ru - rx \in Ru + IR$, para todo $r \in R$. Portanto $R = Ru + IR$ e por (d) $R = Ru$, ou seja, $u \in R^*$. ■

Teorema 4.2: *Seja P um R-módulo projetivo finitamente gerado. Seja I um ideal de R contido em rad(R). Se P/IP é um R/I-módulo livre então P é um R-módulo livre. Em particular, todo módulo projetivo finitamente gerado sobre um anel local é livre.*

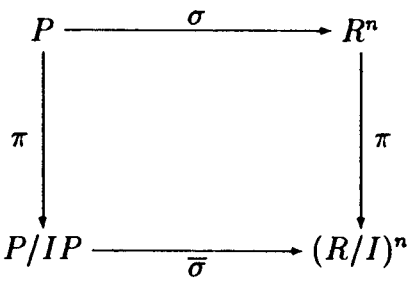
Demonstração:

Seja $I \subset \text{rad}(R)$. Desde que P/IP é livre, temos o seguinte diagrama:

$$\begin{array}{ccc} P & & R^n \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ P/IP & \xrightarrow[\overline{\sigma}]{} & (R/I)^n \end{array}$$

onde π denota a projeção canônica natural e $\overline{\sigma}$ é isomorfismo de R/I-módulos.

Desde que P é R-módulo projetivo e $R^n \xrightarrow{\pi} (R/I)^n \to 0$ é uma sequência exata de R-módulos, pelo Teorema 1.5 existe um homomorfismo de R-módulos $\sigma : P \to R^n$ tal que o diagrama



é comutativo. Desde que $\overline{\sigma}$ é sobrejetor, $\mathrm{Im}\sigma + IR^n = R^n$. Logo, pelo Lema de Nakayama $\mathrm{Im}\sigma = R^n$, ou seja, σ é sobrejetor. Portanto

$$P \xrightarrow{\sigma} R^n \to 0$$

é uma sequência exata de R-módulos e por conseguinte cinde (pois R^n é livre); isto é, $P \simeq R^n \oplus \ker\sigma$. Então $\ker\sigma$ é um R-módulo finitamente gerado. Desde que $\overline{\sigma}$ é injetor, $\ker\sigma/I\ker\sigma \subset \ker\overline{\sigma} = 0$ e consequentemente $\ker\sigma = I\ker\sigma$. Novamente, pelo Lema de Nakayama, temos $\ker\sigma = 0$, ou seja, σ é injetor. Portanto $\sigma : P \to R^n$ é um isomorfismo de R-módulos, ou seja, P é um R-módulo livre.

A segunda afirmação do teorema é imediata, uma vez que se R é um anel local com ideal maximal m então $\mathrm{rad}(R) = m$, $R/\mathrm{rad}(R) = R/m$ é corpo e todo R/m-módulo é um R/m-espaço vetorial e portanto livre. ■

Dados um ideal primo $\wp$ de R e $\Gamma = R - \wp$ a parte multiplicativa de R correspondente, é sabido que $R_\wp = \Gamma^{-1}R$ é um anel local com ideal maximal $\Gamma^{-1}\wp$. Logo, decorre do Teorema 4.2 que se P é um R-módulo projetivo finitamente gerado então o módulo de frações $\Gamma^{-1}P = \{\frac{p}{t} \mid p \in P,\ t \in \Gamma\} = P_\wp \simeq R_\wp \otimes P$ é um $R_\wp$-módulo livre de dimensão finita.

Definimos o *$\wp$-posto* de P como sendo a $\dim_{R_\wp} P_\wp$. Denotamos o $\wp$-posto de P por $\mathrm{rank}_\wp(P)$. Dizemos que P é um *R-módulo projetivo de posto constante n* se $\mathrm{rank}_\wp(P) = n$, para todo ideal primo $\wp$ de R. Em particular, P é

um *R-módulo projetivo de posto 1* se $\text{rank}_{\wp}(P) = 1$, para todo ideal primo $\wp$ de R.

Corolário 4.3: *Seja R um anel semi-local (isto é, um anel comutativo com apenas um número finito de ideais maximais). Se P é um R-módulo projetivo finitamente gerado e de posto constante então P é livre.*

Demonstração:

Seja m um ideal maximal de R. É fácil ver que $R/m \simeq Rm/mR_m$ e por conseguinte $\text{rank}_m(P) = \dim_{R/m}(P/mP)$.

Como P tem posto constante n, se $m_1, \cdots, m_t$ são todos os ideais maximais de R, então $n = \dim_{R/m_i}(P/m_iP)$ para todo $1 \leq i \leq t$ e

$$\begin{aligned}
\frac{P}{\text{rad}(R)P} &\simeq \frac{R}{\text{rad}(R)} \otimes P \simeq \left(\frac{R}{m_1} \times \cdots \times \frac{R}{m_t}\right) \otimes P \simeq \\
&\simeq \left(\frac{R}{m_1} \otimes P\right) \oplus \cdots \oplus \left(\frac{R}{m_t} \otimes P\right) \\
&\simeq \frac{P}{m_1P} \oplus \cdots \oplus \frac{P}{m_tP} \\
&\simeq \left(\frac{R}{m_1}\right)^n \oplus \cdots \oplus \left(\frac{R}{m_t}\right)^n \\
&\simeq \left(\frac{R}{m_1} \times \cdots \times \frac{R}{m_t}\right)^n \\
&\simeq \left(\frac{R}{\text{rad}(R)}\right)^n .
\end{aligned}$$

Então $P/\text{rad}(R)P$ é livre como $R/\text{rad}(R)$-módulo e, portanto, pelo Teorema 4.2, P é um R-módulo livre. ■

Para a próxima caracterização de módulo projetivo de posto 1 que abordaremos, e que nos será extremamente útil na sequência, necessitamos de um "princípio local-global". Para tanto são necessárias algumas considerações sobre o espectro do anel R.

Denotamos por $\mathrm{Spec}(R)$ o conjunto de todos os ideais primos de R, chamado *espectro* de R. Para todo subconjunto E de R denotamos

$$\begin{aligned} V(E) &= \{\wp \in \mathrm{Spec}(R) \mid E \subseteq \wp\} \text{ e} \\ \Gamma(E) &= \{\wp \in \mathrm{Spec}(R) \mid E \not\subseteq \wp\} \end{aligned}$$

Observemos que esses conjuntos $V(E)$ satisfazem as seguintes propriedades:

(a) $V(0) = \mathrm{Spec}(R)$.

(b) $V(1) = V(R) = \emptyset$.

(c) Se $\{E_\lambda \mid \lambda \in \Lambda\}$ é uma família de ideais de R então

$$\cap_{\lambda\in\Lambda} V(E_\lambda) = V\left(\sum_{\lambda\in\Lambda} E_\lambda\right) .$$

(d) Se E_1 e E_2 são ideais de R então $V(E_1) \cup V(E_2) = V(E_1E_2)$.

(e) Se $E_1 \subseteq E_2$ então $V(E_1) \supseteq V(E_2)$.

Os conjuntos $\Gamma(E)$ verificam as propriedades complementares:

(a) $\Gamma(0) = \emptyset$.

(b) $\Gamma(1) = \Gamma(R) = \mathrm{Spec}(R)$.

(c) Se $\{E_\lambda \mid \lambda \in \Lambda\}$ é uma família de ideais de R então

$$\cup_{\lambda\in\Lambda} \Gamma(E_\lambda) = \Gamma\left(\sum_{\lambda\in\Lambda} E_\lambda\right) .$$

(d) Se $E_1 \subseteq E_2$ então $\Gamma(E_1) \subseteq \Gamma(E_2)$.

Esses conjuntos induzem uma topologia sobre $\mathrm{Spec}(R)$, onde os abertos são os conjuntos $\Gamma(E)$ e os fechados $V(E)$, para todo $E \subseteq R$. Esta topologia é chamada a *topologia de Zariski*. Além disso, como espaço topológico,

Spec(R) é compacto, isto é, toda cobertura de abertos de Spec(R) admite uma subcobertura finita. De fato, suponhamos que $\text{Spec}(R) = \cup_{\lambda\in\Lambda}\Gamma(E_\lambda)$. Podemos supor, sem perda de generalidade, que os E_λ são ideais de R, pois é fácil ver que $\Gamma(E_\lambda) = \Gamma$ (ideal gerado por E_λ). Assim, temos

$$\text{Spec}(R) = \cup_{\lambda\in\Lambda}\Gamma(E_\lambda) = \Gamma\left(\sum_{\lambda\in\Lambda} E_\lambda\right) .$$

Disto segue que $\sum_{\lambda\in\Lambda} E_\lambda = R$. Logo $1 \in \sum_{\lambda\in\Lambda} E_\lambda$ e consequentemente deve existir um subconjunto finito $J \subset \Lambda$ tal que $1 \in \sum_{\lambda\in J} E_\lambda$. Portanto,

$$\text{Spec}(R) = \Gamma(1) \subset \Gamma(\sum_{j\in J} E_j) = \cup_{j\in J}\Gamma(E_j) \subset \text{Spec}(R) ,$$

ou seja, $\text{Spec}(R) = \cup_{j\in J}\Gamma(E_j)$.

Teorema 4.4 (Princípio Local-Global): *Sejam M um R-módulo e $x \in M$. As seguintes afirmações são equivalentes:*

(a) $x = 0$.

(b) $x/1 = 0$ *em* $M_\wp$, *para todo* $\wp \in$ *Spec*(R).

Demonstração:

(a) $\Rightarrow$ (b) Óbvio.

(b) $\Rightarrow$ (a) Suponhamos que $x/1 = 0$ em $M_\wp$ para todo $\wp \in \text{Spec}(R)$. Logo, para cada $\wp \in \text{Spec}(R)$ existe $t_\wp \in R - \wp$ tal que $t_\wp x = 0$. Desde que $t_\wp \in R - \wp$ então $\wp \in \Gamma(Rt_\wp)$ e por conseguinte

$$\text{Spec}(R) = \cup_{\wp\in\text{Spec}(R)}\Gamma(Rt_\wp) .$$

Como Spec(R) é compacto, existem ideais primos $\wp_1, \cdots, \wp_n$ de R tais que $\text{Spec}(R) = \cup_{1\le i\le n}\Gamma(Rt_{\wp_i}) = \Gamma\left(\sum_{1\le i\le n} Rt_{\wp_i}\right)$ e portanto $R = \sum_{1\le i\le n} Rt_{\wp_i}$.

Logo existem $r_1, \cdots, r_n \in R$ tais que $1 = r_1 t_{\wp_1} + \cdots + r_n t_{\wp_n}$ e consequentemente

$$x = 1x = r_1 t_{\wp_1} x + \cdots + r_n t_{\wp_n} x = 0 \ .$$

■

Corolário 4.5: *Sejam M e N R-módulos e $\sigma : M \to N$ um homomorfismo. As seguintes afirmações são equivalentes:*

(a) σ é injetor (resp. sobrejetor, bijetor, nulo);

(b) $\sigma_\wp : M_\wp \to N_\wp$, dada por $x/t \mapsto \sigma(x)/t$, para quaisquer $t \in R - \wp$ e $x \in M$ é injetor (resp. sobrejetor, bijetor, nulo), para todo $\wp \in Spec(R)$.

Demonstração: Imediata. ■

Consideremos agora P um R-módulo qualquer e $P^* = \mathrm{Hom}_R(P, R)$. Seja a aplicação

$$\begin{aligned} [\ ,\ ] \ : \ P \times P^* &\to \mathrm{End}_R(P) = \mathrm{Hom}_R(P, P) \ , \\ (p, f) &\mapsto [p, f] \ : \ q \mapsto f(q)p \ , \end{aligned}$$

para quaisquer $p, q \in P$ e $f \in P^*$. $[\ ,\ ]$ é obviamente R-bilinear e portanto induz o seguinte homomorfismo:

$$\begin{aligned} [\ ,\ ] \ : \ P \otimes P^* &\to \mathrm{End}_R(P) \ , \\ p \otimes f &\mapsto [p, f] \ , \end{aligned}$$

para quaisquer $p \in P$ e $f \in P^*$.

Teorema 4.6: *Seja P um R-módulo. As seguintes afirmações são equivalentes:*

(a) P é um R-módulo projetivo e finitamente gerado.

(b) $[\ ,\ ] : P \otimes P^* \to End_R(P)$ *é um isomorfismo.*

Demonstração:

(a) $\Rightarrow$ (b) Suponhamos que P seja projetivo e finitamente gerado. Então existem $p_i \in P$ e $f_i \in P^*$, $1 \leq i \leq n$ tais que $p = \sum_{1\leq i\leq n} f_i(p)p_i$, para todo $p \in P$. Dado $\sigma \in \mathrm{End}_R(P)$ temos

$$[\ ,\ ]\left(\sum_{1\leq i\leq n} p_i \otimes f_i\sigma\right) = \sum_{1\leq i\leq n} [p_i, f_i\sigma] \quad \text{e}$$

$$\sum_{1\leq i\leq n} [p_i, f_i\sigma](p) = \sum_{1\leq i\leq n} f_i(\sigma(p))p_i = \sigma(p)\ , \quad \text{para todo} \quad p \in P\ ,$$

o que mostra que $\sum_{1\leq i\leq n}[p_i, f_i\sigma] = \sigma$, ou seja, $[\ ,\ ]$ é sobrejetor.

Seja agora $\alpha = \sum_{1\leq j\leq m} q_j \otimes g_j \in \ker[\ ,\ ]$. Então

$$\begin{aligned}\alpha &= \sum_{1\leq j\leq m} q_j \otimes g_j = \sum_{1\leq j\leq m}\left(\sum_{1\leq i\leq n} f_i(q_j)p_i\right) \otimes g_j \\ &= \sum_{i,j} f_i(q_j)p_i \otimes g_j = \sum_{i,j} p_i \otimes f_i(q_j)g_j\end{aligned}$$

e como

$$\begin{aligned}f_i(q_j)g_j(p) &= f_i(g_j(p)q_j) \\ &= f_i([q_j, g_j](p)) = f_i[q_j, g_j](p)\ ,\end{aligned}$$

para todo $p \in P$, temos

$$\begin{aligned}\alpha &= \sum_{i,j} p_i \otimes f_i(q_j)g_j = \sum_{i,j} p_i \otimes f_i[q_j, g_j] \\ &= \sum_i p_i \otimes f_i\left(\sum_j [q_j, g_j]\right) = 0\ .\end{aligned}$$

Portanto [,] é injetor, ou seja, [,] é um isomorfismo.

(b) $\Rightarrow$ (a) Suponhamos que [,] é um isomorfismo. Em particular [,] é sobrejetor. Então existem $p_i \in P$, $f_i \in P^*$, $1 \leq i \leq n$, tais que $\mathrm{id}_P = \sum_{1\leq i\leq n}[p_i, f_i]$. Logo, para todo $p \in P$, temos

$$p = \mathrm{id}_P(p) = \sum_{1\leq i\leq n} [p_i, f_i](p) = \sum_{1\leq i\leq n} f_i(p)p_i \ .$$

Decorre agora do Teorema 1.5 que P é um R-módulo projetivo finitamente gerado. ■

Observemos que a equivalência exata no Teorema 4.6 acima é a seguinte: P é projetivo finitamente gerado se, e somente se, [,] é sobrejetor. A injetividade de [,] é uma consequência da sua sobrejetividade.

Corolário 4.7: *Seja P um R-módulo projetivo finitamente gerado. As seguintes afirmações são equivalentes:*

(a) $rank_\wp(P) = 1$, para todo $\wp \in Spec(R)$.

(b) A aplicação $f : R \to End_R(P)$, dada por $f(r)p = rp$, para quaisquer $r \in R$ e $p \in P$, é um isomorfismo de R-módulos.

Demonstração:

(a) $\Rightarrow$ (b) Suponhamos que $\mathrm{rank}_\wp(P) = 1$, para todo $\wp \in \mathrm{Spec}(R)$. Logo $P_\wp \simeq R_\wp$ e consequentemente $\mathrm{End}_{R_\wp}(P_\wp) \simeq \mathrm{End}_{R_\wp}(R_\wp) \overset{f_\wp}{\simeq} R_\wp$, para todo $p \in \mathrm{Spec}(R)$. Pelo Corolário 4.5 decorre então que f é isomorfismo.

(b) $\Rightarrow$ (a) Se $\mathrm{End}_R(P) \overset{f}{\simeq} R$ então $P \otimes P^* \simeq R$ (pelo Teorema 4.6) e consequentemente $P_\wp \otimes P^*_\wp \simeq R_\wp$, donde segue que

$$(\dim_{R_\wp} P_\wp)(\dim_{R_\wp} P^*_\wp) = \dim_{R_\wp}(P_\wp \otimes P^*_\wp) = \dim_{R_\wp}(R_\wp) = 1 \ ,$$

para todo $\wp \in \mathrm{Spec}(R)$. Portanto $\mathrm{rank}_{\wp}(P) = 1$, para todo $\wp \in \mathrm{Spec}(R)$. ■

De acordo com este último corolário podemos então dizer que um R-módulo projetivo finitamente gerado P tem posto 1 se, e somente se, $\mathrm{End}_R(P) \simeq R$.

Denotemos por $\mathrm{Pic}(R)$ o conjunto das classes de isomorfismo $[P]$ dos R-módulos P projetivos de posto 1. Dados $[P]$, $[P'] \in \mathrm{Pic}(R)$ temos

$$\begin{aligned}\dim_{R_\wp}(P \otimes P')_\wp &= \dim_{R_\wp}(P_\wp \otimes P'_\wp) \\ &= (\dim_{R_\wp} P_\wp)(\dim_{R_\wp} P'_\wp) = 1.1 = 1, \quad \text{para todo} \quad \wp \in \mathrm{Spec}(R)\ ,\end{aligned}$$

e portanto $[P \otimes P'] \in \mathrm{Pic}(R)$. Definimos sobre $\mathrm{Pic}(R)$ a operação $*$ dada por

$$[P] * [P'] = [P \otimes P'], \quad \text{para quaisquer} \quad [P], [P'] \in \mathrm{Pic}(R)\ .$$

Claramente, devido às propriedades do produto tensorial, a operação $*$ está bem definida, é associativa e comutativa e o elemento neutro é a classe representada pelo R-módulo livre R. Pelo Teorema 4.6 e Corolário 4.7, o elemento inverso $[P]^{-1}$ é a classe representada pelo R-módulo $P^* = \mathrm{Hom}_R(P, R)$. Portanto $\mathrm{Pic}(R)$ é um grupo abeliano, chamado *grupo de Picard*. Se R é um anel tal que todo R-módulo projetivo finitamente gerado é livre (por exemplo, corpo, anel local ou semi-local) então $\mathrm{Pic}(R) = 1$. Este grupo $\mathrm{Pic}(R)$ será de fundamental importância no estudo da teoria de Kummer para anéis, que abordaremos na seção seguinte.

Sejam agora G um grupo abeliano finito e S uma extensão abeliana de R, com grupo de Galois G. Denotemos por RG a R-álgebra do grupo G, isto é, RG como R-módulo é livre com base G e a multiplicação sobre RG é aquela induzida pela multiplicação de G. Notemos que a extensão abeliana S tem uma estrutura natural de RG-módulo dada pela ação:

$$\sum_{\sigma \in G} r_\sigma \sigma \ : \ s \longmapsto \sum_{\sigma \in G} r_\sigma \sigma(s)\ , \quad \text{para todo} \quad s \in S\ .$$

Veremos a seguir que, de fato, S é um RG-módulo projetivo finitamente gerado. Pelo Teorema 2.2b, temos que as S-álgebras $S \otimes S$ e $E_G(S) = \oplus_{\sigma \in G} S e_\sigma$ (onde os e_σ, $\sigma \in G$, são idempotentes ortogonais e de soma 1) são isomorfos. O isomorfismo neste caso é dado por $h : s \otimes t \mapsto \sum_{\tau \in G} s\tau(t)e_\tau$. Por outro lado, $E_G(S)$ e $S \otimes S$ têm estruturas naturais de SG-módulos dados respectivamente, pelas ações:

$$\begin{aligned} s_\sigma &: \sum_{\tau \in G} s_\tau e_\tau \mapsto \sum_{\tau \in G} s s_\tau e_{\sigma^{-1}\tau} \quad \text{e} \\ s_\sigma &: s_1 \otimes s_2 \mapsto s s_1 \otimes \sigma(s_2) \ , \quad \text{para quaisquer} \quad s \in S, \ \sigma \in G \end{aligned}$$

Além disso,

$$\begin{aligned} h(s\sigma(s_1 \otimes s_2)) &= h(s s_1 \otimes \sigma(s_2)) = \sum_{\tau \in G} s s_1 \tau\sigma(s_2) e_\tau \\ &= \sum_{\rho \in G} s s_1 \rho(s_2) e_{\sigma^{-1}\rho} = s\sigma \left(\sum_{\rho \in G} s_1 \rho(s_2) e_\rho \right) \\ &= s\sigma h(s_1 \otimes s_2) \ , \quad \text{para quaisquer} \quad s \in S, \ \sigma \in G \ . \end{aligned}$$

Portanto $h : S \otimes S \to E_G(S)$ é um isomorfismo de SG-módulos. Desde que a aplicação k dada por

$$\begin{aligned} k \ : \ E_G(S) &\to SG \\ \sum_{\sigma \in G} s_\sigma e_\sigma &\mapsto \sum_{\sigma \in G} s_\sigma \sigma \ , \end{aligned}$$

é claramente um isomorfismo de SG-módulos, obtemos

$$S \otimes S \overset{h}{\simeq} E_G(S) \overset{k}{\simeq} SG \simeq S \otimes RG$$

como SG-módulos. Pelo Teorema 2.2.a, S é um R-módulo projetivo finitamente gerado e portanto $S \oplus M \simeq R^n$ para algum R-módulo M e $n \geq 1$. Consequentemente, $(RG)^n \simeq R^n \otimes RG \simeq (S \oplus M) \otimes RG \simeq (S \otimes RG) \oplus (M \otimes RG) \simeq$

$(S \otimes S) \oplus (M \otimes RG)$, ou seja, $S \otimes S$ é um RG-módulo projetivo finitamente gerado. Mas, pelo Corolário 2.3.b, R é um somando direto de S como RG-módulo e por conseguinte $S \simeq R \otimes S$ é um RG-somando direto de $S \otimes S$. Portanto S é um RG-módulo projetivo finitamente gerado.

Finalmente mostremos que $\mathrm{End}_{RG}(S) \simeq RG$, ou seja, que S tem posto 1 como RG-módulo projetivo finitamente gerado (conforme Corolário 4.7).

Notemos que a R-álgebra $\Delta(S,G)$ considerada no Teorema 2.2 é exatamente igual a SG como S-módulos. Além disso $\Delta(S,G)$ e $\mathrm{End}_R(S)$ têm uma estrutura natural de RG-módulos e o isomorfismo dado por

$$\begin{aligned} \phi \ : \ \Delta(S,G) &\to \mathrm{End}_R(S) \\ \sum_{\sigma\in G} a_\sigma u_\sigma &\mapsto \sum_{\sigma\in G} a_\sigma \sigma \text{ (cf. Teorema 2.2.a)} \end{aligned}$$

é claramente um isomorfismo de RG-módulos. Então, para mostrarmos que $\mathrm{End}_{RG}(S) \simeq RG$ é suficiente mostrarmos que $\phi(RG) = \mathrm{End}_{RG}(S)$, onde RG (resp. $\mathrm{End}_{RG}(S)$) é visto como um subanel de $\Delta(S,G)$ (resp. $\mathrm{End}_R(S)$) de maneira óbvia. Seja $f \in \mathrm{End}_{RG}(S) \subset \mathrm{End}_R(S)$. Logo existe

$$\begin{aligned} \alpha &= \sum_{\tau\in G} s_\tau u_\tau \ \in \Delta(S,G) \ \text{ tal que} \\ f &= \phi\left(\sum_{\tau\in G} s_\tau u_\tau\right) = \sum_{\tau\in G} s_\tau \tau \ , \end{aligned}$$

pois ϕ é sobrejetor. Como $f \in \mathrm{End}_{RG}(S)$ então $\sigma f = f\sigma$ e portanto

$$\begin{aligned} \sum_{\tau\in G} s_\tau \tau(\sigma(s)) &= \sigma\left(\sum_{\tau\in G} s_\tau \tau(s)\right) = \sum_{\tau\in G} \sigma(s_\tau)\sigma\tau(s) \\ &= \sum_{\tau\in G} \sigma(s_\tau)\tau(\sigma(s)) \ , \ \text{ para quaisquer } \ s \in S, \ \sigma \in G \ . \end{aligned}$$

Mas, para todo $t \in S$, $t = \sigma(s)$ para algum $s \in S$. Portanto temos

$$\sum_{\tau\in G} s_\tau \tau(t) = \sum_{\tau\in G} \sigma(s_\tau)\tau(t) \ , \ \text{ para quaisquer } \ t \in S, \ \sigma \in G \ ,$$

donde segue que

$$\phi\left(\sum_{\tau\in G} s_\tau u_\tau\right) = \sum_{\tau\in G} s_\tau\tau = \sum_{\tau\in G}\sigma(s_\tau)\tau = \phi\left(\sum_{\tau\in G}\sigma(s_\tau)u_\tau\right) ,$$

para todo $\sigma \in G$. Como ϕ é injetor, obtemos $\sum_{\tau\in G} s_\tau u_\tau = \sum_{\tau\in G}\sigma(s_\tau)u_\tau$ e consequentemente $s_\tau = \sigma(s_\tau)$, para quaisquer $\sigma, \tau \in G$, ou seja, $s_\tau \in S^G = R$, para todo $\tau \in G$. Isto mostra que $\alpha \in RG$ e por conseguinte $\mathrm{End}_{RG}(S) \subset \phi(RG)$. Reciprocamente, se $\alpha = \sum_{\tau\in G} r_\tau u_\tau \in RG$ então

$$\begin{aligned}\phi(\alpha)(\sigma(s)) &= \sum_{\tau\in G} r_\tau\tau(\sigma(s)) = \left(\sum_{\tau\in G} r_\tau\sigma(\tau(s))\right)\\ &= \sigma\left(\sum_{\tau\in G} r_\tau\tau(s)\right) = \sigma\phi(\alpha)(s) ,\end{aligned}$$

para quaisquer $s \in S$, $\sigma \in G$, ou seja, $\phi(\alpha) \in \mathrm{End}_{RG}(S)$. Disto concluímos que

$$\mathrm{End}_{RG}(S) = \phi(RG) \simeq RG .$$

Desta forma temos mostrado o seguinte teorema:

Teorema 4.8: *Toda extensão abeliana S de R, com grupo de Galois G, é um RG-módulo projetivo finitamente gerado de posto* 1.

Corolário 4.9: *Seja S uma extensão abeliana de R com grupo de Galois G. Se R é corpo então $S \simeq RG$ como RG-módulos.*

Demonstração:

É suficiente observar que se R é corpo, então RG é anel semi-local. O resultado decorre então do Corolário 4.3 e do Teorema 4.8. ■

Uma extensão galoisiana S de R com grupo de Galois G é dita ter *base normal* se existe $s \in S$ tal que $\{\sigma(s) \mid \sigma \in G\}$ é base de S como R-módulo

livre. Isto é equivalente a dizer que $S \simeq RG$ como RG-módulos. Portanto o Corolário 4.9 pode ser reformulado da seguinte maneira:

Corolário 4.10: *Seja S uma extensão abeliana de R, com grupo de Galois G. Se R é corpo então S tem base normal.*

Graças ao Teorema 4.8 temos então uma aplicação

$$\theta : T(G,R) \rightarrow \mathrm{Pic}(RG)$$

definida de modo óbvio. Concluiremos esta seção mostrando que θ é um homomorfismo de grupos abelianos.

Para diferenciar e condensar a notação, denotaremos por $\otimes$ (resp. $\bigotimes$) o produto tensorial sobre R (resp. RG), por $[S]$ (resp. $[\![S]\!]$) a classe de isomorfismo representada por S em $T(G,R)$ (resp. $\mathrm{Pic}(RG)$) e por $*$ (resp. $\ast$) a operação de multiplicação em $T(G,R)$ (resp. $\mathrm{Pic}(RG)$).

Dados $[S_1],[S_2] \in T(G,R)$, definimos sobre $S_1 \bigotimes S_2$ a seguinte operação:

$$(s_1 \bigotimes s_2) \circ (s_1' \bigotimes s_2') = \sum_{\sigma \in G} \sigma^{-1}(s_1)s_1' \bigotimes \sigma(s_2)s_2' \ .$$

Pode ser verificado facilmente que esta operação está bem definida e que ela define sobre $S_1 \bigotimes S_2$ uma estrutura de anel associativo e comutativo.

Seja $e_i \in S_i$, $i = 1,2$, os elementos verificando $\mathrm{tr}(e_i) = \sum_{\sigma \in G} \sigma(e_i) = 1$ (ver Corolário 2.3.a). Então,

$$\begin{aligned}
e_1 \bigotimes 1 &= e_1 \bigotimes \sum_{\sigma \in G} \sigma(e_2) = \sum_{\sigma \in G} \sigma(e_1) \bigotimes e_2 = 1 \bigotimes e_2 \ ; \\
(s_1 \bigotimes s_2) \circ (e_1 \bigotimes 1) &= \sum_{\sigma \in G} \sigma^{-1}(s_1)e_1 \bigotimes \sigma(s_2) = \sum_{\sigma \in G} s_1\sigma(e_1) \bigotimes s_2 \\
&= s_1 \left(\sum_{\sigma \in G} \sigma(e_1) \right) \bigotimes s_2 = s_1 \bigotimes s_2 \quad \text{e} \\
(e_1 \bigotimes 1) \circ (s_1 \bigotimes s_2) &= \sum_{\sigma \in G} \sigma^{-1}(e_1)s_1 \bigotimes s_2 = s_1 \bigotimes s_2 \ ;
\end{aligned}$$

ou seja, $e_1 \otimes 1 = 1 \otimes e_2$ é o elemento neutro para a operação o.

Além disso, $S_1 \otimes S_2$ é uma R-álgebra e G age sobre $S_1 \otimes S_2$ via a ação $\sigma(s_1 \otimes s_2) = \sigma(s_1) \otimes s_2 = s_1 \otimes \sigma(s_2)$, o que dá a estrutura de RG-módulo.

Se $r \in R$ é tal que $e_1 \otimes r = 0$, então

$$1 \otimes r = \sum_{\sigma \in G} \sigma(e_1) \otimes r = e_1 \otimes \sum_{\sigma \in G} \sigma(r) = |G| e_1 \otimes r = 0 \ .$$

Isto nos permite identificar R com $e_1 \otimes R$ em $S_1 \otimes S_2$.

A aplicação tr dada por

$$\begin{aligned} \mathrm{tr} \ : \ S_1 \otimes S_2 &\to S_1 \otimes S_2 \\ s_1 \otimes s_2 &\mapsto \sum_{\sigma \in G} \sigma(s_1) \otimes s_2 = s_1 \otimes \sum_{\sigma \in G} \sigma(s_2) \ , \end{aligned}$$

é R-linear e

$$\begin{aligned} \mathrm{tr}(s_1 \otimes s_2) &= 1 \otimes \mathrm{tr}(s_1) s_2 \\ &= \mathrm{tr}(e_1) \otimes \mathrm{tr}(s_1) s_2 \ = \ e_1 \otimes \mathrm{tr}(\mathrm{tr}(s_1) s_2) \\ &= e_1 \otimes \mathrm{tr}(s_1) \mathrm{tr}(s_2) \ \in e_1 \otimes R \ = \ R \ . \end{aligned}$$

Além disso, $\mathrm{tr}(e_1 \otimes e_2) = e_1 \otimes \mathrm{tr}(e_2) = e_1 \otimes 1$. Portanto $\mathrm{tr}(S_1 \otimes S_2) = R$ e, considerando que tr é também $(S_1 \otimes S_2)^G$-linear, obtemos

$$(S_1 \otimes S_2)^G = R \ .$$

Consideremos agora a aplicação

$$\begin{aligned} f \ : \ (S_1 \otimes S_2)^{\delta G} &\to S_1 \otimes S_2 \\ \sum_i s_i \otimes t_i &\mapsto \sum_i s_i e_1 \otimes t_i \ . \end{aligned}$$

Observemos que dados

$$\alpha, \alpha' \in (S_1 \otimes S_2)^{\delta G} \ , \ \alpha = \sum_i s_i \otimes t_i \ , \quad \alpha' = \sum_j s'_j \otimes t'_j \ ,$$

temos

$$\begin{aligned} f(\alpha)\circ f(\alpha') &= \left(\sum_i s_i e_1 \otimes t_i\right)\circ\left(\sum_j s'_j e_1 \otimes t'_j\right) \\ &= \sum_{\sigma\in G}\sum_{i,j}\left(\sigma^{-1}(s_i e_1)s'_j e_1 \otimes \sigma(t_i)t'_j\right) \\ &= f\left(\sum_{\sigma\in G}\sum_{i,j}\sigma^{-1}(s_i e_1)s'_j \otimes \sigma(t_i)t'_j\right) \\ &= f\left[\sum_{\sigma\in G}(\textstyle\sum_i \sigma^{-1}(s_i)\otimes\sigma(t_i))\left(\sum_j s'_j\otimes t'_j\right)(\sigma^{-1}(e_1)\otimes 1)\right] \\ &= f\left[(\textstyle\sum_i s_i\otimes t_i)\left(\sum_j s'_j\otimes t'_j\right)(\sum_{\sigma\in G}\sigma^{-1}(\epsilon_1)\otimes 1)\right] \\ &= f\left[(\textstyle\sum_i s_i\otimes t_i)\left(\sum_j s'_j\otimes t'_j\right)\right] = f(\alpha\alpha') \end{aligned}$$

Portanto f é uma aplicação multiplicativa. Além disso, f é claramente R-linear e

$$\begin{aligned} &f(\sigma(\alpha)) = f(\textstyle\sum_i \sigma(s_i)\otimes t_i) = f(\sum_i s_i\otimes\sigma(t_i)) \\ &= \sum_i s_i e_1\otimes\sigma(t_i) = \sigma(\textstyle\sum_i s_i e_1\otimes t_i) \\ &= \sigma f(\alpha)\ , \quad \text{para quaisquer } \alpha = \sum_i s_i\otimes t_i \in (S_1\otimes S_2)^{\delta G} \text{ e } \sigma\in G\ . \end{aligned}$$

Isto mostra que f é um homomorfismo de RG-módulos e de R-álgebras. Pela Proposição 3.3 decorre então que f é isomorfismo de R-álgebras e RG-módulos. Consequentemente,

$$\begin{aligned} \theta([S_1]*[S_2]) &= \theta\left([(S_1\otimes S_2)^{\delta G}]\right) = [\![(S_1\otimes S_2)^{\delta G}]\!] \\ &= [\![S_1\otimes S_2]\!] = [\![S_1]\!] \ast [\![S_2]\!] \\ &= \theta([S_1]) \ast \theta([S_2]) \end{aligned}$$

O que vimos acima pode agora ser sintetizado no seguinte teorema:

Teorema 4.11: *A aplicação* $\theta : T(G,R) \to Pic(RG)$, *dada por*

$$\theta([S]) = [\![S]\!]\ ,$$

é um homomorfismo de grupos abelianos.

Referências

[1] S. Chase, D.K. Harrison, A. Rosenberg; Galois theory and Galois cohomology of commutative rings, Memoirs AMS, **52** (1965), 15-33.

[2] G. Garfinkel, M. Orzech; Galois extensions as modules over the group ring, Canadian J. Math., **22** (1970), 242-248.

[3] D.K. Harrison; Abelian extensions of commutative rings, Memoirs AMS, **52** (1965), 1-14.

[4] B.R. MacDonald. Linear Algebra over Commutative Rings. Marcel Dekker Inc., 1984.

5 Teoria de Kummer

Dados um anel comutativo R e um grupo abeliano finito G, o Teorema 4.12 nos assegura a existência de homomorfismo de grupos

$$\begin{aligned} \theta \ : \ & T(G,R) \ \to \ \mathrm{Pic}(RG) \ , \\ & [S] \ \mapsto \ \mathbf{[}S\mathbf{]}, \ \text{para todo} \ \ [S] \in T(G,R) \ . \end{aligned}$$

Notemos que $\ker\theta$ é formado pelos classe $[S]$ das extensões abelianas S de R, com grupo de Galois G, que possuem base normal. Denotaremos esse subgrupo $\ker\theta$ por $\mathrm{NB}(G,R)$. Assim temos a seguinte sequência exata de grupos abelianos

$$1 \ \to \ \mathrm{NB}(G,R) \ \xrightarrow{i} \ T(G,R) \ \xrightarrow{\theta} \ \mathrm{Pic}(RG) \ .$$

onde i denota a inclusão canônica.

Observemos que se $\mathrm{Pic}(RG) = 1$ então $T(G,R) = \mathrm{NB}(G,R)$. Isto ocorre, por exemplo, se R é corpo (ver Corolário 4.10 ou 4.11).

A sequência exata acima sugere-nos um caminho para o estudo do grupo $T(G,R)$, isto é, uma forma de descrever tal grupo através dos grupos $\mathrm{NB}(G,R)$ e $\theta(T(G,R))$. Isto é o que faremos nesta seção para anéis R verificando certas condições específicas, próprias de uma teoria de Kummer. Recordemos que a construção do grupo $T(G,R)$ nos dá um funtor $T(-,R)$ da categoria dos grupos abelianos finitos na categoria dos grupos abelianos, o qual é aditivo (ver seção 3). Consequentemente, graças ao Teorema Fundamental para grupos abelianos finitos, podemos restringir nosso estudo ao caso em que G é um grupo cíclico.

No que se seguirá G denotará sempre um grupo ciclíco de ordem $n \geq 2$ e R um anel comutativo com identidade, verificando a seguinte condição:

(K): "Existe um elemento $\omega \in R^*$ tal que $\omega^n = 1$ e $1 - \omega^i \in R^*$, para todo $i = 1, \cdots, n-1$."

onde R^* denota o grupo multiplicativo das unidades de R.

Notemos que, se R satisfaz a condição (K), então podemos obter facilmente $\mathsf{x}^n - 1 = \prod_{1 \le i \le n-1}(\mathsf{x} - \omega^i)$ em $R[\mathsf{x}]$ de onde resulta que

$$\sum_{0 \le i \le n-1} \omega^i = 0 \quad \text{e} \quad n = \prod_{i \neq 0}(1 - \omega^i) \in R^* .$$

Esta seção se divide em três partes, nas quais iremos mostrar que

$$\mathrm{NB}(G,R) \simeq \frac{R^*}{(R^*)^n} ,$$

$$\theta(T(G,R)) \simeq \mathrm{Pic}_n(R) = \text{ o subgrupo de expoente } n \text{ de } \mathrm{Pic}(R) \text{ e}$$

$$T(G,R) \simeq \mathrm{NB}(G,R) \oplus \mathrm{Pic}_n(R) .$$

Para tanto, necessitamos de alguns resultados preliminares.

Denotemos por Ω o subgrupo cíclico de R^* gerado por ω. Seja $\hat{G} = \mathrm{Hom}(G, \Omega)$ o grupo de caracteres de G com a multiplicação usual. Evidentemente $\hat{G}$ é um grupo naturalmente isomorfo a G. Sejam $\sigma \in G$ e $\chi \in \hat{G}$ os geradores de G e $\hat{G}$ respectivamente. Escolhamos χ tal que $\chi(\sigma) = \omega$. Observemos que

$$\sum_{0 \le j \le n-1} \chi^i(\sigma^j) = \sum_{0 \le j \le n-1} \chi^{ij}(\sigma) = \sum_{0 \le j \le n-1} \omega^{ij} = \begin{cases} 0 & \text{se } i \neq 0 \\ n & \text{se } i = 0 \end{cases}$$

para todo $0 \le i \le n-1$. De fato, se $i = 0$ o resultado é óbvio. Suponhamos $0 < i \le n-1$. Neste caso,

$$\omega^i \sum_{0 \le j \le n-1} \omega^{ij} = \sum_{0 \le j \le n-1} \omega^{i(j+1)} = \sum_{0 \le j \le n-1} \omega^{ij} ,$$

donde segue que $(1 - \omega^i) \sum_{0 \le j \le n-1} \omega^{ij} = 0$ e consequentemente

$$\sum_{0 \le j \le n-1} \omega^{ij} = 0 .$$

Para cada $i = 0, \cdots, n-1$ consideremos o elemento $v_i \in RG$ dado por

$$v_i = \frac{1}{n} \sum_{0 \leq j \leq n-1} \chi^{-i}(\sigma^j)\, \sigma^j \ .$$

Estes elementos são ortogonais dois a dois e têm soma 1. De fato,

$$\begin{aligned} \sum_{0 \leq i \leq n-1} v_i &= \frac{1}{n} \sum_i \sum_j \chi^{-i}(\sigma^j)\sigma^j = \frac{1}{n} \sum_i \left(\sum_j \chi^{-ij}(\sigma) \right) \sigma^j \\ &= \frac{1}{n} \left(\sum_i \chi^0(\sigma) \right) \sigma^0 = \sigma^0 = 1 \ \text{ e} \end{aligned}$$

$$\begin{aligned} v_i v_j = v_j v_i &= \left(\frac{1}{n} \sum_l \chi^{-j}(\sigma^l)\sigma^l \right) \left(\frac{1}{n} \sum_k \chi^{-i}(\sigma^k)\sigma^k \right) \\ &= \left(\frac{1}{n} \sum_l \chi^{-j}(\sigma^l) \right) \left(\frac{1}{n} \sum_k \chi^{-i}(\sigma^k)\sigma^{l+k} \right) \\ &= \left(\frac{1}{n} \sum_l \chi^{-j}(\sigma^l) \right) \left(\frac{1}{n} \sum_t \chi^{-i}(\sigma^{t-l})\sigma^t \right) \\ &= \left(\frac{1}{n} \sum_l \chi^{-j}(\sigma^l)\chi^i(\sigma^l) \right) \left(\frac{1}{n} \sum_t \chi^{-i}(\sigma^t)\sigma^t \right) \\ &= \left(\frac{1}{n} \sum_l \chi^{(i-j)}(\sigma^l) \right) v_i = \begin{cases} v_i & \text{se } i = j \ , \\ 0 & \text{se } i \neq j \ . \end{cases} \end{aligned}$$

Portanto, $RG = \oplus_{0 \leq i \leq n-1} Rv_i$ e $Rv_i \simeq R$ como anéis, para todo $0 \leq i \leq n-1$. Disto decorre então que $\mathrm{Pic}(RG) \simeq \mathrm{Pic}(R^n) \simeq (\mathrm{Pic}(R))^n$ como grupos abelianos.

Seja agora S uma extensão abeliana de R com grupo de Galois G. Então S é um RG-módulo projetivo de posto 1 (cf. Teorema 4.9) e

$$S = RG.S = \oplus_{0 \leq i \leq n-1} v_i S = \oplus_{0 \leq i \leq n-1} P_{\chi^i}$$

como R-módulos, onde $P_{\chi^i} = v_i S = \{ \frac{1}{n} \sum_{0 \leq k \leq n-1} \chi^{-i}(\sigma^k)\sigma^k(s); s \in S \}$.

Usando localização e o Teorema 2.2.a, podemos ver facilmente que S é um R-módulo projetivo de posto $n = |G|$ e, consequentemente, P_{χ^i} é um R-módulo projetivo de posto 1. Portanto $[P_{\chi^i}] \in \mathrm{Pic}(R)$, para todo $0 \leq i \leq n-1$. Também pode ser visto facilmente que

$$P_{\chi^i} = \{s \in S; \sigma(s) = \chi^i(\sigma)s\} \ .$$

Além disso, $P_{\chi^i}P_{\chi^j} = P_{\chi^{i+j}}$, $0 \leq i,j \leq n-1$. De fato, se $s \in P_{\chi^i}P_{\chi^j}$ então $s = \sum_k s_k t_k$, com $s_k \in P_{\chi^i}$ e $t_k \in P_{\chi^j}$ e

$$\sigma(s) = \sum_k \sigma(s_k)\sigma(t_k) = \sum_k \chi^i(\sigma)s_k\chi^j(\sigma)t_k = \chi^{i+j}(\sigma)s \ .$$

Reciprocamente, se $s \in P_{\chi^{i+j}}$ então $\sigma(s) = \chi^{i+j}(\sigma)s$, donde segue que $\sigma^k(s) = \chi^{i+j}(\sigma^k)s$ e consequentemente

$$s = \frac{1}{n} \sum_{0 \leq k \leq n-1} \chi^{-(i+j)}(\sigma^k)\sigma^k(s) \ .$$

Agora, como S é extensão galoisiana de R, com grupo de Galois G, pelo Teorema 2.2.c existem $x_l, y_l \in S$, $1 \leq l \leq m$, tais que

$$\sum_l x_l\sigma^t(y_l) = \delta_{0,t} \ .$$

Então

$$s = \sum_{l,t} x_l\sigma^t(y_l)\sigma^t(s)\chi^{-j}(\sigma^t) \ \text{ e,}$$

portanto,

$$\begin{aligned} s &= \frac{1}{n}\sum_k \chi^{-(i+j)}(\sigma^k)\sigma^k(s) \\ &= \frac{1}{n}\sum_k \chi^{-(i+j)}(\sigma^k)\sigma^k\left(\sum_{l,t} x_l\sigma^t(y_l)\sigma^t(s)\chi^{-j}(\sigma^t)\right) \\ &= \frac{1}{n}\sum_{k,l,t} \chi^{-(i+j)}(\sigma^k)\sigma^k(x_l)\sigma^{k+t}(y_l)\sigma^{k+t}(s)\chi^{-j}(\sigma^t) \\ &= \sum_l \left(\frac{1}{n}\sum_k \chi^{-i}(\sigma^k)\sigma^k(x_l)\right)\left(\frac{1}{n}\sum_{k+t} \chi^{-j}(\sigma^{k+t})\sigma^{k+t}(nsy_l)\right) \ \in P_{\chi^i}P_{\chi^j} \ . \end{aligned}$$

Disto resulta que $P_{\chi^i} = P_\chi^i$ e portanto $P_\chi^n = P_{\chi^n} = \{s \in S; \sigma(s) = \chi^n(\sigma)s = s\} = S^G = R$.

No que se seguirá, o símbolo $\otimes$ denotará sempre o produto tensorial sobre R.

Consideremos agora

$$\mu : P_{\chi^i} \otimes P_{\chi^j} \to P_{\chi^{i+j}} = P_{\chi^i} P_{\chi^j}$$

a aplicação induzida pela multiplicação de S. É imediato que μ é um homomorfismo sobrejetor de R-módulos e desde que $P_{\chi^i} \otimes P_{\chi^j}$ e $P_{\chi^{i+j}}$ são R-módulos projetivos de posto 1, segue-se, por localização, que μ é um isomorfismo (ver Corolário 4.5). Portanto $P_{\chi^i} \otimes P_{\chi^j} \simeq P_{\chi^{i+j}}$, $0 \leq i, j \leq n-1$, e por consequência existe um isomorfismo de R-módulos.

$$(P_\chi)^{\otimes^n} \simeq P_{\chi^n} = R \ , \quad \text{ou seja,} \quad [P_\chi] \in \mathrm{Pic}_n(R) \ ,$$

onde $(P_\chi)^{\otimes^i}$ denota o produto tensorial

$$\underbrace{P_\chi \otimes \cdots \otimes P_\chi}_{i \text{ vezes}} \ .$$

Portanto,

$$S \simeq \oplus_{0 \leq i \leq n-1} P_\chi^{\otimes^i} \simeq \oplus_{0 \leq i \leq n-1} P_\chi^i \ ,$$

com $P_\chi \in \mathrm{Pic}_n(R)$.

Suponhamos agora que S' seja um outro representante da classe $[S] \in T(G, R)$. Então existe um isomorfismo de R-álgebras $h : S \to S'$ tal que $h\sigma = \sigma h$. Sejam $f = h|_{P_\chi}$ e

$$P'_\chi = v_1 S' = \{\frac{1}{n} \sum_{0 \leq k \leq n-1} \chi^{-1}(\sigma^k)\sigma^k(s'); s' \in S'\} = \{s' \in S'; \sigma(s') = \chi(\sigma)s'\} \ .$$

Logo, para todo $s \in P_\chi$, temos $\sigma(f(s)) = \sigma(h(s)) = h(\sigma(s)) = h(\chi(\sigma)s) = \chi(\sigma)h(s) = \chi(\sigma)f(s)$ e portanto $f(P_\chi) \subset P'_\chi$. Reciprocamente, para todo

$s' \in P'_\chi$, existe $s \in S$ tal que $s' = h(s)$ e de $\sigma(s') = \chi(\sigma)s'$ resulta que $h(\sigma(s)) = \sigma h(s) = \sigma(s') = \chi(\sigma)s' = \chi(\sigma)h(s) = h(\chi(\sigma)s)$ donde segue que $\sigma(s) = \chi(\sigma)s$, pois h é injetor. Portanto $f = h|_{P_\chi} : P_\chi \to P'_\chi$ é um isomorfismo de R-módulos. Isto mostra que se $[S] = [S']$ em $T(G,R)$ então $[P_S] = [P_{S'}]$ em $\mathrm{Pic}_n(R)$ onde $P_S = v_1 S$ e $P_{S'} = v_1 S'$.

Finalmente, dados $[S_1]$, $[S_2] \in T(G,R)$,

$$S_1 = \oplus_{0 \le i \le n-1} P_{S_1}^i \quad \text{e} \quad S_2 = \oplus_{0 \le j \le n-1} P_{S_2}^j \ ,$$

temos $S_1 \otimes S_2 = \oplus_{i,j} P_{S_1}^i \otimes P_{S_2}^j$. Seja $T = (S_1 \otimes S_2)^{\delta G}$. Um elemento $s \in S_1 \otimes S_2$, $s = \sum_{i,j} s_{1i} \otimes s_{2j}$ com $s_{1i} \in P_{S_1}^i$ e $s_{2j} \in P_{S_2}^j$, pertence a T se, e somente se, $(\sigma^{-1}, \sigma)(s) = s$ ou, equivalentemente, $(\sigma^{-1}, \sigma)(s_{1i} \otimes s_{2j}) = s_{1i} \otimes s_{2j}$, $0 \le i, j \le n-1$. Mas

$$\begin{aligned} (\sigma^{-1}, \sigma)(s_{1i} \otimes s_{2j}) &= \chi^{-i}(\sigma)s_{1i} \otimes \chi^j(\sigma)s_{2j} \\ &= \chi^{(j-i)}(\sigma)s_{1i} \otimes s_{2j} = \omega^{j-i} s_{1i} \otimes s_{2j} \ . \end{aligned}$$

Logo, $(\sigma^{-1}, \sigma)(s_{1i} \otimes s_{2j}) = s_{1i} \otimes s_{2j}$, se, e somente se, $\omega^{j-i} s_{1i} \otimes s_{2j} = s_{1i} \otimes s_{2j}$ se, e somente se, $(\omega^{j-i} - 1)s_{1i} \otimes s_{2j} = 0$, donde decorre, por localização, que

$$(\sigma^{-1}, \sigma)(s_{1i} \otimes s_{2j}) = s_{1i} \otimes s_{2j}$$

se, e somente se, $i = j$. Portanto $s \in T = (S_1 \otimes S_2)^{\delta G}$ se, e somente se,

$$s = \sum_{0 \le i \le n-1} s_{1i} \otimes s_{2i} \ \in \oplus_{0 \le i \le n-1} P_{S_1}^i \otimes P_{S_2}^i \ ,$$

o que mostra que

$$(S_1 \otimes S_2)^{\delta G} = \oplus_{1 \le i \le n-1} P_{S_1}^i \otimes P_{S_2}^i \simeq \oplus_{1 \le i \le n-1} (P_{S_1} \otimes P_{S_2})^i \ .$$

O que vimos acima mostra que existe, de fato, um homomorfismo de grupos abelianos $\tilde{\theta} : T(G,R) \to \mathrm{Pic}_n(R)$ dado por $\tilde{\theta}([S]) = [P_S] = [v_1 S]$. Notemos também que esse homomorfismo depende do caractere χ escolhido.

Vejamos agora como esse homomorfismo $\tilde{\theta}$ se relaciona com o homomorfismo θ considerado no início desta seção.

Observemos que a decomposição $RG = \oplus_{0\leq i\leq n-1} Rv_i$, com $Rv_i \simeq R$, vista inicialmente, acarreta a decomposição $P = RG.P = \oplus_{0\leq i\leq n-1} v_i P$, para todo $[P] \in \mathrm{Pic}[RG]$, $0 \leq i \leq n-1$. Desde que RG é um R-módulo livre de dimensão $n = |G|$, também pode ser visto, por localização, que $[v_i P] \in \mathrm{Pic}(R)$, $0 \leq i \leq n-1$. Isto induz um isomorfismo de grupos abelianos

$$\begin{aligned} \mathrm{Pic}(RG) &\overset{\psi}{\tilde{\to}} (\mathrm{Pic}(R))^n \,, \\ [P] &\mapsto ([v_i P])_{0\leq i\leq n-1} \,. \end{aligned}$$

Considerando ainda a projeção canônica dada por

$$\begin{aligned} \pi_1 \;:\; (\mathrm{Pic}(R))^n &\to \mathrm{Pic}(R) \,, \\ ([P_i])_{1\leq i\leq n-1} &\mapsto [P_1] \,, \end{aligned}$$

obtemos a seguinte sequência de grupos abelianos

$$T(G,R) \xrightarrow{\theta} \mathrm{Pic}(RG) \overset{\psi}{\tilde{\to}} (\mathrm{Pic}(R))^n \xrightarrow{\pi_1} \mathrm{Pic}(R) \,.$$

A composição desses homomorfismos nos dá o homomorfismo $\tilde{\theta}$. Ainda mais, $\tilde{\theta}(T(G,R)) \subset \mathrm{Pic}_n(R)$. Notemos também que

$$\psi\theta([S]) = ([P_S^i])_{0\leq i\leq n-1} = ([P_S^{\otimes i}])_{0\leq i\leq n-1}$$

em $(\mathrm{Pic}(R))^n$ e que portanto a restrição de π_1 a $\psi\theta(T(G,R))$ é injetiva. Disto segue facilmente que $\ker\tilde{\theta} = \ker\theta = \mathrm{NB}(G,R)$ e que $\theta(T(G,R)) \simeq \tilde{\theta}(T(G,R))$.

Assim obtivemos uma nova sequência exata de grupos abelianos, mais precisa que aquela considerada inicialmente. Esta sequência é a seguinte:

$$1 \to \mathrm{NB}(G,R) \xrightarrow{i} T(G,R) \xrightarrow{\tilde{\theta}} \mathrm{Pic}_n(R) \,.$$

Teorema 5.1:

$$NB(G,R) \xrightarrow{\sim} \frac{R^*}{(R^*)^n} .$$

Demonstração:

Seja $[S] \in \mathrm{NB}(G,R) = \ker \hat{\theta}$. Então $P_S \simeq R$, como R-módulos, e portanto existe $x \in P_S$ livre sobre R e tal que $P_S = Rx$. Além disso, $Rx^n = P_S^n = R$ e por conseguinte existe $\lambda \in R$ tal que $\lambda x^n = 1$. Como $\sigma(x^n) = \sigma(x)^n = (\omega x)^n = \omega^n x^n$, então $x^n \in R$. Disto segue que $x^n = u_s$ para algum $u_s \in R^*$ e consequentemente $x \in S^*$. Suponhamos agora que S' seja outro representante da classe $[S]$. Então, da forma como vimos acima $P_{S'} = Rx'$, para algum $x' \in S'^*$, com $x'^n = u_{S'} \in R^*$. Como $[S] = [S']$, existe um homomorfismo de R-álgebras $h : S \to S'$ tal que $h\sigma = \sigma h$. Pode-se ver facilmente que $h(P_S) = P_{S'}$ e portanto $f = h|_{P_S} : P_S \to P_{S'}$ é um isomorfismo de R-módulos. Se $f(x) = \lambda x'$ então $\lambda \in R^*$ e $\lambda^n u_{S'} = \lambda^n x'^n = (\lambda x')^n = f(x)^n = h(x)^n = h(x^n) = h(u_S) = u_S$. Disto segue que $[u_S] = [u_{S'}]$ em $R^*/(R^*)^n$, onde

$$(R^*)^n = \{u^n; u \in R^*\} .$$

Portanto temos uma aplicação (bem definida) $\varphi : \ker \hat{\theta} \to R^*/(R^*)^n$. Dados $[S_i] \in \ker \hat{\theta}$, com $P_{S_i} = Rx_i$ e $x_i^n = u_{S_i} \in R^*$, $i = 1,2$, se $T = (S_1 \otimes S_2)^{\delta G}$ então

$$P_T = P_{S_1} \otimes P_{S_2} = Rx_1 \otimes Rx_2 = Rx_1 \otimes x_2 \text{ e } (x_1 \otimes x_2)^n = u_{S_1} u_{S_2} .$$

Portanto $\varphi([S_1] * [S_2]) = [u_{S_1}][u_{S_2}] = \varphi([S_1])\varphi([S_2])$, o que mostra que φ é um homomorfismo de grupos abelianos.

Se $[S] \in \ker\varphi$ e $P_S = Rx$ então existe $\lambda \in R^*$ tal que $x^n = \lambda^n$. Isto nos permite definir um homomorfismo de R-álgebras $\beta : S \to R$, dado por

$$\beta\left(\sum_{0\leq i\leq n-1} r_i x^i\right) = \sum_{0\leq i\leq n-1} r_i\lambda^i \text{ (notemos que } S = \oplus_{0\leq i\leq n-1} Rx^i) \ .$$

Seja agora $\gamma : S \to E_G(R)$ a aplicação dada por

$$\gamma(s) = \sum_{0\leq i\leq n-1} \beta(\sigma^{-i}(s))e_{\sigma^i} \ ,$$

onde $E_G(R) = \oplus_{0\leq i\leq n-1} Re_{\sigma^i}$ representa o elemento neutro de $T(G,R)$ (ver seção 3). É fácil ver que a aplicação γ é um homomorfismo de R-álgebras que verifica $\gamma\sigma = \sigma\gamma$. Portanto, pela Proposição 3.3., $[S] = [E_G(R)]$. Isto mostra que φ é injetor.

Seja $[u] \in R^*/(R^*)^n$ e consideremos a R-álgebra $S = R[\mathsf{x}]/(\mathsf{x}^n - u) = R[x] = \oplus_{0\leq i\leq n-1} Rx^i$, onde $x = \mathsf{x} + (\mathsf{x}^n - u)$. Sobre S definimos a ação de G dada por $\sigma(x^i) = \omega^i x^i$, $0 \leq i \leq n-1$. Agora, se $s \in S^G$ então $s = \sum_i r_i x^i$ e $\sigma(s) = s$, o que implica $\sum_i r_i x^i = \sum_i r_i\omega^i x^i$ e consequentemente, $r_i = \omega^i r_i$, $0 \leq i \leq n-1$. Desde que $(1-\omega^i) \in R^*$, obtemos $r_i = 0$, $1 \leq i \leq n-1$ e $s = r_0 \in R$. Logo $S^G = R$. Além disso, $\sigma^i(x) - x = (\omega^i - 1)x \in S^*$, $1 \leq i \leq n-1$. Pelo Teorema 2.2.d, S é uma extensão abeliana de R com grupo de Galois G. Por construção, $[S] \in \ker\tilde{\theta} = \mathrm{NB}(G,R)$ e $\varphi([S]) = [u]$, o que mostra que φ é sobrejetor. Portanto

$$\varphi \ : \ \mathrm{NB}(G,R) = \ker\tilde{\theta} \ \longrightarrow \ R^*/(R^*)^n$$

é um isomorfismo. ■

Teorema 5.2:

$$\theta(T(G,R)) \simeq Pic_n(R) \ .$$

Demonstração:

Desde que $\theta(T(G,R)) \simeq \tilde{\theta}(T(G,R))$ é suficiente verificarmos que

$$\tilde{\theta}(T(G,R)) = \mathrm{Pic}_n(R) \ .$$

Para mostrar que $\tilde{\theta}$ é sobrejetor procederemos de forma análoga ao que vimos acima na demonstração de que φ é sobrejetor. Para cada $[P] \in \mathrm{Pic}_n(R)$ consideremos o R-módulo $S_P = \oplus_{0 \leq i \leq n-1} P^{\otimes^i}$. Sobre esse módulo S_P definimos a multiplicação seguinte (é suficiente defini-la sobre os elementos homogêneos de S):

$$(s_1 \otimes \cdots \otimes s_i)(t_1 \otimes \cdots \otimes t_j) =$$
$$\begin{cases} s_1 \otimes \cdots \otimes s_i \otimes t_1 \otimes \cdots \otimes t_j & \text{se } i+j < n \\ \nu(s_1 \otimes \cdots \otimes s_i \otimes t_1 \otimes \cdots \otimes t_j) & \text{se } i+j = n \\ \nu(s_1 \otimes \cdots \otimes s_i \otimes t_1 \otimes \cdots \otimes t_n) t_{n+1} \otimes \cdots \otimes t_j & \text{se } i+j > n \end{cases}$$

onde $\nu : P^{\otimes^n} \xrightarrow{\sim} R$ é o isomorfismo de R-módulos dado (notemos que $[P] \in \mathrm{Pic}_n(R)$). Pode ser visto facilmente, via localização, que esta multiplicação define sobre S_P uma estrutura de R-álgebra associativa e comutativa, com elemento identidade. Observemos que localmente S_P é exatamente a R-álgebra $R[\mathsf{x}]/(\mathsf{x}^n - \nu(\mathsf{x}^n))$, onde $P = Rx$, construída na demonstração do teorema acima. Efetivamente S_P é o quociente da R-álgebra tensorial $T(P) = \oplus_{i \geq 0} P^{\otimes^i}$ pelo ideal gerado pelos elementos da forma $s - \nu(s)$, $s \in P^{\otimes^n}$. Notemos que essa estrutura de R-álgebras sobre S_P depende do R-módulo P e do isomorfismo $\nu : P^{\otimes^n} \to R$.

Definimos a ação de G sobre S_P dada por $\sigma(x_i) = \omega^i x_i$, para todo $x_i \in P^{\otimes^i}$, $0 \leq i \leq n-1$. Desde que $(1 - \omega^i) \in R^*$, pode ser visto facilmente que $S_P^G = R$. Além disso, se supomos que existem $1 \leq i \leq n-1$ e um

ideal maximal m de S_P tais que $\sigma^i(s) - s \in m$, para todo $s \in S_P$, então $\sigma^i(s) - s \in m$, para todo $s \in P$, ou seja,

$$(\omega^i - 1)s \in m \ , \quad \text{para todo} \ \ s \in P \ ,$$

o que acarreta $s \in m$, para todo $s \in P$. Neste caso, temos $R = \nu(P^{\otimes^n}) = P^n \subset m$ o que é um absurdo. Portanto, pela Teorema 2.2.d, S_P é um extensão abeliana de R, com grupo de Galois G, ou seja, $[S_P] \in T(G,R)$. Por construção, $\tilde{\theta}([S_P]) = [P]$. ■

Teorema 5.3:

$$T(G,R) \simeq NB(G,R) \oplus Pic_n(R) \ .$$

Demonstração:

Do que vimos no teorema acima a sequência de grupos abelianos

$$1 \ \rightarrow \ \mathrm{NB}(G,R) \ \xrightarrow{i} \ T(G,R) \ \xrightarrow{\tilde{\theta}} \ \mathrm{Pic}_n(R) \ \rightarrow \ 1$$

é exata. Logo para demonstrarmos este teorema é suficiente mostrarmos que essa sequência cinde. Observemos que $\mathrm{Pic}_n(R)$ pode ser decomposto em um produto direto de grupos cíclicos, isto é, $\mathrm{Pic}_n(R) = \prod_{\lambda \in \Lambda} \langle [P_\lambda] \rangle$. Para cada $\lambda \in \Lambda$, fixamos o R-módulo P_λ e um isomorfismo de R-módulos

$$f_\lambda \ : \ P_\lambda^{\otimes m_\lambda} \ \rightarrow \ R \ (m_\lambda = \mathcal{O}([P_\lambda]), \ m_\lambda d_\lambda = n) \ .$$

Denotemos $\nu_\lambda = f_\lambda^{d_\lambda} : P_\lambda^{\otimes^n} \rightarrow R$. Então cada elemento $[P]$ define um R-módulo fixo $P = \prod_{\lambda \in \Lambda} P_\lambda^{\otimes^{l_\lambda}}$ e um isomorfismo

$$\nu \ : \ \prod_{\lambda \in \Lambda} \nu_\lambda^{l_\lambda} \ : \ P^{\otimes^n} \ \rightarrow \ R$$

$(0 \leq l_\lambda < m_\lambda$ e $l_\lambda = 0$, exceto para um número finito de $\lambda \in \Lambda)$. Associamos ao elemento $[P]$ a classe $[S_P] \in T(G,R)$ representada pela extensão abeliana S_P conforme construída na demonstração do Teorema 5.2. Desta forma temos definido uma aplicação $\theta' : \mathrm{Pic}_n(R) \to T(G,R)$ que obviamente verifica $\tilde{\theta} \circ \theta' = \mathrm{id}$. Pode ser visto facilmente que θ' é um homomorfismo de grupos, o que conclui a demonstração. ■

Referências

[1] A.Z. Borevich; Kummer extensions of rings, J. Soviet Math. **11** (1979), 514-534.

[2] S. Chase, D.K. Harrison, A. Rosenberg; Galois theory and Galois cohomology of commutative rings, Memoirs AMS, **52** (1965), 15-33.

[3] L. Childs; Abelian Galois extension of rings containing roots of unity, Illinois J. Math. **15** (1971), 273-280.

[4] D.K. Harrison; Abelian extensions of commutative rings, Memoirs AMS, **52** (1965), 1-14.