Universidade Estadual de Campinas

Instituto de Matemática, Estatística
e Computação Científica

Sobre as extensões cíclicas de grau p de um anel comutativo

Tese de Doutorado em Matemática

por

Alvino Alves Sant'Ana

Antonio Paques
orientador

Agosto de 2004

Sobre extensões cíclicas de grau p de um anel comutativo

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Alvino Alves Sant'Ana** e aprovada pela comissão julgadora.

Campinas, 24 de agosto de 2004.

Prof. Dr. Antonio Paques
Orientador

Banca Examinadora

Prof. Dr. Antonio Paques

Prof. Dr. Antonio José Engler

Prof. Dr. Flávio Ulhoa Coelho

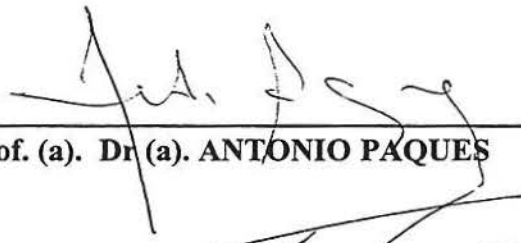
Prof. Dr. Miguel Angel Alberto Ferrero

Prof. Dr. Vitor de Oliveira Ferreira

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de DOUTOR em Matemática.

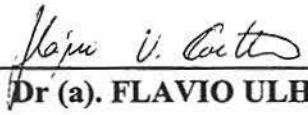
Tese de Doutorado defendida em 13 de agosto de 2004 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

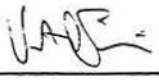


Prof. (a). Dr (a). ANTONIO PAQUES

Prof. (a). Dr (a). MIGUEL ANGEL ALBERTO FERRERO



Prof. (a). Dr (a). FLAVIO ULHOA COELHO



Prof. (a). Dr (a). VITOR DE OLIVEIRA FERREIRA

Prof. (a) Dr. (a) ANTONIO JOSÉ ENGLER

Dedico este trabalho à Marilaine, ao Victor e à Júlia

AGRADECIMENTOS:

Ao professor Paques, pela atenção e paciência, pelos conselhos, pela sua amizade, bagagem matemática e por nossas conversas.

Aos demais professores do IMECC com quem convivi e estudei, em especial, aos professores Brumati e Engler.

À Cidinha e ao Ednaldo pela competência e amizade.

Ao DMPA/UFRGS, que permitiu o afastamento integral de minhas atividades junto à Universidade e, em especial, aos amigos e colegas Ada, Alveri, Beth, Claus, Éder, Eduardo, Fernanda, Liana, Luísa, Media, Miguel e Vânia.

Aos colegas do Predinho, pelos momentos de estudo, concentração e cooperação e também pelos momentos descontraídos que tornavam nosso ambiente mais leve. Em especial ao Sinval, Oscar, João, Serginho, Bahiano, Lu, Elis, Érica, Ximena, Marcela, Claudinha, Denilson, Iara, Ryuichi, Zé e Leo.

Ao Nelson e Ângela, pela amizade e acolhida.

À Rosa e sua família que é a minha família em Campinas.

À Turma do Patê, pela amizade, pelo apoio e pelas agradáveis conversas entre copos de vinho.

Aos meus pais (in memorian) e meus sogros Zé e Zu.

Finalmente, quero agradecer à minha esposa Mari, ao meu grande Victor e à minha pequena Júlia, pelo amor, pelo incentivo, pela cumplicidade e pela compreensão com minhas ausências.

RESUMO

O objetivo da tese é descrever o grupo de Harrison $T(G;R)$ para o caso em que G é um grupo cíclico de ordem prima ímpar p e R é um anel (comutativo com unidade) que não possui raiz p-ésima da unidade, exigindo-se apenas que p seja regular em R.

Para isso, precisamos considerar o anel $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle} = R[\varepsilon]$, onde $\Phi_p(X)$ é o p-ésimo polinômio ciclotômico em $R[X]$ e $\varepsilon = X + \langle \Phi_p(X) \rangle$ é uma raiz p-ésima primitiva da unidade em S, e a seqüência exata de L. Childs $1 \longrightarrow H(G;S) \longrightarrow T(G;S) \longrightarrow P(S;G) \longrightarrow 1$, onde $H(S;G)$ é o subgrupo de $T(G;S)$ formado pelas classes de isomorfismos das extensões abelianas de S com grupo de Galois G que possuem S-base normal, e $P(S;G)$ é o co-núcleo da inclusão $H(G;S) \hookrightarrow T(G;S)$.

Denotando $\Gamma = \{\gamma_{\bar{i}} \mid \bar{i} \in \mathcal{U}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)\}$, o subgrupo dos R-automorfismos de S dados por $\gamma_{\bar{i}}(\varepsilon) = \varepsilon^i$, definimos uma ação de Γ sobre a seqüência de L. Childs. A seguir, mostramos que a seqüência dos subgrupos estáveis por esta ação também é exata. Além disso, cada grupo estável por Γ é isomorfo ao correspondente grupo obtido pela "descida" de S ao anel R, ou seja, a seqüência abaixo é exata:

$$1 \longrightarrow H(G;R) \longrightarrow T(G;R) \longrightarrow P(G;R) \longrightarrow 1$$

A ação citada acima coincide com a $*$-ação de C. Greither e R. Miranda sobre a seqüência exata de Kummer quando p for invertível em R. Assim, estendemos o resultado de C. Greither e R. Miranda para p regular em R. Também descrevemos $P(G;R)$ como o grupo dos elementos primitivos de p-torsão do grupo de Picard $Pic(R[G])$.

Concluímos este trabalho com uma aplicação ao caso cúbico, descrevendo o grupo $H\left(\frac{\mathbb{Z}}{3\mathbb{Z}};R\right)$ independente da ação de Γ.

ABSTRACT

The objective of the thesis is to describe the Harrison group $T(G;R)$ in the case G is a cyclic group of prime odd order p and R is a ring (commutative with identity) without a primitive p^{th} root of unity, assuming only that p is regular in R.

For this purpose we need consider the ring $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle} = R[\varepsilon]$, where $\Phi_p(X)$ is the p^{th} cyclotomic polynomial in $R[X]$ and $\varepsilon = X + \langle \Phi_p(X) \rangle$ is a primitive p^{th} root of unity in S, and the exact sequence of L. Childs $1 \longrightarrow H(G;S) \longrightarrow T(G;S) \longrightarrow P(S;G) \longrightarrow 1$, where $H(G;S)$ is the subgroup of $T(G;S)$ whose elements are the isomorphism classes of the abelian extensions of S with Galois group G having normal S-base, and $P(S;G)$ is the cokernel of the inclusion $H(G;S) \hookrightarrow T(G;S)$.

Denoting by $\Gamma = \{\gamma_i \mid \overline{i} \in \mathcal{U}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)\}$, the subgroup of the R-automorphisms of S defined by $\gamma_i(\varepsilon) = \varepsilon^i$, we define an action on the L. Childs' sequence. We then show that the sequence of the subgroups stable under this action is also exact. In addition, each subgroup stable under Γ is isomorphic to the corresponding group obtained by "descent" from S to the ring R, so that the sequence below is exact:

$$1 \longrightarrow H(G;R) \longrightarrow T(G;R) \longrightarrow P(G;R) \longrightarrow 1$$

The above mentioned action coincides with the $*$-action of C. Greither and R. Miranda on Kummer's sequence when p is invertible in R. In this way we extend the result of C. Greither and R. Miranda to the case in which p is regular in R. We also describe $P(G;R)$ as the group of primitive p-torsion elements of the Picard's group $Pic(R[G])$.

We finish this work with an application to the cubic case, and present a description of the $H\left(\frac{\mathbb{Z}}{3\mathbb{Z}};R\right)$ that does not depend on the action of Γ.

Índice

Introdução

Em todo este trabalho R denotará sempre um anel associativo, comutativo e com elemento identidade $1 \in R$. Uma álgebra sobre R será sempre associativa, comutativa com elemento identidade, e os morfismos de anéis preservarão a identidade. O grupo aditivo (resp. multiplicativo das unidades) de R será denotado por R^+ (resp. $\mathcal{U}(R)$), e denotaremos por $R^\times$ o conjunto dos elementos regulares de R, isto é, $R^\times = \{r \in R \mid r \text{ não é divisor de zero em } R\}$.

Em 1965, S. U. Chase, D. K. Harrison e A. Rosenberg [6] desenvolveram a teoria de Galois para anéis comutativos, a partir do trabalho de M. Auslander e O. Goldman sobre álgebras separáveis ([2] de 1960). Sejam A uma R-álgebra e G um subgrupo finito de R-automorfismos de A. Segundo estes autores, A é uma *extensão galoisiana (finita) de R com grupo de Galois G*, se:

- $R \subseteq A$ como subanel (isto é, $R \approx R \cdot 1 \subseteq A$, ou ainda, mais geralmente, A é uma R-álgebra fiel),
- $A^G = \{a \in A \mid \sigma(a) = a, \sigma \in G\} = R$,
- para cada $id \neq \sigma \in G$ e para cada ideal maximal $\mathfrak{M}$ de A, existe $a \in A$ tal que $\Big(\sigma(a) - a\Big) \notin \mathfrak{M}$.

Dizemos que A é uma *extensão abeliana* (resp. *extensão cíclica*) de R, se o grupo G é abeliano (resp. cíclico).

Observemos que toda extensão galoisiana de R com grupo de Galois G é, como R-módulo, projetivo finitamente gerado de posto constante igual à ordem de G [6], chamado de *grau da extensão.*

Sejam A e B duas extensões galoisianas de R, com mesmo grupo de Galois G. A e B são ditas *isomorfas* se existe um isomorfismo de R-álgebras $f : A \to B$ que comuta com a ação de G, ou seja, $f\sigma = \sigma f$, para qualquer $\sigma \in G$. Seja $T(G;R)$ o conjunto das classes de isomorfismos das extensões galoisianas de R com mesmo grupo de Galois G. Se G for abeliano, então $T(G;R)$ possui uma estrutura de grupo abeliano dado por

$$[A] * [B] = [(A \otimes_R B)^{\delta(G)}] \qquad \text{para quaisquer} \quad [A], [B] \in T(G;R)$$

onde $\delta(G) = \{(\sigma^{-1} \otimes \sigma) \mid \sigma \in G\}$ e $(A \otimes_R B)^{\delta(G)}$ é o subanel de $A \otimes_R B$ fixo pela ação (componente a componente) de $\delta(G)$ sobre $A \otimes_R B$. É claro que $(A \otimes_R B)^{\delta(G)}$ é uma extensão abeliana de R com grupo de Galois $\frac{G \otimes G}{\delta(G)}$, naturalmente isomorfo a G. A ação de G sobre $(A \otimes_R B)^{\delta(G)}$ é via primeira coordenada. O elemento neutro de $T(G;R)$ é $[e_G(R)]$, com $e_G(R) = \bigoplus_{\sigma \in G} Rv_\sigma$, onde $\{v_\sigma\}_{\sigma \in G}$ é uma família de idempotentes (dois a dois) ortogonais e de soma 1. A ação de G sobre $e_G(R)$ é induzida pelo produto de G, isto é, $\sigma(v_\tau) = v_{\sigma\tau}$, para quaisquer $\sigma, \tau \in G$. Para cada elemento $[A] \in T(G;R)$, o seu inverso $[A]^{-1}$ é representado pela própria extensão A, com a ação de G dada por $\sigma : a \mapsto \sigma^{-1}(a)$, $a \in A$ e $\sigma \in G$. $T(G;R)$ é chamado de grupo de Harrison de G sobre R.

Em 1968, D. K. Harrison [20], generalizou a teoria clássica de Kummer sobre extensões abelianas finitas de corpos contendo raízes da unidade para o contexto de anéis comutativos. Nesse trabalho, D. K. Harrison construiu formalmene o grupo $T(G;R)$. O principal resultado de [20], obtido para anéis conexos (anéis onde os únicos idempotentes são 0 e 1) é o seguinte:

" Seja R um anel conexo. 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 $T(\mathbb{Z}/n\mathbb{Z};R)$, $1 \leq n \in \mathbb{N}$.

No nosso contexto, de extensões abelianas (finitas) com mesmo grupo de Galois G, o resultado de D. K. Harrison pode ser reescrito na seguinte forma:

" Seja R um anel conexo. Então existe uma correspondência biunívoca entre as extensões abelianas de R com mesmo grupo de Galois G e os subgrupos finitos de $T(G;R)$".

Por exemplo, se $|G| = n$ (resp. $|G| = p$, p primo) e R é um corpo de característica zero que contém uma raiz n-ésima primitiva da unidade (resp. de característica p), então o grupo de Harrison $T(G;R)$ é isomorfo ao grupo quociente $\frac{\mathcal{U}(R)}{\mathcal{U}(R)^n}$ $\left(\text{resp. } \frac{R^+}{\{r-r^p \mid r\in R\}}\right)$. Este exemplo mostra que a teoria desenvolvida por D. K. Harrison não só estende as teorias clássicas (multiplicativa) de Kummer e (aditiva) de Artin-Schreier, como também as une numa única linguagem. Na realidade, D. K. Harrison queria desenvolver uma teoria da qual pudesse derivar todas as teorias até então conhecidas no estudo das extensões abelianas de um corpo. E ele obteve êxito com as

teorias clássicas de Kummer e de Artin-Schreier. Já naquela época, tinha-se consciência de uma sutil conexão entre a teoria de D. K. Harrison e a teoria de números algébricos. Essa conexão torna-se bem mais explícita, envolvendo inclusive as conjecturas de Leopoldt e Vandiver, com os trabalhos mais recentes de I. Kersten e J. Michaliček [24] e [25], ambos de 1989, e de C. Greither [16] de 1992. Mas é preciso destacar que o trabalho de D. K. Harrison dá um novo e importante enfoque para o estudo de extensões abelianas finitas de um corpo ou, mais geralmente, de um anel comutativo qualquer. Este novo enfoque oferece mais vantagens que a teoria clássica de corpos, destacando-se aqui as propriedades funtoriais do grupo $T(G;R)$, já que o grupo de Harrison $T(G;R)$ é um bifuntor covariante nos dois fatores e aditivo no primeiro [20].

Toda extensão galoisiana de R com grupo de Galois G tem, de modo natural, uma estrutura de $R[G]$-módulo. Esse $R[G]$-módulo é projetivo e de posto constante 1, se G for abeliano [34]. Denotamos por $Pic(R[G])$ o grupo de Picard das classes de isomorfismo dos $R[G]$-módulos projetivos de posto constante 1. Assim, temos a aplicação canônica $\pi : T(G,R) \to Pic(R[G])$. Na verdade, π é um homomorfismo de grupos abelianos [14]. O núcleo de π, que denotamos por $H(G;R)$, consiste das classes de isomorfismo das extensões abelianas de R com mesmo grupo de Galois G, que possuem R-base normal. Portanto, o estudo do grupo $T(G;R)$, se remete ao estudo dos subgrupos núcleo e imagem de π. Além disso, já que $T(G;R)$ é aditivo no primeiro fator, é suficiente estudar os grupos $T(\mathbb{Z}/p^m\mathbb{Z};R)$, p primo e

$1 \leq m \in \mathbb{N}$. Ou seja, estudaremos o grupo de Harrison das extensões cíclicas de R cujo grau é uma potência de um primo p.

Seguindo esta idéia, existem vários trabalhos dando contribuição ao estudo desses subgrupos e, conseqüentemente, à descrição do grupo de Harrison $T(G;R)$. A seguir, destacamos alguns dos trabalhos mais relevantes sobre o assunto até então obtidos, de nosso conhecimento:

1) Teoria de Kummer com raízes da unidade: [3], [8], [9], [19] e [32].
n invertível em R, $G \approx \mathbb{Z}/n\mathbb{Z}$ e R contém raiz n-ésima primitiva da unidade (cf. [3] e [8]): Neste caso, temos que $H(G;R) \approx \mathcal{U}(R)/\mathcal{U}(R)^n$, $Im(\pi) \approx Pic_n(R)$ e que a seqüência exata de grupos abelianos

$$1 \longrightarrow \mathcal{U}(R)/\mathcal{U}(R)^n \xrightarrow{\iota} T(G;R) \xrightarrow{\pi} Pic_n(R) \longrightarrow 1$$

cinde, onde $Pic_n(R)$ é o subgrupo de n-torção de $Pic(R)$.

2) Teoria de Kummer sem raízes da unidade: [10], [17], [16], [23].
p primo ímpar invertível em R, $G \approx \mathbb{Z}/p^m\mathbb{Z}$, $1 \leq m \in \mathbb{N}$ e R conexo (cf. [16]): Neste caso, precisamos de alguns resultados preliminares:

i) Por [22], para cada inteiro $m \geq 1$, R pode ser imerso em uma R-álgebra conexa S tal que S contém uma raiz ε do polinômio ciclotômico $\Phi_{p^m}(X) = \Phi_p(X^{p^{m-1}}) = (X^{p^{m-1}})^{p-1} + \cdots + X^{p^{m-1}} + 1$. Além disso $S = R[\varepsilon]$ é uma extensão cíclica de R com grupo de Galois Γ tal que $\gamma(\varepsilon) = \varepsilon^{t(\gamma)}$, onde $\Gamma = <\gamma>$ e $t : \Gamma \to \mathcal{U}(\mathbb{Z}/p^m\mathbb{Z})$ é um isomorfismo de grupos.

ii) O grupo Γ tem uma ação natural sobre o grupo $T(G;S)$, dada por $\gamma \cdot [A] = [{}_\gamma A]$, $\gamma \in \Gamma$ e $[A] \in T(G;S)$, onde o S-módulo ${}_\gamma A$ coincide com o grupo aditivo A e a ação de S sobre ${}_\gamma A$ é induzida por γ : $s \cdot a = \gamma(s)a$,

para quaisquer $s \in S$ e $a \in A$. Também temos que Γ age de modo similar sobre $Pic(S)$ e de maneira canônica, como grupo de Galois, sobre $\mathcal{U}(S)$. Isto permite definir uma *-ação de Γ sobre $\mathcal{U}(S)/(\mathcal{U}(S))^{p^m}$ $\Big(resp.\ Pic_{p^m}(S)\Big)$, conhecida na literatura como "ação de Stickelberger" [10], dada por $\gamma^*(s) = \gamma^{-1}(s^{t(\gamma)})(\mathrm{mod}\,\mathcal{U}(S)^{p^m})$ $\Big(\text{resp. } \gamma^*(\overline{P}) = \overline{\gamma(P^{t(\gamma)})}\Big)$, para todo $s \in \mathcal{U}(S)$ $\Big(resp.\ \overline{P} \in Pic_{p^m}(S)\Big)$.

iii) Com a ação de Γ sobre $T(G;S)$ e as *-ações de Γ sobre $\mathcal{U}(S)/\mathcal{U}(S)^{p^m}$ e $Pic_{p^m}(S)$, as aplicações ι e π na seqüência exata de grupos abelianos

$$1 \longrightarrow \mathcal{U}(S)/(\mathcal{U}(S))^{p^m} \xrightarrow{\iota} T(G;S) \xrightarrow{\pi} \mathrm{Pic}_{p^m}(S) \longrightarrow 1$$

são Γ-lineares. Conseqüentemente, a seqüência dos subgrupos estáveis

$$1 \longrightarrow \Big(\mathcal{U}(S)/(\mathcal{U}(S))^{p^m}\Big)^{^*\Gamma} \xrightarrow{\iota'} \Big(T(G;S)\Big)^{\Gamma} \xrightarrow{\pi'} \Big(Pic_{p^m}(S)\Big)^{^*\Gamma} \longrightarrow 1$$

também é exata, onde ι' e π' denotam as respectivas restrições de ι e π.

iv) A aplicação $j : T(G;R) \to T(G;S)$, dada por $j([A]) = [S \otimes_R A]$, é um homomorfismo de grupos cujo núcleo (resp. conúcleo) é igual ao núcleo (resp. conúcleo) de sua restrição j_0 a $H(G;R)$. Claramente, $j(T(G;R)) \subseteq \big(T(G;S)\big)^{\Gamma}$ e, a menos de isomorfismo, $j_0\big(H(G;R)\big) \subseteq \Big(\mathcal{U}(S)/\mathcal{U}(S)^{p^m}\Big)^{^*\Gamma}$

Finalmente estamos em condições de escrever o resultado principal obtido neste caso, que pode ser representado pelo seguinte diagrama de grupos, cujas linhas e colunas são exatas:

$$
\begin{array}{ccccccccc}
 & & ker(j_0) & = & ker(j) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & H(G;R) & \xrightarrow{i} & T(G;R) & \xrightarrow{\pi} & P(G;R) & \longrightarrow & 1 \\
 & & {\scriptstyle j_0}\downarrow & & {\scriptstyle j}\downarrow & & {\scriptstyle j'}\downarrow & & \\
1 & \longrightarrow & \left(\mathcal{U}(S)/\mathcal{U}(S)^{p^m}\right)^{*\Gamma} & \xrightarrow{\iota'} & \left(T(G;S)\right)^{\Gamma} & \xrightarrow{\pi'} & \left(Pic_{p^m}(S)\right)^{*\Gamma} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & coker(j_0) & = & coker(j) & & & &
\end{array}
$$

onde $P(G;R) = coker(i) = \dfrac{T(G;R)}{H(G;R)}$ e j' é um isomorfismo.

Além disso, se $m = 1$ então j_0 e j são isomorfismos [17].

3) Teoria de Artin-Schreier: [12], [33], [45].

$\boldsymbol{p = 0}$ **em** $\boldsymbol{R}$ **e** $\boldsymbol{G \approx \mathbb{Z}/p^m\mathbb{Z}}$ (cf. [12]): Neste caso $H(G;R) = T(G;R)$ ([26], [39]) e $T(G;R)$ é um $\mathbb{Z}/p^m\mathbb{Z}$-módulo livre de posto constante igual à dimensão de $R/\{r - r^p \mid r \in R\}$ como $\mathbb{Z}/p\mathbb{Z}$-espaço vetorial [12].

De um modo geral, o estudo do grupo $T(\mathbb{Z}/p^m\mathbb{Z};R)$ nesses trabalhos ainda está restrito aos casos p invertível ou $p = 0$ em R. Além disso, dentre os trabalhos mais completos com a hipótese p invertível, exige-se a condição $p \neq 2$, se $m > 1$. Quando p é um primo não necessariamente invertível em R, podemos reduzir o estudo do grupo $T(\mathbb{Z}/p^m\mathbb{Z};R)$ a dois casos [15]: p não divisor de zero ou $p = 0$ em R.

O caso $p = 0$ já está completamente resolvido, conforme descrito acima

em 3). No caso em que p não é divisor de zero em R, existem vários trabalhos muito interessantes na literatura (cf. [9], [16] e [19] para primos ímpares e [18] e [43] para $p = 2$), mas todos supondo que R possui uma raiz p-ésima primitiva da unidade. Dentre estes, é preciso destacar o trabalho de C. Greither [16] como o mais completo, mas para uma melhor leitura desta tese, faremos a seguir um breve resumo dos resultados obtidos por L. Childs em [9].

Sejam p um primo ímpar, $\varepsilon \in R$ uma raiz p-ésima primitiva da unidade e G um grupo cíclico de ordem p. Suponhamos que $p \in R^{\times}$ e seja $Prim(G;R)$ o conúcleo da inclusão canônica $i : H(G;R) \to T(G;R)$. Conseqüentemente, a seqüência de grupos dada abaixo é exata:

$$1 \longrightarrow H(G;R) \xrightarrow{i} T(G;R) \xrightarrow{\pi} Prim(G;R) \longrightarrow 1$$

onde π é a aplicação canônica.

Em [9] Childs descreve $Prim(G;R)$ como sendo isomorfo ao subgrupo dos elementos primitivos do grupo de Picard $Pic(R[G])$, isto é, isomorfo ao subgrupo $\{\overline{P} \in Pic(R[G]) \mid P \otimes_R P \approx R[G \otimes G] \otimes^{\Delta}_{R[G]} P\}$ onde o isomorfismo exigido é de $R[G \otimes G]$-módulos e $\Delta : R[G] \to R[G \otimes G]$ é o homomorfismo de R-álgebras induzido por $\Delta(\sigma) \mapsto \sigma \otimes \sigma$, $\sigma \in G$. Na realidade, como $|G| = p$ este subgrupo é de p-torsão ([36] Théorème 1.1), isto é, $Prim(G;R)$ é isomorfo ao subgrupo dos elementos primitivos de $Pic_p(R[G])$, que denotamos por $PrimPic_p(R[G])$.

O grupo $H(G;R)$ é descrito por L. Childs como sendo isomorfo ao grupo quociente $\mathcal{U}_{\lambda^p}(R)/\mathcal{U}_{\lambda}(R)^p$, onde $\lambda = \varepsilon - 1$ e $\mathcal{U}_{\lambda}(R)$ denota o grupo das

unidades de R do tipo $1 + \lambda r$, com $r \in R$.

O objetivo desta tese é dar uma descrição dos grupos $T(G;R)$, $H(G;R)$ e $PrimPic_p(R[G])$ para o caso em que G é um grupo cíclico de ordem p, R não possui uma raiz p-ésima primitiva da unidade, com p um primo ímpar, exigindo-se apenas que p seja um elemento regular em R. Obtemos esta descrição através da construção de uma nova seqüência exata de grupos. Fazemos isto, aplicando técnicas da teoria de "descente" galoisiana desenvolvidas por L. Childs em [10], e generalizadas por Greither em [16], à seqüência exata de L. Childs [9], para o caso em que $p \in R^{\times}$.

De agora em diante, assumimos que p é um primo ímpar regular em R e que o anel R não possui uma raiz p-ésima primitiva da unidade. Sejam G um grupo cíclico de ordem p e $S = \frac{R[X]}{\langle \Phi_p(X) \rangle} = R[\varepsilon]$, onde ε representa a classe de X módulo $\Phi_p(X)$, isto é, $\varepsilon = X + \langle \Phi_p(X) \rangle$ é uma raiz primitiva da unidade em S. Para cada $1 \leq i \leq p-1$, consideremos a aplicação $\gamma_i : S \to S$, induzida por $\gamma_i : \varepsilon \mapsto \varepsilon^i$. Claramente, $\gamma_i \in \mathcal{A}ut_R(S)$, $1 \leq i \leq p-1$ e $\Gamma = \{id = \gamma_1, \ldots, \gamma_{p-1}\}$ é um grupo cíclico de ordem $p-1$.

Consideramos a ação natural de Γ sobre os grupos $PrimPic_p(S[G])$ e $T(G;S)$ e a *-ação de Stickelberger sobre o grupo $\mathcal{U}_{\lambda^p}(S)/\mathcal{U}_{\lambda}(S)^p$. Estas ações comutam com as aplicações (cf. capítulo 2)

$\mathcal{U}_{\lambda^p}(S)/\mathcal{U}_{\lambda}(S)^p \approx H(G;S) \hookrightarrow T(G;S)$ e $T(G;S) \xrightarrow{\pi} PrimPic_p(S[G])$.

Então, aplicando alguns resultados clássicos e básicos de cohomologia,

obtemos que a seqüência dos grupos estáveis por Γ

$$1 \longrightarrow \Big(\mathcal{U}_{\lambda^p}(S)/\mathcal{U}_\lambda(S)^p\Big)^{*\Gamma} \longrightarrow \Big(T(G;S)\Big)^{\Gamma} \longrightarrow \Big(PrimPic_p(S[G])\Big)^{\Gamma} \longrightarrow 1$$

é exata. Além disso, mostramos que

$$H(G;R) \approx \Big(\mathcal{U}_{\lambda^p}(S)/\mathcal{U}_\lambda(S)^p\Big)^{*\Gamma} \approx \eta\Big(\mathcal{U}_{\lambda^p}(S)/\mathcal{U}_\lambda(S)^p\Big) \approx H(G;S)^{*\Gamma},$$

$$PrimPic_p(R[G]) \approx \Big(PrimPic_p(S[G])\Big)^{\Gamma} \approx \eta\Big(PrimPic_p(S[G])\Big), \quad \text{e}$$

$T(G;R) \approx \Big(T(G;S)\Big)^{\Gamma}$, onde η denota a norma definida para $S[\Gamma]$-módulos M tais que $pM = 0$, dada por $\eta(x) = \prod_{\gamma\in\Gamma} \gamma(x)$, $x \in M$. O isomorfismo $H(G;R) \approx \eta\Big(\mathcal{U}_{\lambda^p}(S)/\mathcal{U}_\lambda(S)^p\Big)$ já tinha sido obtido por D. Maurer [29], com hipóteses um pouco mais restritivas. Além disso, aqui mostramos esse isomorfismo utilizando métodos mais simples.

Dividimos este trabalho em três capítulos: um preliminar, com as notações e os resultados básicos, que nos permitem desenvolver o tema proposto (segundo capítulo). Terminamos esta tese com uma aplicação ao caso cúbico (terceiro capítulo), obtendo uma descrição do grupo $H(\mathbb{Z}/3\mathbb{Z};R)$ independente da *-ação de Γ. Em particular,

$$H(\mathbb{Z}/3\mathbb{Z},R) \approx \frac{\mathcal{U}_{\lambda^3}(S)}{\mathcal{U}_{\lambda^3}(R)\cdot\Big(\mathcal{U}_\lambda(S)\Big)^3}.$$

Capítulo 1: Pré-requisitos

1.1 Extensões galoisianas

O conceito de extensão de Galois de um anel comutativo foi introduzido por M. Auslander e O. Goldman [2] em 1960, e a teoria correspondente foi desenvolvida por S. U. Chase, D. K. Harrison e A. Rosenberg [6] em 1965. A seguir enunciamos o Teorema 1.3 de [6], onde os autores apresentam várias definições equivalentes deste conceito. Enunciamos este teorema segundo [11], [13] e [40], onde alguns ítens foram reescritos com hipóteses menos restritivas. Para isso, precisamos fixar a notação utilizada.

Seja R um anel comutativo com unidade. Dizemos que uma R-álgebra comutativa com unidade A é uma *extensão de* R, se A é um R-módulo fiel. Nesse caso, existe uma imersão natural de R em A que associa r com $r \cdot 1_A$, para cada $r \in R$. Para simplificar a notação identificamos R com $R \cdot 1_A$.

Agora, sejam A uma extensão de R e G um subgrupo finito do grupo $\mathcal{A}ut_R(A)$, dos R-automorfismos de A. Denotamos por $\Delta(A;G)$ o A-módulo livre com base $\{u_\sigma \mid \sigma \in G\}$. Observemos que $\Delta(A;G)$ possui uma estrutura de R-álgebra com a multiplicação dada por:

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

Consideremos o homomorfismo de R-álgebras $\phi : \Delta(A;G) \longrightarrow \mathcal{E}nd_R(A)$ definido por $\phi\Big(\sum_{\sigma\in G} a_\sigma u_\sigma\Big)(a) = \sum_{\sigma\in G} a_\sigma\sigma(a)$, para cada $a \in A$.

Por outro lado, denotamos por $e_G(A)$ a A-álgebra das funções de G em A, com as operações de adição e multiplicação usuais. Seja $v_\tau : G \longrightarrow A$ dada por $v_\tau(\rho) = \delta_{\tau,\rho} = \begin{cases} 1 & \text{se } \tau = \rho \\ 0 & \text{se } \tau \neq \rho \end{cases}$ para cada $\tau, \rho \in G$. Quando $\tau = id$, denotamos $\delta_{id,\rho}$ por $\delta_{1,\rho}$. Claramente, $\{v_\tau\}_{\tau\in G}$ é uma família de idempotentes (dois a dois) ortogonais com soma 1, e conseqüentemente, $e_G(A) = \underset{\tau\in G}{\oplus} Av_\tau$. Consideremos $A \otimes_R A$ como A-álgebra via primeira coordenada e o homomorfismo de A-álgebras $h : A \otimes_R A \longrightarrow e_G(A)$ induzido por $h(a \otimes b) : \rho \mapsto a\rho(b)$, para quaisquer $a, b \in A$ e $\rho \in G$. Finalmente, denotamos por $A^G = \{a \in A \mid \rho(a) = a, \quad \rho \in G\}$ o subanel de A formado pelos elementos estáveis sob a ação de G, e dado um $\Delta(A;G)$-módulo M, denotamos por M^G o R-submódulo de M formado pelos elementos estáveis sob a ação de G. Agora podemos enunciar o teorema

1.1.1. Teorema ([6], Theorem 1.3)

Sejam A uma extensão de R e G um subgrupo finito de $Aut_R(A)$.

As seguintes condições são equivalentes:

(i) *A é um R-módulo projetivo finitamente gerado e $\phi : \Delta(A;G) \longrightarrow \mathcal{E}nd_R(A)$ é um isomorfismo de R-álgebras.*

(ii) *A é um R-módulo projetivo finitamente gerado e para qualquer $\Delta(A;G)$-módulo a esquerda M, a aplicação $g : A \otimes_R M^G \longrightarrow M$, induzida por $g : a \otimes m \mapsto a \cdot m$ é um isomorfismo de A-módulos.*

(iii) *A é um R-módulo projetivo finitamente gerado e $h : A \otimes_R A \longrightarrow e_G(A)$é um isomorfismo de A-álgebras.*

(iv) *$A^G = R$ e existem $m \in \mathbb{N}$ e $x_j, y_j \in A$ $(1 \leq j \leq m)$ tais que $\sum_{j=1}^{m} x_j \sigma(y_j) = \delta_{1,\sigma}$, para todo $\sigma \in G$.*

(v) *$A^G = R$ e para cada $id \neq \sigma \in G$ e para cada ideal maximal $\mathcal{M}$ de A existe $a \in A$ tal que $(\sigma(a) - a) \notin \mathcal{M}$.*

(vi) *$A^G = R$, A é separável sobre R e para cada idempotente não nulo $\mathbf{e}$ de A e para quaisquer $\sigma, \tau \in G$, $\sigma \neq \tau$, existe $a \in A$ tal que $\sigma(a)\mathbf{e} \neq \tau(a)\mathbf{e}$.*

Dizemos que A é uma *extensão galoisiana de R com grupo de Galois G*, se A, R e G satisfazem uma (e portanto todas) das afirmações do Teorema 1.1.1. Os elementos x_i, y_i $(1 \leq i \leq m)$ do item **(iv)** são chamados *coordenadas de Galois* de A. Se, em particular, o grupo G é cíclico (resp. abeliano, p-grupo) dizemos que a extensão galoisiana A é cíclica (resp. abeliana, p-extensão). Toda extensão galoisiana de R com grupo de Galois G é, como R-módulo, projetivo finitamente gerado de posto constante igual à ordem de G (Lemma 4.1 de [6]), chamado de *grau da extensão.*

1.1.2. Lema ([6], Lemma 1.6)

Seja A, uma extensão galoisiana de R com grupo de Galois G. Então, existe $c \in A$ tal que $tr(c) = \sum_{\sigma \in G} \sigma(c) = 1$ e R é somando direto de A como R-módulo.

Dadas A e B duas extensões galoisianas de R com mesmo grupo de Galois G, seja $f : A \longrightarrow B$ um isomorfismo de R-álgebras. Dizemos que f é um *isomorfismo de extensões de Galois* se f comutar com a ação de G, isto é, se o diagrama

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \sigma \downarrow & & \downarrow \sigma \\ A & \xrightarrow{f} & B \end{array}$$

for comutativo, para todo $\sigma \in G$.

O próximo resultado estende o Teorema 3.4 de [6] e nos dá condições suficientes para que um R-homomorfismo entre uma extensão galoisiana de R e uma R-álgebra seja um isomorfismo. Em particular, se A e B são duas extensões galoisianas de R com mesmo grupo de Galois G tais que existe um homomorfismo $h : A \longrightarrow B$ satisfazendo $\sigma f = f\sigma$, para qualquer $\sigma \in G$, então A e B são isomorfas como extensões galoisianas.

1.1.3. Proposição

Sejam A, extensão galoisiana de R com grupo de Galois G e B uma extensão de R tal que exista uma imersão $\tau : G \longrightarrow \mathcal{A}ut_R(B)$ e $B^{\tau(G)} = R$. Se $f : A \longrightarrow B$ é um homomorfismo de R-álgebras satisfazendo $\tau(\sigma)f = f\sigma$ para cada $\sigma \in G$, então f é um isomorfismo.

Demonstração : Para simplificar a notação, para cada $\sigma \in G$, denotamos também por σ a sua imagem pela imersão em $\mathcal{A}ut_R(B)$. Sejam $x_i, y_i \in A$ $1 \leq i \leq m$ as coordenadas de Galois de A, ou seja, $\sum_{i=1}^{m} x_i\sigma(y_i) = \delta_{1,\sigma}$ para qualquer $\sigma \in G$. Consideremos $tr = \sum_{\sigma\in G} \sigma : A \longrightarrow R$ a aplicação traço. Seja $b \in B$. Temos:

$$f\Big(\sum_{i=1}^{m} x_i tr\big(f(y_i)b\big)\Big) = \sum_{i=1}^{m} f(x_i)tr(f(y_i)b) = \sum_{i=1}^{m} f(x_i)\cdot\sum_{\sigma\in G}\sigma\big(f(y_i)b\big)$$

$= \sum_{i=1}^{m} f(x_i) \cdot \sum_{\sigma \in G} f\big(\sigma(y_i)\big)\sigma(b) = \sum_{\sigma \in G} f\Big(\sum_{i=1}^{m} x_i \sigma(y_i)\Big)\sigma(b)$

$= \sum_{\sigma \in G} \delta_{1,\sigma}\sigma(b) = b$, isto é, f é sobrejetor.

Agora, seja $a \in A$ tal que $f(a) = 0$. Então, $f\Big(\sigma(y_i a)\Big) = \sigma\Big(f(y_i a)\Big) = \sigma\Big(f(y_i)f(a)\Big) = \sigma(0) = 0$, para quaisquer $\sigma \in G$ e $1 \leq i \leq m$. Assim, $tr(y_i a) = f(tr(y_i a)) = 0$, para todo $1 \leq i \leq m$. Conseqüentemente, $0 = \sum_{i=1}^{m} x_i tr(y_i a) = \sum_{\sigma \in G}\Big(\sum_{i=1}^{m} x_i \sigma(y_i)\Big)\sigma(a) = \sum_{\sigma \in G} \delta_{1,\sigma}\sigma(a) = a$, ou seja, f é injetor. □

Tomando a inclusão na proposição anterior, obtemos o

1.1.4. Corolário

Sejam $A \subseteq B$ extensões galoisianas de R com mesmo grupo de Galois G. Então $A = B$.

Mostremos, por exemplo, que $e_G(R)$ (que é o elemento identidade do grupo de Harrison $T(G;R)$) é, de fato, uma extensão galoisiana de R com grupo de Galois G. Nesse caso, identificamos R com $R \cdot 1_{e_G(R)} = R \cdot \sum_{\tau \in G} v_\tau$. A ação de G sobre $e_G(R)$ é dada pela permutação dos v_τ induzida pela multiplicação de G, isto é, $\sigma(v_\tau) = v_{\sigma\tau}$, $\sigma, \tau \in G$. Claramente $R \subseteq e_G(R)^G$. Seja $\alpha = \sum_{\tau \in G} r_\tau v_\tau \in e_G(R)^G$. Então, $\sigma \cdot \alpha = \sum_{\tau \in G} r_\tau v_{\sigma\tau} = \sum_{\tau \in G} r_\tau v_\tau$, para qualquer $\sigma \in G$. Conseqüentemente, para cada τ fixo, a coordenada r_τ de α coincide com a coordenada $r_{\sigma^{-1}\tau}$ de $\sigma \cdot \alpha$, para qualquer $\sigma \in G$. Ou seja, $r_\tau = r_{\sigma^{-1}\tau}$, para todo $\sigma \in G$. Logo, existe $r \in R$ tal que $r = r_\tau$, para todo $\tau \in G$. Assim,

$$\alpha = \sum_{\tau \in G} r_\tau v_\tau = \sum_{\tau \in G} r v_\tau = r \sum_{\tau \in G} v_\tau = r \cdot 1 = r, \quad \text{isto é,} \quad e_G(R)^G = R.$$

Finalmente, sejam $x_\tau = y_\tau = v_\tau$, para cada $\tau \in G$. Conforme já observado, $\{v_\sigma\}_{\sigma \in G}$ é um conjunto de idempotentes ortogonais, ou seja, $v_\tau v_\sigma = \delta_{\sigma,\tau} v_\tau$ para quaisquer $\sigma, \tau \in G$. Portanto $x_\tau, y_\tau \quad \tau \in G$ são as coordenadas de Galois de $e_G(R)$.

O próximo lema caracteriza quando uma extensão galoisiana A de R com grupo de Galois G é isomorfa a $e_G(R)$.

1.1.5. Lema ([20], Corollary 2)

Seja A, uma extensão galoisiana de R com grupo de Galois G.

As seguintes afirmações são equivalentes:

(i) *A e $e_G(R)$ são extensões galoisianas isomorfas.*

(ii) *Existe um homomorfismo de R-álgebras $f : A \to R$.*

Consideremos agora B uma R-álgebra comutativa. A partir de uma extensão galoisiana de R, construímos uma extensão galoisiana de B com mesmo grupo de Galois. Fazemos esta "subida" via produto tensorial sobre R, como mostra o próximo lema, devido a S. U. Chase, D. K. Harrison e A. Rosemberg.

1.1.6. Lema ([6], Lemma 1.7)

Sejam A, uma extensão galoisiana de R com grupo de Galois G e B uma R-álgebra comutativa. Consideramos G agindo sobre $B \otimes_R A$ via $\sigma(b \otimes a) = b \otimes \sigma(a)$, para quaisquer $a \in A$, $b \in B$ e $\sigma \in G$. Então, $B \otimes_R A$ é uma extensão galoisiana de B com grupo de Galois G.

O próximo resultado é uma conseqüência imediata do Lema 1.1.6 e da Proposição 1.1.3.

1.1.7. Corolário

Sejam A, uma extensão galoisiana de S com grupo de Galois G e H um grupo finito qualquer. Então, $A[H]$ é uma extensão galoisiana de $S[H]$ com grupo de Galois G agindo sobre $A[H]$ via $\sigma\Big(\sum_{h\in H} a_h h\Big) = \sum_{h\in H} \sigma(a_h)h$.

O Lema que enunciamos a seguir, devido a M. Orzech (Lemma 1.5 de [34]), nos dá uma recíproca do Lema 1.1.6 no caso em que S é uma R-álgebra fielmente plana ([4], pg.46).

1.1.8. Lema ([34], Lemma 1.5-b)

Sejam A uma R-álgebra comutativa e G um subgrupo finito de $Aut_R(A)$. Seja S uma R-álgebra fielmente plana tal que $S \otimes_R A$ seja uma extensão galoisiana de S com grupo de Galois G. Então, A é uma extensão galoisiana de R com grupo de Galois G.

1.2 Raiz Primitiva da Unidade

Sejam S um anel com unidade, $S^\times = \{s \in S \mid s \text{ é regular em } S\}$ e $n \in \mathbb{N}$, $n \neq 0$. Nosso objetivo nesta secção é estender o conceito de raiz primitiva n-ésima da unidade ao anel S, com $n \in S^\times$, a partir da raiz complexa $\xi = e^{2\pi i/n}$. Também descrevemos o ideal gerado pelo primo p, quando o anel S possui uma raiz primitiva p-ésima da unidade.

Temos, que em $\mathbb{Z}[\xi][X]$, $X^n - 1 = \prod_{i=0}^{n-1}(X - \xi^i)$ e $n = \prod_{i=1}^{n-1}(1 - \xi^i)$.

Seja $\phi_d(X) = \prod_{\substack{1\leq i\leq d \\ (i,d)=1}} (X - \xi^i)$ o d-ésimo polinômio ciclotômico. Então,

$X^n - 1 = \prod_{d|n} \phi_d(X)$ e $\phi_d(X) \in \mathbb{Z}[X]$ é irredutível e mônico ([30], pg.40).

Dado um homomorfismo de anéis com unidade $\sigma : S \to S'$, denotamos por $\sigma^* : S[X] \to S'[X]$ o homomorfismo de anéis induzido por σ, isto é, $\sigma^*\left(\sum_{i=0}^{m} a_i X^i\right) = \sum_{i=0}^{m} \sigma(a_i) X^i$. Então o d-ésimo polinômio ciclotômico em $S[X]$, que denotamos por $\Phi_d(X)$, é a imagem de $\phi_d(X)$ pelo homomorfismo $\sigma^* : \mathbb{Z}[X] \to S[X]$ com $\sigma(t) = t \cdot 1_S$, para todo $t \in \mathbb{Z}$.

Consideremos agora o epimorfismo de anéis $\theta : \mathbb{Z}[X] \to \mathbb{Z}[\xi]$ definido por $\theta(g) = g(\xi)$. Como $\phi_n(\xi) = 0$ e $\phi_n(X)$ é irredutível e mônico em $\mathbb{Z}[X]$, $Ker(\theta) = \langle \phi_n(X) \rangle$. Assim, pelo teorema do homomorfismo,

$\overline{\theta} : \dfrac{\mathbb{Z}[X]}{\langle \phi_n(X) \rangle} \longrightarrow \mathbb{Z}[\xi]$ onde $\overline{\theta} : \overline{g} \mapsto g(\xi)$ é um isomorfismo de anéis.

O lema a seguir nos permite estender o conceito de raiz primitiva da unidade ao anel S.

1.2.1. Lema

Sejam $0 \neq n \in \mathbb{N}$ e $\varepsilon \in S$. As seguintes afirmações são equivalentes:

(i) $n \in S^\times$ e $\Phi_n(\varepsilon) = 0$.

(ii) $\varepsilon^n = 1$ e $(1 - \varepsilon^i) \in S^\times$, *para todo* $1 \leq i \leq n-1$.

Demonstração : Sejam $\rho : S[X] \longrightarrow S$ dado por $\rho : g \mapsto g(\varepsilon)$ e $h = \rho \circ \sigma^* : \mathbb{Z}[X] \longrightarrow S$. Como acima, $\phi_n \in Ker(h)$. Conseqüentemente, existe um homomorfismo de anéis $\overline{h} : \dfrac{\mathbb{Z}[X]}{\langle \phi_n(X) \rangle} \longrightarrow S$. Assim, $\beta = \overline{h} \circ \overline{\theta}^{-1} : \mathbb{Z}[\xi] \longrightarrow S$, $\beta : g(\xi) \mapsto g(\varepsilon)$ é um homomorfismo de anéis.

Agora, em $\mathbb{Z}[\xi]$, $\xi^n = 1$ e $n = \prod_{i=1}^{n-1}(1 - \xi^i)$. Portanto, em S,

$$\varepsilon^n = \beta(\xi)^n = \beta(\xi^n) = \beta(1) = 1 \quad \text{e} \quad n = \beta(n) = \prod_{i=1}^{n-1} \beta(1 - \xi^i) = \prod_{i=1}^{n-1}(1 - \varepsilon^i).$$

Mas $n \in S^\times$, e então, $(1 - \varepsilon^i) \in S^\times$, para todo $1 \leq i \leq n-1$.

Reciprocamente, suponhamos que $\varepsilon^n = 1$ e que, para cada $1 \leq i \leq n-1$, $(1 - \varepsilon^i) \in S^\times$. Então, segue que

$$0 = (\varepsilon^i)^n - 1 = (\varepsilon^i - 1)\Big((\varepsilon^i)^{n-1} + (\varepsilon^i)^{n-2} + \ldots + \varepsilon^i + 1\Big), \quad \text{donde}$$

concluímos que $\Big((\varepsilon^i)^{n-1} + (\varepsilon^i)^{n-2} + \ldots + \varepsilon^i + 1\Big) = 0$, pois $(\varepsilon^i - 1) \in S^\times$. Ou seja, ε^i é raiz do polinômio $f(X) = X^{n-1} + \ldots + X + 1$ para cada $1 \leq i \leq n-1$. Como f é mônico e $(\varepsilon^i - \varepsilon^j) \in S^\times$ para quaisquer $1 \leq i \neq j \leq n-1$, é fácil ver que $f = \prod_{i=1}^{n-1}(X - \varepsilon^i)$. Assim, $n = f(1) = \prod_{i=1}^{n-1}(1 - \varepsilon^i) \in S^\times$. Além disso, em $\mathbb{Z}[X]$, $(X^\ell - 1) = \prod_{d|\ell} \phi_d(X)$ e então, aplicando σ^*, obtemos que, em $S[X]$, $(X^\ell - 1) = \prod_{d|\ell} \Phi_d(X)$. Conseqüentemente, $(\varepsilon^\ell - 1) = \prod_{d|\ell} \Phi_d(\varepsilon)$. Agora, se $\ell < n$, então $(\varepsilon^\ell - 1) \in S^\times$ e segue que $\Phi_d(\varepsilon) \in S^\times$, para todo $d \mid \ell$. Em particular, $\Big(\prod_{\substack{\ell|n \\ \ell \neq n}} \Phi_\ell(\varepsilon)\Big) \in S^\times$.

Já que $\prod_{\ell|n} \phi_\ell(X) = (X^n - 1)$ em $\mathbb{Z}[X]$, segue que $\prod_{\ell|n} \Phi_\ell(\varepsilon) = \varepsilon^n - 1 = 0$,

isto é, $0 = \Big(\prod_{\substack{\ell|n \\ \ell \neq n}} \Phi_\ell(\varepsilon)\Big) \cdot \Phi_n(\varepsilon)$. Logo, $\Phi_n(\varepsilon) = 0$. □

Sejam $0 \neq n \in \mathbb{N}$ e $\varepsilon \in S$. Dizemos que ε é raiz n-ésima primitiva da unidade em S, se ε e n satisfazem uma das condições equivalentes do lema.

Observemos que para p primo, em $\mathbb{Z}[\xi][X]$, $\phi_p(X) = \sum_{i=0}^{p-1} X^i = \prod_{i=1}^{p-1}(X - \xi^i)$. Então, segue do homomorfismo β definido na demonstração acima que $\sum_{i=0}^{p-1} z^i = \prod_{i=1}^{p-1}(z - \varepsilon^i)$ para todo $z \in S$. Em particular, $p = \prod_{i=1}^{p-1}(1 - \varepsilon^i)$.

Consideremos agora $0 \neq n \in \mathbb{N}$ e R um anel com unidade que não contém uma raiz n-ésima primitiva da unidade, com $n \in R^\times$. Sejam $S = \dfrac{R[X]}{\langle \Phi_n(X) \rangle}$ e $\varepsilon = X + \langle \Phi_n(X) \rangle \in S$. Claramente $n = n \cdot 1_S \in S^\times$ e $\Phi(\varepsilon) = 0$, e portanto ε é uma raiz n-ésima primitiva da unidade em $S = R[\varepsilon]$. Por outro lado, temos que $\{1, \varepsilon, \ldots, \varepsilon^{m-1}\}$ é uma R-base de $R[\varepsilon]$, onde m é o grau de $\Phi_n(X)$. Então, segue que todo elemento regular de R também é regular em $R[\varepsilon]$, ou seja, $R^\times \subseteq (R[\varepsilon])^\times$. Por outro lado, é imediato que todo elemento de $R \cap (R[\varepsilon])^\times$ é regular em R. Isto mostra que os elementos regulares se comportam muito bem com relação à contração. O lema abaixo registra este fato:

1.2.2. Lema

Sejam $0 \neq n \in \mathbb{N}$, ε raiz n-ésima primitiva da unidade num anel S que

contém R *e* $S = R[\varepsilon]$. *Então,* $R \bigcap S^{\times} = R^{\times}$.

O próximo lema, juntamente com a igualdade $p = \prod_{i=1}^{p-1}(1-\varepsilon^i)$ em S, que vimos acima, nos permite dar uma descrição do ideal gerado por p, pS, em função de $(1-\varepsilon)$.

1.2.3. Lema

Sejam $p \in \mathbb{Z}$ *primo,* $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle}$ *e* $\varepsilon = X + \langle \Phi_p(X) \rangle$. *Então,*

$$(1-\varepsilon^i)S = (1-\varepsilon)S \quad \textit{para cada} \quad 1 \leq i \leq p-1.$$

Demonstração : Seja $i \in \{1, \ldots, p-1\}$. Logo, existem números inteiros s e t satisfazendo $1 = si + tp$. Mas ε é uma raiz p-ésima primitiva da unidade em S, e então $\varepsilon - 1 = (\varepsilon^i - 1)\big(\varepsilon^{i(s-1)} + \cdots + \varepsilon^i + 1\big)$. Por outro lado, $\varepsilon^i - 1 = (\varepsilon - 1)\big(\varepsilon^{i-1} + \cdots + \varepsilon + 1\big)$. Logo,

$$\varepsilon - 1 = (\varepsilon - 1)\big(\varepsilon^{i-1} + \cdots + \varepsilon + 1\big)\big(\varepsilon^{i(s-1)} + \cdots + \varepsilon^i + 1\big)$$

ou seja, $\big(\varepsilon^{i-1} + \cdots + \varepsilon + 1\big)\big(\varepsilon^{i(s-1)} + \cdots + \varepsilon^i + 1\big) = 1$. Assim, $u = \varepsilon^{i-1} + \cdots + \varepsilon + 1 \in \mathcal{U}(S)$, onde $\mathcal{U}(S)$ denota o conjunto das unidades do anel S. Portanto, $1 - \varepsilon^i = u(1-\varepsilon)$, com $u \in \mathcal{U}(S)$. Segue que $(1-\varepsilon^i)S = (1-\varepsilon)uS = (1-\varepsilon)S$. □

1.2.4. Corolário

Sejam $p \in \mathbb{Z}$ *primo,* $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle}$ *e* $\varepsilon = X + \langle \Phi_p(X) \rangle$. *Então,*

$$pS = \prod_{i=1}^{p-1}(1-\varepsilon^i)S = (1-\varepsilon)^{(p-1)}S.$$

O corolário a seguir será muito útil no próximo capítulo. Ele nos permitirá definir os isomorfismos necessários para dar uma caracterização do grupo das extensões galoisianas sobre o anel R com mesmo grupo de Galois (ver capítulo 2).

1.2.5. Corolário

Sejam S uma álgebra comutativa, $\varepsilon \in S$ uma raiz p-ésima primitiva da unidade, $\lambda = (\varepsilon - 1)$ e $a = \lambda^p s + 1$ com $s \in S$. Então, existe um polinômio mônico $f \in S[X]$ tal que $(\lambda X + 1)^p - a = \lambda^p f(X)$.

Demonstração : Claramente $(\lambda X + 1)^p - a = \sum_{i=1}^{p} \binom{p}{i} \lambda^i X^i - \lambda^p s$. Mas, pelo corolário anterior, $\binom{p}{i}\lambda^i \in \lambda^i pS = \lambda^i \lambda^{p-1} S \subseteq \lambda^p S$. Logo, para cada $i \in \{1, \ldots, p\}$ existe $s_i \in S$ tal que $\binom{p}{i}\lambda^i = \lambda^p s_i$. Então, $(\lambda X + 1)^p - a = \sum_{i=1}^{p} \lambda^p s_i X^i - \lambda^p s = \lambda^p \left(\sum_{i=1}^{p} s_i X^i - s \right)$. Como $\binom{p}{p}\lambda^p = \lambda^p$, $s_p = 1$. Conseqüentemente, o polinômio $f(X) = \sum_{i=1}^{p} s_i X^i - s \in S[X]$ é mônico e, por construção, satisfaz $(\lambda X + 1)^p - a = \lambda^p f(X)$. □

Dado um anel A, denotamos por $\mathcal{M}ax(A)$ o conjunto dos ideais maximais de A.

1.2.6. Lema

Sejam S uma extensão inteira de R, $\Gamma \subseteq \mathcal{A}ut_R(S)$ subgrupo finito tal que $S^\Gamma = R$, $\wp \in \mathcal{M}ax(R)$ e $\mathcal{F} = \{q \in \mathcal{M}ax(S) \mid q \cap R = \wp\}$. Então, Γ age transitivamente sobre $\mathcal{F}$. Em particular, se R é um anel semi-local então S também é semi-local.

Demonstração : Claramente, $\mathcal{F} = \{q \in \mathcal{M}ax(S) \mid \wp S \subseteq q\}$. Logo, como $\wp S$ é um ideal não nulo de S, existe um ideal maximal de S que contém $\wp S$. Então, este ideal pertence à $\mathcal{F}$, e portanto $\mathcal{F} \neq \emptyset$. Seja $q \in \mathcal{F}$ e suponhamos, por absurdo, que exista $q' \in \mathcal{F}$ satisfazendo $q' \neq \gamma(q)$, para todo $\gamma \in \Gamma$. Assim, $S = q' + \gamma(q)$, para cada $\gamma \in \Gamma$. Logo, $\{q', \gamma(q) \mid \gamma \in \Gamma\}$ é um conjunto finito de ideais co-maximais. Pelo Teorema Chinês dos Restos, existe $x \in S$ tal que $x \in q'$ e $x \equiv 1 \big(\mathrm{mod}\, \gamma(q)\big)$, para todo $\gamma \in \Gamma$. Em particular, $x \notin \gamma(q)$, ou seja, $\gamma^{-1}(x) \notin q$ para qualquer $\gamma \in \Gamma$. Segue que $\prod_{\gamma \in \Gamma} \gamma^{-1}(x) \notin q$. Por outro lado, $\prod_{\gamma \in \Gamma} \gamma^{-1}(x) \in S^{\Gamma} = R$. Temos ainda que $x \in q'$, donde obtemos que $\prod_{\gamma \in \Gamma} \gamma^{-1}(x) \in q' \cap R = \wp \subseteq q$, o que contradiz a hipótese assumida. Portanto Γ age transitivamente sobre $\mathcal{F}$.

Agora Γ é um grupo finito, e portanto segue que $\mathcal{F}$ é uma família finita. Conseqüentemente, se R é um anel semi-local então S também é semi-local (ver [1] Corollary 5.8). □

Finalizamos esta secção, observando que se R é um anel local, $S = R[\varepsilon]$ é semilocal. Isto é uma conseqüência do Lema anterior, já que $S = R[\varepsilon]$ é uma extensão inteira de R tal que $R = S^{\Gamma}$, onde $\Gamma = \{\gamma_i \mid \gamma_i : \varepsilon \mapsto \varepsilon^i, 1 \leq i \leq p-1\}$ subgrupo finito de $\mathcal{A}ut_R(S)$.

1.3 Extensões de Galois com base normal

Seja A, uma extensão galoisiana de R com grupo de Galois G. Nesta secção caracterizamos os elementos geradores de uma R-base normal de A, isto é, os elementos $x \in A$ tais que $\{\sigma(x) \mid \sigma \in G\}$ é uma base de A como R-módulo livre. A proposição a seguir relaciona a existência de uma R-base normal com a invertibilidade de matrizes. Isto nos dá uma boa ferramenta para verificar se uma determinada R-base de A é gerada pela ação de G sobre um elemento de A, ou seja, se A possui uma R-base normal.

1.3.1. Proposição ([39], Proposition 3.1)

Sejam A uma, extensão galoisiana de R com grupo de Galois $G = \{\sigma_1 = id_A, \sigma_2, \ldots, \sigma_n\}$ e $x \in A$. As seguintes condições são equivalentes:

(i) $\{x_i = \sigma_i(x) \mid 1 \leq i \leq n\}$ *é R-base normal de A.*

(ii) $det\Big(\sigma_i(x_j)\Big)_{1 \leq i,j \leq n} \in \mathcal{U}(A)$.

Demonstração : Sejam $a_i, b_i \in A$, $1 \leq i \leq m$, tais que $\sum_{i=1}^{m} a_i \sigma_j(b_i) = \delta_{1,j}$ para todo $1 \leq j \leq n$. Agora, para cada $i \in \{1, \ldots, m\}$, existem $\lambda_{i,k} \in R$, $1 \leq k \leq n$ tais que $a_i = \sum_{k=1}^{n} \lambda_{i,k} x_k$. Assim,
$\delta_{1,j} = \sum_{i=1}^{m} a_i \sigma_j(b_i) = \sum_{i=1}^{m} \sum_{k=1}^{n} \lambda_{i,k}\, x_k \cdot \sigma_j(b_i) = \sum_{k=1}^{n} x_k \cdot \sigma_j\Big(\sum_{i=1}^{m} \lambda_{i,k} b_i\Big) =$
$\sum_{k=1}^{n} x_k \sigma_j(y_k)$ para qualquer $1 \leq j \leq n$, onde $y_k = \sum_{i=1}^{m} \lambda_{i,k} b_i$, para cada $1 \leq k \leq n$.

Definimos as matrizes $M = \Big(\sigma_i(x_j)\Big) = \Big(\sigma_i \sigma_j(x)\Big)$ e $N = \Big(\sigma_j(y_i)\Big)$ com $1 \leq i, j \leq n$. Então, $MN = I_n$, a matriz identidade $n \times n$. De fato,

$$\Big(\sigma_i(x_1), \ldots, \sigma(x_n)\Big) \cdot \Big(\sigma_j(y_1), \ldots, \sigma_j(y_n)\Big)^t = \sum_{k=1}^{n} \sigma_i(x_k)\sigma_j(y_k)$$

$= \sigma_i \sum_{k=1}^{n} x_k(\sigma_i^{-1}\sigma_j)(y_k) = \delta_{i,j}$. Logo, $det\Big(\sigma_i\sigma_j(x)\Big)_{1\leq i,j\leq n} \in \mathcal{U}(A)$.

Reciprocamente, seja $x \in A$ tal que $det\Big(\sigma_i\sigma_j(x)\Big)_{1\leq i,j\leq n} \in \mathcal{U}(A)$. Como $M = \Big(\sigma_i\sigma_j(x)\Big)$ é invertível, sejam $y_1, \ldots, y_n \in A$, as entradas da primeira coluna da matriz M^{-1}. Logo, para qualquer $1 \leq i \leq n$,
$\sum_{j=1}^{n} \sigma_i\sigma_j(x)y_j = \delta_{id,\sigma_i} = \delta_{1,i}$. Então, $M^{-1} = \Big(\sigma_j(y_i)\Big)_{1\leq i,j\leq n}$. De fato,

$$\Big(\sigma_i(x_1), \ldots, \sigma_i(x_n)\Big) \cdot \Big(\sigma_j(y_1), \ldots, \sigma_j(y_n)\Big)^t = \sum_{k=1}^{n} \sigma_i(x_k)\sigma_j(y_k)$$

$$= \sigma_j\Big(\sum_{k=1}^{n} \sigma_j^{-1}\sigma_i(x_k)y_k\Big) = \sigma_j(\delta_{id,\sigma_j^{-1}\sigma_i}) = \sigma_j(\delta_{i,j}) = \delta_{i,j}.$$

Seja $T_M : A^n \longrightarrow A^n$ definido por $T_M(a_1, \ldots, a_n) = (a_1, \ldots, a_n) \cdot M^t$. Então, T_M é um isomorfismo de R-módulos. Seja $a \in A$. Da sobrejetividade de T_M, decorre que existem $\lambda_1, \ldots, \lambda_n \in A$ tais que $T_M(\lambda_1, \ldots, \lambda_n) = (a, \sigma_2(a), \ldots, \sigma_n(a))$. Desta igualdade decorre que $\sum_{i=1}^{n} \lambda_i x_i = a$ e que $(\lambda_1, \ldots, \lambda_n) = (a, \sigma_2(a), \ldots, \sigma_n(a))(M^t)^{-1}$. Segue que $\lambda_i = \sum_{j=1}^{n} \sigma_j(ax_i) \in A^G = R$. Conseqüentemente, $\{x_1, \ldots, x_n\}$ é um sistema de geradores de A sobre R. Agora, sejam, $r_1, \ldots, r_n \in R$ tais que $\sum_{i=1}^{n} r_i x_i = 0$. Mas,

$$\begin{aligned} T_M(r_1, \ldots, r_n) &= (r_1, \ldots, r_n)M^t \\ &= \Big(\sum_{i=1}^{n} r_i\sigma_1(x_i), \sum_{i=1}^{n} r_i\sigma_2(x_i), \ldots, \sum_{i=1}^{n} r_i\sigma_n(x_i)\Big) \\ &= \Big(\sum_{i=1}^{n} r_i x_i, \sigma_2(\sum_{i=1}^{n} r_i x_i), \ldots, \sigma_n(\sum_{i=1}^{n} r_i x_i)\Big), \end{aligned}$$

e segue que $T_M(r_1, \ldots, r_n) = 0$. Como T_M é injetor, temos que $r_i = 0$ para todo $1 \leq i \leq n$. Logo, $\{x_1, \ldots, x_n\}$ é R-linearmente independente, e portanto $\{x_1 = \sigma_1(x), \ldots, x_n = \sigma_n(x)\}$ é uma R-base de A. □

1.3.2. Corolário

Suponhamos que A seja extensão galoisiana de R com grupo de Galois cíclico $G = \langle \sigma \mid \sigma^n = 1 \rangle$ e $\alpha = \sum_{i=0}^{n-1} \alpha_i \sigma^{-i} \in A[G]$. As condições abaixo são equivalentes:

(i) *$\{\alpha_i\}_{i=0}^{n-1}$ é R-base de A e $\sigma^i(\alpha_0) = \alpha_i$, para todo $0 \leq i \leq n-1$.*

(ii) *$\alpha \in \mathcal{U}(A[G])$ e $\sigma(\alpha) = \alpha\sigma$, onde a ação de G sobre $A[G]$ é dada pela ação nas coordenadas.*

Demonstração : Mostremos que $\sigma^i(\alpha_0) = \alpha_i$, $1 \leq i \leq n-1$ é equivalente a $\sigma(\alpha) = \alpha\sigma$. Temos: $\alpha = \sum_{i=0}^{n-1} \alpha_i \sigma^{-i} = \sum_{i=0}^{n-1} \sigma^i(\alpha_0)\sigma^{-i}$, e portanto, segue que $\sigma(\alpha) = \sum_{i=0}^{n-1} \sigma^{i+1}(\alpha_0)\sigma^{-i} = \sum_{j=1}^{n} \sigma^j(\alpha_0)\sigma^{-j}\sigma = \left(\sum_{j=0}^{n-1} \sigma^j(\alpha_0)\sigma^{-j}\right)\sigma = \alpha\sigma$. Reciprocamente, $\sum_{i=0}^{n-1} \sigma(\alpha_i)\sigma^{-i} = \sum_{i=0}^{n-1} \alpha_i \sigma^{-i+1} = \sum_{j=0}^{n-1} \alpha_{j+1}\sigma^{-j}$, e então, $\alpha_{j+1} = \sigma(\alpha_j)$, para qualquer $0 \leq j \leq n-1$, ou seja, $\alpha_i = \sigma^i(\alpha_0)$, para todo $1 \leq i \leq n-1$.

Resta verificar que $\{\alpha_i\}_{i=0}^{n-1}$ é R-base de A equivale a $\alpha \in \mathcal{U}(A[G])$. Seja

$$\mathcal{C}_n(A) = \left\{ M = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{pmatrix} \mid a_i \in A,\ 0 \leq i \leq n-1 \right\},$$

a R-subálgebra comutativa de $A_{n\times n}$ das matrizes circulantes. Consideremos agora $\tau : A^n \longrightarrow A^n$ a permutação circular $\tau : (a_0, a_1, \dots, a_{n-1}) \mapsto (a_{n-1}, a_0, a_1, \dots, a_{n-2})$. Claramente, $\tau \in \mathcal{A}ut_A(A^n)$ e $\tau^n = id_{A^n}$. Também é fácil ver que uma matriz quadrada $M \in \mathcal{C}_n(A)$ se, e somente se, existe $v = (a_0, a_1, \dots, a_{n-1}) \in A^n$ tal que $M = \left(v, \tau(v), \dots, \tau^{n-1}(v)\right)^t$.

Sejam $v_0 = (0, \ldots, 0, 1) \in A^n$ e $\theta = \Big(v_0, \tau(v_0), \ldots, \tau^{n-1}(v_0)\Big)^t$. É fácil ver que $\theta^n = I_n$ (a matriz identidade) e para cada $1 \leq i \leq n-1$, $\theta^i = \Big(v_i, \tau(v_i), \ldots, \tau^{n-1}(v_i)\Big)^t$, onde $v_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ com 1 na i-ésima coordenada $(1 \leq i \leq n-1)$. Além disso, para cada matriz circulante M, temos $M = \Big(v, \tau(v), \ldots, \tau^{n-1}(v)\Big)^t$ com $v = (a_0, a_1, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} a_i v_i$, e portanto,

$$M = \Big(v, \tau(v), \ldots, \tau^{n-1}(v)\Big)^t = \Big(\sum_{i=0}^{n-1} a_i v_i, \sum_{i=0}^{n-1} a_i \tau(v_i), \ldots, \sum_{i=0}^{n-1} a_i \tau^{n-1}(v_i)\Big)^t$$

$$= \sum_{i=0}^{n-1} a_i \Big(v_i, \tau(v_i), \ldots, \tau^{n-1}(v_i)\Big)^t = \sum_{i=0}^{n-1} a_i \theta^i.$$

Finalmente, seja $\phi\colon A[G] \longrightarrow \mathcal{C}_n(A)$ dado por $\phi\Big(\sum_{i=0}^{n-1} a_i \sigma^{-i}\Big) = \sum_{i=0}^{n-1} a_i \theta^i$. Então, ϕ é um isomorfismo de A-álgebras. Conseqüentemente, $\mathcal{U}(A[G])$ e $\mathcal{U}\Big(\mathcal{C}_n(A)\Big)$ são isomorfos. Logo, $\alpha \in \mathcal{U}(A[G])$ e $\phi(\alpha) \in \mathcal{U}\Big(\mathcal{C}_n(A)\Big)$ são equivalentes. O resultado segue agora da Proposição 1.3.1. □

Voltemos a considerar $p \in \mathbb{Z}$ primo e regular em R, $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle} = R[\varepsilon]$, $\varepsilon = X + \langle \Phi_p(X) \rangle$. Como já vimos, ε é uma raiz p-ésima primitiva da unidade em S. Denotamos por γ_i o R-automorfismo de S dado por $\gamma_i(\varepsilon) = \varepsilon^i$ e seja $\Gamma = \{\gamma_i \mid 1 \leq i \leq p-1\}$. Como p é primo, $\mathcal{U}\Big(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\Big)$ é um grupo cíclico. Claramente, $\rho : \mathcal{U}\Big(\frac{\mathbb{Z}}{p\mathbb{Z}}\Big) \longrightarrow \Gamma$ dado por $\rho(\overline{i}) = \gamma_i$, para todo $1 \leq i \leq p-1$ é um isomorfismo de grupos. Seja $\overline{i_0}$ um gerador de $\mathcal{U}\Big(\frac{\mathbb{Z}}{p\mathbb{Z}}\Big)$. Portanto, Γ é um grupo cíclico com, por exemplo, $\Gamma = \langle \rho(\overline{i_0}) \rangle$. De agora em diante, fixamos $t \in \{1, \ldots, (p-1)\}$ tal que $\gamma = \gamma_t = \rho(\overline{i_0})$, isto é, $\Gamma = \langle \gamma \rangle$.

Dada A, uma extensão galoisiana de S com grupo de Galois G, dizemos

que A é uma *extensão Γ-normal de S*, se existe $\tilde{\gamma} : A \longrightarrow A$ automorfismo de R-álgebra que comuta com a ação de G e estende γ, isto é, $\tilde{\gamma}|_S = \gamma$ e $\sigma\tilde{\gamma} = \tilde{\gamma}\sigma$ para todo $\sigma \in G$. Por exemplo, $A = e_G(S)$ é uma extensão Γ-normal de S. De fato, seja $\tilde{\gamma} : e_G(S) \longrightarrow e_G(S)$ definida por $\tilde{\gamma}\left(\sum_{\tau\in G} s_\tau v_\tau\right) = \sum_{\tau\in G} \gamma(s_\tau)v_\tau$, para todo $\sum_{\tau\in G} s_\tau v_\tau \in e_G(S)$. Claramente, $\tilde{\gamma}$ é um R-automorfismo de $e_G(S)$ que comuta com a ação de G sobre $e_G(S)$ e estende γ.

Consideremos agora A, uma extensão galoisiana de S com grupo de Galois $G = \langle \sigma \mid \sigma^p = 1 \rangle$ que também é uma extensão Γ-normal de S. Seja $\tilde{\gamma} \in \mathcal{A}ut_R(A)$ satisfazendo $\tilde{\gamma}|_S = \gamma$ e $\tilde{\gamma}\sigma = \sigma\tilde{\gamma}$. Os grupos G e Γ se estendem naturalmente a grupos de automorfismos de $A[G]$, pelas ações abaixo:

$$\sigma(\sum_{i=0}^{p-1} a_i\sigma^{-i}) = \sum_{i=0}^{p-1} \sigma(a_i)\sigma^{-i} \quad \text{e} \quad \tilde{\gamma}(\sum_{i=0}^{p-1} a_i\sigma^{-i}) = \sum_{i=0}^{p-1} \tilde{\gamma}(a_i)\sigma^{-it}$$

satisfazendo $\sigma\tilde{\gamma} = \tilde{\gamma}\sigma$.

Temos, pelo Corolário 1.1.7, que $A[G]$ é extensão galoisiana de $S[G]$ com grupo de Galois G. A seguir, construímos uma S-base normal de A induzida pela ação de $\tilde{\gamma}$ sobre o gerador de uma S-base normal de A conhecida. Isto é uma aplicação direta do corolário anterior.

1.3.3. Corolário

Sejam $R, S, \Gamma, G, A, \gamma, \sigma, t, p$ e ε, como acima. Suponhamos ainda que $\tilde{\gamma}$ estenda γ à $A[G]$ satisfazendo $\tilde{\gamma}\sigma = \sigma\tilde{\gamma}$ e $\alpha_0 \in A$ é tal que $\{\alpha_i = \sigma^i(\alpha_0)\}_{i=0}^{p-1}$ seja uma S-base normal de A, $\alpha = \sum_{i=0}^{p-1} \alpha_i\sigma^{-i}$ e $\beta = \prod_{i=0}^{p-2} \tilde{\gamma}^{-i}(\alpha^{-1})^{t^i}$ $= \sum_{i=0}^{p-1} \beta_i\sigma^{-i} \in A[G]$. Então, $\{\beta_i = \sigma^i(\beta_0)\}_{i=0}^{p-1}$ é também S-base normal de A.

Demonstração : Pelo Corolário 1.3.2, $\sigma(\alpha) = \alpha\sigma$ e $\alpha \in \mathcal{U}(A[G])$. Conseqüentemente, $\sigma(\alpha^{-1}) = \alpha^{-1}\sigma^{-1}$ e $\beta \in \mathcal{U}(A[G])$. Além disso, $\tilde{\gamma}(\sigma^{-1}) = \sigma^{-t}$. Portanto, $\tilde{\gamma}^{-1}(\sigma^{-1}) = (\sigma^{-1})^{t^{-1}}$, e $\tilde{\gamma}^{-i}(\sigma^{-1}) = (\sigma^{-1})^{t^{-i}}$, para todo $1 \leq i \leq p-1$. Agora,

$$\begin{aligned}\sigma(\beta) &= \sigma\Big(\prod_{i=0}^{p-2} \tilde{\gamma}^{-i}(\alpha^{-1})^{t^i}\Big) = \prod_{i=0}^{p-2} \tilde{\gamma}^{-i}\Big(\sigma(\alpha^{-1})\Big)^{t^i} = \prod_{i=0}^{p-2} \tilde{\gamma}^{-i}(\alpha^{-1}\sigma^{-1})^{t^i} \\ &= \Big(\prod_{i=0}^{p-2} \tilde{\gamma}^{-i}(\alpha^{-1})^{t^i}\Big) \cdot \Big(\prod_{i=0}^{p-2} \tilde{\gamma}^{-i}(\sigma^{-1})^{t^i}\Big) = \beta \cdot \prod\Big((\sigma^{-1})^{t^{-i}}\Big)^{t^i} \\ &= \beta \cdot (\sigma^{-1})^{(p-1)} = \beta\sigma.\end{aligned}$$

Segue, novamente do Corolário 1.3.2, que $\{\beta_i\}_{i=0}^{p-1}$ é S-base normal de A. □

Finalizamos esta secção com o teorema, devido a L. Childs, que caracteriza quando A, uma extensão galoisiana de S com grupo de Galois cíclico de ordem prima p, possui uma S-base normal, no caso em que S contém ε, uma raiz p-ésima primitiva da unidade, com p regular em S. Faremos sua demonstração pois usaremos muitas vezes, no próximo capítulo, argumentos que são utilizados aqui. Para isso, seja $\lambda = \varepsilon - 1$ e denotamos por $\mathcal{U}_\lambda(A)$ o subgrupo das unidades de A do tipo $1 + \lambda x$, com $x \in A$. Precisamos do seguinte lema:

1.3.4. Lema

Sejam S anel comutativo com unidade, $p \in \mathbb{Z}$ primo, $\varepsilon \in S$ raiz p-ésima primitiva da unidade, A extensão galoisiana de S com grupo de Galois $G = \langle \sigma \mid \sigma^p = 1 \rangle$ que possui S-base normal e $A_j = \{x \in A \mid \sigma(x) = \varepsilon^j x\}$, para todo $0 \leq j \leq p-1$. Então, existe $z \in \mathcal{U}_\lambda(A)$ tal que $A_j = Sz^j$, para todo $0 \leq j \leq p-1$.

Demonstração : Seja $\alpha \in A$ tal que $\{\alpha_i = \sigma^i(\alpha)\}_{i=0}^{p-1}$ é S-base normal de A. Então, para qualquer $0 \leq j \leq p-1$, $A_j = Sz_j$, onde $z_j = \sum_{i=0}^{p-1} \varepsilon^{-ij}\alpha_i$. De fato: $\sigma(z_j) = \sum_{i=0}^{p-1} \varepsilon^{-ij}\alpha_{i+1} = \sum_{i=1}^{p} \varepsilon^{-(i-1)j}\alpha_i = \varepsilon^j \sum_{i=1}^{p} \varepsilon^{-ij}\alpha_i = \varepsilon^j z_j$, e portanto, $z_j \in A_j$. Assim, $Sz_j \subseteq A_j$, para qualquer $0 \leq j \leq p-1$. Reciprocamente, seja $a \in A_j$, $a = \sum_{i=0}^{p-1} s_i\alpha_i \in A$. Logo, $\sigma(a) = \sum_{i=0}^{p-1} s_i\alpha_{i+1} = \sum_{i=0}^{p-1} \varepsilon^j s_i\alpha_i$. Conseqüentemente, para todo $0 \leq i \leq p-2$, temos que $s_i = \varepsilon^j s_{i+1}$ e $s_{p-1} = \varepsilon^j s_0$, ou equivalentemente, $s_{i+1} = \varepsilon^{-j} s_i$, para qualquer $0 \leq i \leq p-2$, isto é,

$a = s_0\alpha + \varepsilon^{-j}s_0\sigma(\alpha) + \varepsilon^{-2j}s_0\sigma^2(\alpha) + \ldots + \varepsilon^{-ij}s_0\sigma^i(\alpha) + \ldots + \varepsilon^j s_0\sigma^{(p-1)}(\alpha)$

$= s_0\Big(\sum_{i=0}^{p-2} \varepsilon^{-ij}\sigma^i(\alpha) + \varepsilon^j\sigma^{(p-1)}(\alpha)\Big) = s_0 z_j \in Rz_j$, e $A_j = Sz_j$.

Como A é uma extensão galoisiana de S, $z_j \in \mathcal{U}(A)$, para todo $0 \leq j \leq p-1$. Isto segue das coordenadas de Galois: sejam $a_i; b_i$, $1 \leq i \leq n$ tais que $\sum_{i=1}^{n} a_i\sigma^{-j}(b_i) = \delta_{0j}$, para qualquer $0 \leq j \leq p-1$. Mas, para cada $1 \leq i \leq n$, existem $s_{i,k} \in S$ com $0 \leq k \leq p-1$ tais que $a_i = \sum_{k=0}^{p-1} s_{i,k}\alpha_k$. Então, $\delta_{0,j} = \sum_{i-1}^{n}\Big(\sum_{k=0}^{p-1} s_{i,k}\alpha_k\Big)\sigma^{-j}(b_i) = \sum_{k=0}^{p-1}\alpha_k\sigma^{-j}\Big(\sum_{i-1}^{n} s_{i,k}b_i\Big) = \sum_{k=0}^{p-1}\alpha_k\sigma^{-j}(\beta_k)$, onde $\beta_k = \sum_{i-1}^{n} s_{i,k}b_i$, para qualquer $0 \leq k \leq p-1$. Aplicando σ^j, para cada $0 \leq j \leq p-1$, $\delta_{0,j} = \sum_{k=0}^{p-1}\alpha_{k+j}\beta_k$. Assim,

$z_j(\sum_{k}^{p-1}\varepsilon^{kj}\beta_k) = (\sum_{k=0}^{p-1}\varepsilon^{-ij}\alpha_i)(\sum_{k=0}^{p-1}\varepsilon^{kj}\beta_k) = \sum_{l=0}^{p-1}\Big(\sum_{i=k+l}\alpha_i\beta_k\Big)\varepsilon^{-lj}$

$= \sum_{l=0}^{p-1}\Big(\sum_{k=0}^{p-1}\alpha_{k+l}\beta_k\Big)\varepsilon^{-lj} = \sum_{l=0}^{p-1}\delta_{0,l}\varepsilon^{-lj} = 1$, isto é, $z_j \in \mathcal{U}(A)$, para todo $0 \leq j \leq p-1$.

Agora, para cada $0 \leq j \leq p-1$, $\sigma(z_1^j) = \sigma(z_1)^j = (\varepsilon z_1)^j = \varepsilon^j z_1^j$, e então, $z_1^j \in A_j$. Logo, $Sz_1^j \subseteq A_j = Sz_j$. Conseqüentemente, existe $s_j \in S$ tal que $z_1^j = s_j z_j$. Como $z_k \in \mathcal{U}(A)$, para todo $0 \leq k \leq p-1$, $s_j \in \mathcal{U}(A)$. Mas,

$s_j^{-1} = z_1^{-j} z_j$, e portanto, $\sigma(s_j^{-1}) = \sigma(z_1^{-j})\sigma(z_j) = \varepsilon^{-j} z_1^{-j}\, \varepsilon^j z_j = z_1^{-j}\, z_j = s_j^{-1}$. Segue que $s_j^{-1} \in A^G = S$, ou seja, $z_j = s_j^{-1} z_1^j \in S z_1^j$, e concluímos que $A_j = S z_j = S z_1^j$. Resta verificar que $z = z_1 \in \mathcal{U}_\lambda(A)$, isto é, $z \equiv 1 (mod\, \lambda A)$. Temos $S z_0 = A_0 = A^G = S$, e então, $z_0 \in \mathcal{U}(S)$. Substituindo α por $z_0^{-1}\alpha$, podemos supor que $z_0 = 1$. Além disso, $z - z_0 = \sum_{i=1}^{p-1} (\varepsilon^{-i} - 1)\alpha_i = \sum_{i=1}^{p-1} \lambda(\varepsilon^{p-i-1} + \varepsilon^{p-i-2} + \ldots + \varepsilon + 1)\alpha_i$, ou, $z \equiv z_0 \equiv 1 (mod\, \lambda A)$. □

1.3.5. Teorema ([9], Theorem 2.5)

Sejam $p \in \mathbb{Z}$ primo, S um anel comutativo com unidade onde p é regular, $\varepsilon \in S$ raiz p-ésima primitiva da unidade. Seja A, uma extensão galoisiana de S com grupo de Galois G cíclico de ordem p e $G = \langle \sigma \rangle$. Então, as seguintes afirmações são equivalentes:

(i) *Existe $z \in \mathcal{U}_\lambda(A)$ tal que $\sigma(z) = \varepsilon z$.*

(ii) *Existe $x \in A$ tal que $A = S[x]$ e $\sigma(x) = \varepsilon x + 1$.*

(iii) *A possui S-base normal.*

Demonstração : $(i \Rightarrow ii)$ Como $z \in \mathcal{U}_\lambda(A)$, existe $x \in A$ tal que $z = 1 + \lambda x$. Agora, $\varepsilon z = \sigma(z) = 1 + \lambda\sigma(x)$, ou seja, $\varepsilon + \varepsilon\lambda x = 1 + \lambda\sigma(x)$, ou ainda, $\lambda\sigma(x) = (\varepsilon - 1) + \varepsilon\lambda x = \lambda(1 + \varepsilon x)$. Logo, $\lambda(\sigma(x) - 1 - \varepsilon x) = 0$. Mas $\lambda \in R^\times$, e portanto $\sigma(x) = 1 + \varepsilon x$. Mostremos que $A = S[x]$. Observemos que, para todo $1 \leq i \leq p-1$, $\varepsilon^i - 1 = (\varepsilon - 1)(\varepsilon^{i-1} + \ldots + \varepsilon + 1)$ e que $\sigma^i = \varepsilon^i x + (\varepsilon^{i-1} + \ldots + \varepsilon + 1)$. Assim, $\sigma^i(x) - x = (\varepsilon^i - 1)x + (\varepsilon^{i-1} + \ldots + \varepsilon + 1)$ $= (\varepsilon^{i-1} + \ldots + \varepsilon + 1)(1 + \lambda x) \in \mathcal{U}(A)$. Logo $\sigma^i(x) - x \notin \mathcal{M}$, para todo ideal

maximal $\mathcal{M}$ de $S[x]$. Por outro lado, $S \subseteq S[x]^G \subseteq A^G = S$. Segue que $S[x]$ é uma extensão galoisiana de S com grupo de Galois G (Teorema 1.1.1,v). Agora, como a inclusão $S[x] \hookrightarrow A$ comuta com a ação de G, temos que $S[x] = A$ (Corolário 1.1.4).

$(ii \Rightarrow i)$ Seja $z = 1 + \lambda x = \sigma(x) - x$. Então $\sigma(x) = x + z$. Logo, $\sigma(z) = 1 + \lambda\sigma(x) = 1 + \lambda(x + z) = (1 + \lambda x) + \lambda z = (1 + \lambda)z = \varepsilon z$. Resta ver que $z \in \mathcal{U}_\lambda(A)$. Suponhamos que exista $\mathcal{M}$ um ideal maximal de A tal que $z \in \mathcal{M}$. Assim, $z = (\sigma(x) - x) \in \mathcal{M}$. Conseqüentemente, $(\sigma(a) - a) \in \mathcal{M}$, para qualquer $a \in S[x] = A$ o que é uma contradição com o fato de A ser uma extensão galoisiana de S (Teorema 1.1.1,v). Logo $z \in \mathcal{U}(A)$, isto é, $z = 1 + \lambda x \in \mathcal{U}_\lambda(A)$.

$(iii \Rightarrow i)$ Decorre do lema 1.3.4: basta tomar $z = z_1$ no lema.

$(ii \Rightarrow iii)$ Seja $x \in A$ tal que $A = S[x]$ e $\sigma(x) = \varepsilon x + 1$, e consideremos $z = 1 + (\varepsilon - 1)x = 1 + \lambda x$. Pelo que vimos acima na parte $(ii \Rightarrow$ i) desta demonstração, $z \in \mathcal{U}_\lambda(A)$ e $\sigma(z) = \varepsilon z$. Então $\sigma(z^p) = \varepsilon^p z^p = z^p$, ou seja, $z^p \in S = A^G$. Portanto $z^p \in \left(\mathcal{U}_\lambda(A)\right)^p \cap S \subseteq \mathcal{U}_{\lambda^p}(A) \cap S = \mathcal{U}_{\lambda^p}(S)$.

Expandindo$(\lambda x + 1)^p - z^p = 0$ como um polinômio em x, temos que os coeficientes pertencem a $\lambda^p S$, ou seja, x é raiz de um polinômio, de grau p, mônico, em $\lambda^p S[X]$, ou ainda, existem $a_i \in S$, $0 \leq i \leq p - 1$, tais que $\lambda^p x^p + \lambda^p a_{p-1} x^{p-1} + \ldots + \lambda^p a_1 x + \lambda^p a_0 = 0$. Mas $\lambda^p \in S^\times$, logo x é raiz do polinômio mônico $f(X) = \sum_{i=0}^{p} a_i X^i \in S[X]$.

Do fato de f ser mônico, segue que para cada $g \in S[X]$, existem $q, r \in S[X]$ tais que $g = fq + r$ com $r = 0$ ou $\partial(r) < p = \partial(f)$. Assim, $g(x) = f(x)q(x) + r(x) = r(x)$, para qualquer $g \in S[X]$, e portanto, $A = S[x] =$

$\sum_{i=1}^{p-1} Sx^i$. Consideremos o seguinte epimorfismo de anéis $\pi : S[X] \longrightarrow S[x] = A$ definido por $\pi(g) = g(x)$. Claramente, $f(X) \in Ker(\pi)$, e portanto, existe um epimorfismo de anéis $\overline{\pi} : \dfrac{S[X]}{< f(X) >} \longrightarrow S[x] = A$ dado por $\overline{\pi}(\overline{g}) = g(x)$.

Por outro lado, $B = \dfrac{S[X]}{< f(X) >}$ é um S-módulo livre de posto constante $p = \partial(f)$ com base $\{\overline{1}, \overline{X}, \ldots, \overline{X}^{p-1}\}$, e A também é S-módulo projetivo de posto $p =\mid G \mid$ ([6], Lemma 4.1). Então, $\overline{\pi}$ é um isomorfismo de anéis ([27], I.2.4). Conseqüentemente, $\{1, x, \ldots, x^{p-1}\}$ é uma S-base de A. Logo, a soma $A = S[x] = \sum_{i=1}^{p-1} Sx^i$ é direta.

Segue da observação feita logo após o Lema 1.2.1 que, $\displaystyle\sum_{i=0}^{p-1} z^i = \prod_{i=1}^{p-1}(z - \varepsilon^i)$. Além disso, $(z - \varepsilon^i) \equiv z - 1 \equiv 0(mod \lambda A)$. De fato : $z - \varepsilon^i = (1 - \varepsilon^i) + \lambda x = \lambda s + \lambda x = \lambda(s + x) \in \lambda A$, para certo $s \in S$. Então,

$\displaystyle\sum_{i=0}^{p-1} z^i = \prod_{i=1}^{p-1}(z - \varepsilon^i) \in \lambda^{p-1} A = pA$ (Corolário 1.2.4). Seja $\beta \in A$ satisfazendo

$\displaystyle\sum_{i=0}^{p-1} z^i = p\beta$. Temos que β é único, pois p é regular em A. Resta verificar que β gera uma S-base normal para A. Sejam

$$\overline{\beta} = \begin{pmatrix} \beta \\ \sigma\beta \\ \vdots \\ \sigma^{p-1}\beta \end{pmatrix}, \quad \overline{z} = \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{p-1} \end{pmatrix} \quad \text{e} \quad \overline{x} = \begin{pmatrix} 1 \\ x \\ \vdots \\ x^{p-1} \end{pmatrix}. \text{ Então, } \overline{\beta} = M\overline{x}$$

para única matriz $M \in \mathfrak{M}_{p\times p}(S)$, pois $\{x^i\}_{i=0}^{p-1}$ é uma S-base de A. Também, temos que $p\sigma^i(\beta) = \sum_{j=0}^{p-1} \varepsilon^{ij} z^j$ e $z^i = \sum_{j=0}^{i} \binom{i}{j} \lambda^i x^j$. Então segue que $p\overline{\beta} = D\overline{z}$ e $\overline{z} = E\overline{x}$, onde $D, E \in \mathfrak{M}_{p\times p}(S)$ com $pM = DE$,

$det(D) = \eta\lambda^{\frac{p(p-1)}{2}}$ com $\eta \in \mathcal{U}(S)$ e $det(E) = \lambda^{\frac{p(p-1)}{2}}$. Conseqüentemente, $p^p det(M) = det(pM) = det(D)det(E) = \eta\lambda^{p(p-1)}$ e, como $p = \lambda^{p-1}s$ para algum $s \in S$ (Corolário 1.2.4), obtemos que $\lambda^{p(p-1)}s^p det(M) = \eta\lambda^{p(p-1)}$, ou seja, $s^p det(M) = \eta$. Segue que M é invertível. Então, já que $\{x^i\}_{i=0}^{p-1}$ é uma S-base de A, concluímos que $\{\sigma^i(\beta)\}_{i=0}^{p-1}$ também é. O teorema está demonstrado. □

1.4 Extensões abelianas: o grupo de Harrison

Seja $T(G;R)$ o conjunto das classes de isomorfismos das extensões galoisianas de R com mesmo grupo de Galois G. Denotamos a classe de uma extensão A por $[A]$ e lembramos que, se G for abeliano, $T(G;R)$ é um grupo multiplicativo (grupo de Harrison de G sobre R), com o produto definido por $[A] * [B] = [(A \otimes_R B)^{\delta G}]$, onde $\delta G = \{\sigma \otimes \sigma^{-1} \mid \sigma \in G\}$. A ação de G sobre $(A \otimes_R B)^{\delta G}$ é via primeira coordenada, que coincide com a ação dada na segunda coordenada. O elemento identidade de $T(G;R)$ é representado por $e_G(R) = \underset{\sigma\in G}{\oplus} Rv_\sigma$. Segue do Lema 1.1.5, que $[A] = [e_G(R)]$ se, e somente se, existe um homomorfismo de R-álgebras de A em R. Para cada $[A] \in T(G;R)$, temos que $[A]^{-1}$ é representado pela própria extensão A, com a ação de G dada por $\sigma : a \mapsto \sigma^{-1}(a)$, $a \in A$, $\sigma \in G$.

Quando $G \approx \dfrac{\mathbb{Z}}{n\mathbb{Z}}$, escrevemos $T_n(R)$ para denotar o grupo de Harrison. Se o grupo G for cíclico, a ação de G sobre A é completamente determinada pela ação de um gerador. Assim, se $G = \langle \sigma \mid \sigma^p = id \rangle$, denotamos a classe de A, em $T_p(R)$, por $[A, \sigma]$. Por exemplo, é fácil ver que $[e_G(R)] = [R^{|G|}; \tau]$,

onde a ação de τ é dada por $\tau(r_1, \ldots, r_{|G|}) = (r_{|G|}, r_1, \ldots, r_{|G|-1})$.

Segue de ([36] Théorème 1.1) que $[A, \sigma^k] = [A, \sigma^{k^{-1} \pmod p}]$, para todo $k \not\equiv 0 \pmod p$. Conseqüentemente, todo elemento não trivial de $T_p(R)$ tem ordem p, ou seja, T_p é de p-torsão (novamente por[36] Théorème 1.1).

Denotamos por $H(G;R)$ o subgrupo de $T(G;R)$ formado pelas classes $[A] \in T(G;R)$ que possuem R-base normal. Para o caso em que G é cíclico de ordem prima p, denotamos $H(G;R)$ por $H_p(R)$.

Para dar uma descrição do grupo das extensões cíclicas de grau p de R que possuem uma R-base normal, no caso em que p é um primo ímpar regular e R possui uma raiz p-ésima primitiva da unidade, o grupo $\mathcal{U}_\lambda(R)$, com $\lambda = \varepsilon - 1$, desempenha o papel correspondente do grupo das unidades $\mathcal{U}(R)$ na Teoria de Kummer, onde temos p invertível. Isso fica evidente no teorema, devido a L. Childs, que mostramos abaixo. Outra vez vamos incluir a demonstração pois, no próximo capítulo, usaremos muitas vezes argumentos contidos aqui.

1.4.1. Teorema ([9], Theorem 2.4)

Sejam p primo ímpar regular em R e G um grupo cíclico de ordem p. Suponhamos que R possui ε, uma raiz p-ésima primitiva da unidade. Então, os grupos $H_p(R) = H(G;R)$ *e* $\dfrac{\mathcal{U}_{\lambda^p}(R)}{\left(\mathcal{U}_\lambda(R)\right)^p}$ *são isomorfos.*

O isomorfismo citado no Teorema acima associa, a cada classe $\overline{a} \in \dfrac{\mathcal{U}_{\lambda^p}(R)}{\left(\mathcal{U}_\lambda(R)\right)^p}$, a classe $[A] \in H_p(R)$, onde $A = \dfrac{R[X]}{\langle f(X) \rangle}$ com

$f(X) \in R[X]$ mônico dado pela equação (ver Corolário 1.2.5)

$$\Big(\lambda X + 1\Big)^p - a = \lambda^p f(X).$$

Demonstração : Sejam $G =< \sigma >$, A uma extensão galoisiana de R com grupo de Galois G tal que $[A] \in H(G;R)$ e $G_p(R) = \dfrac{\mathcal{U}_{\lambda^p}(R)}{\Big(\mathcal{U}_\lambda(R)\Big)^p}$.

Segue do Teorema 1.3.5 que existe $z = 1+\lambda x \in \mathcal{U}_\lambda(A)$ satisfazendo $\sigma(z) = \varepsilon z$. Agora, pela demonstração do mesmo Teorema 1.3.5, $z^p \in \mathcal{U}_{\lambda^p}(R)$. Então, definimos $\varphi : H(G;R) \longrightarrow G_p(R)$ por $\varphi([A]) = \overline{z^p}$, e mostremos que φ é um isomorfismo de grupos.

Sejam $[A] = [A'] \in H(G;R)$ e $f : A \longrightarrow A'$ um isomorfismo de extensões de Galois. Pelo Teorema 1.3.5 existem $z \in \mathcal{U}_\lambda(A)$ e $z' \in \mathcal{U}_\lambda(A')$ stisfazendo $\sigma(z) = \varepsilon z$ e $\sigma(z') = \varepsilon z'$. Seja $z'' \in A$ tal que $f(z'') = z'$. Logo $\sigma(z'') = \sigma(f^{-1}(z')) = f^{-1}(\sigma(z')) = f^{-1}(\varepsilon z') = \varepsilon f^{-1}(z') = \varepsilon z''$ e conseqüentemente $\sigma(z''z^{-1}) = z''z^{-1}$, isto é, $z''z^{-1} \in A^G = R$. Seja $u \in R$ com $z'' = uz$. Assim, $u \in \mathcal{U}_\lambda(A) \cap R = \mathcal{U}_\lambda(R)$, $(z'')^p \in R$ e $\overline{(z'')^p} = \overline{u^p z^p} = \overline{z^p}$. Agora, podemos supor que $f(z) = z'$, pois $uf : A \longrightarrow A'$ dada por $uf(x) = f(ux)$ para cada $x \in A$, também é um isomorfismo de extensões de Galois. Então, $\varphi([A']) = \overline{(z')^p} = \overline{f(z)^p} = \overline{f(z^p)} = \overline{z^p} = \varphi([A])$. É fácil ver que a definição de φ independe da escolha de z. De fato, suponhamos que exista $z'' \in A$ tal que $\sigma(z'') = \varepsilon z''$. Como acima, existe $u \in \mathcal{U}_\lambda(R)$ satisfazendo $z'' = uz$ e $\overline{(z'')^p} = \overline{(z')^p}$ em $G_p(R)$. Segue que φ está bem definida.

Sejam $[A_1], [A_2] \in H(G;R)$ e $[A_3] = [A_1][A_2] = \Big[\big(A_1 \otimes_R A_2\big)^{<\sigma\otimes\sigma^{-1}>}\Big]$. Pelo Teorema 1.3.5, existem $z_i \in \mathcal{U}_\lambda(A_i)$, i=1 e 2, tais que $\sigma(z_i) = \varepsilon z_i$ e

$z_i^p \in \Big(\mathcal{U}_\lambda(R)\Big)^p$. Tomamos $z_3 = z_1 \otimes z_2 \in \mathcal{U}_\lambda(A_1 \otimes_R A_2)$. Então, $(\sigma \otimes 1)z_3 = \sigma(z_1) \otimes z_2 = \varepsilon z_3$ e $(1 \otimes \sigma)z_3 = \varepsilon z_3$ em A_3. Logo, $z_3 \in \mathcal{U}_\lambda(A_1 \otimes_R A_2) \cap A_3 = \mathcal{U}_\lambda(A_3)$ e $\sigma(z_3) = \varepsilon z_3$. Consideremos $R \overset{\mu}{\approx} R \otimes_R R \subseteq A_1 \otimes_R A_2$. Temos:

$z_3^p = z_1^p \otimes z_2^p \overset{\mu}{=} z_1^p z_2^p$, ou seja, $\varphi([A_3]) = \overline{z_3} = \overline{z_1}\,\overline{z_2} = \varphi(z_1)\,\varphi(z_2)$. Isto mostra que φ é um homomorfismo de grupos.

Seja $[A] \in H(G;R)$ com $\varphi([A]) = \overline{1}$, isto é, $z^p = u^p$, onde $z \in \mathcal{U}_\lambda(A)$ é dado pelo teorema 1.3.5, e $u \in \mathcal{U}_\lambda(R)$. Então, $\Big(u^{-1}z\Big)^p = 1$ e $\sigma(u^{-1}z) = \varepsilon(u^{-1}z)$. Conseqüentemente, podemos assumir que $z^p = 1$.

Seja $x \in A$ tal que $z = 1 + \lambda x$. Segue da demonstração do teorema 1.3.5, que $A = R[x]$ e $\sigma(x) = \varepsilon x + 1$. Por outro lado, $z^p - 1 = \Big(\lambda x + 1\Big)^p - 1 = \lambda^p f(x) = 0$, onde $f(X)$ é um polinômio mônico de grau p e com termo constante nulo. Mas $\lambda \in R^\times$, e assim, $f(x) = 0$ e $A = R[x] \approx \dfrac{R[X]}{\langle f(X)\rangle}$.

Seja $h : R[X] \longrightarrow R$ dado por $h(g) = g(0)$. Claramente h é um homomorfismo de anéis. Segue, já que $\langle f(X)\rangle \subseteq Ker(h)$, do teorema do homomorfismo, que existe um homomorfismo de anéis $\overline{h} : \dfrac{R[X]}{\langle f(X)\rangle} \longrightarrow R$, tal que $\overline{h}(\overline{g}) = h(g) = g(0)$. Pelo Lema 1.1.5, $[A] = e_G(R)$, isto é, φ é injetor.

Finalmente, mostremos que φ é sobrejetor. Seja $a \in \mathcal{U}_{\lambda^p}(R)$. Então, $\Big(\lambda X + 1\Big)^p - a = \lambda^p f(X)$ com $f(X) \in R[X]$ mônico (Corolário 1.2.5). Seja $A = \dfrac{R[X]}{\langle f(X)\rangle} = R[x]$, onde $x = \overline{X} = x + \langle f(X)\rangle$. Logo, $f(x) = 0$. Definimos a ação de $G =< \sigma >$ sobre A via $\sigma(x) = \varepsilon x + 1$. Como $\lambda(\varepsilon x + 1) + 1 = \varepsilon(\lambda x + 1)$ obtemos que $\lambda^p f(\varepsilon x + 1) = \Big(\varepsilon(\lambda x + 1)\Big)^p - a = \varepsilon^p(\lambda x + 1)^p - a = \lambda^p f(x) = 0$. Assim, $f(\sigma(x)) = f(\varepsilon x + 1) = 0$, e a ação de G sobre A está bem definida.

Precisamos mostrar ainda que A é uma extensão galoisiana de R com

grupo de Galois $G =< \sigma >$. Seja $\sum_{i=0}^{p-1} a_i x^i \in A^G$. Então,

$$\sum_{i=0}^{p-1} a_i x^i = \sum_{i=0}^{p-1} a_i \sigma(x^i) = \sum_{i=0}^{p-1} a_i \Big(\sigma(x)\Big)^i = \sum_{i=0}^{p-1} a_i \Big(\varepsilon\Big)^i = \sum_{i=0}^{p-1} a_i \Big(\sum_{j=0}^{i} \binom{i}{j} \varepsilon^i x^i\Big).$$

Comparando os coeficientes de x_i, vemos que:

se $i = p-1$, então $a_{p-1} = a_{p-1}\varepsilon^{p-1}$, e portanto $a_{p-1} = 0$.

se $i = p-2$, então $a_{p-2} = a_{p-2}\varepsilon^{p-2}$, e portanto $a_{p-2} = 0$.

Continuando este processo, concluímos que $a_{p-1} = a_{p-2} = \ldots = a_1 = 0$ e $a_0 \in R$, ou seja, $A^G \subseteq R$. Logo $A^G = R$.

Por outro lado, $\sigma(x) - x = \varepsilon x + 1 - x = (\varepsilon - 1)x + 1 = \lambda x + 1 = z$, com $z^p = a \in \mathcal{U}_\lambda(R)$. Então $z = (\sigma(x) - x) \in \mathcal{U}_\lambda(A)$. Pelo Teorema 1.1.1 segue que A é uma extensão galoisiana de R com grupo de Galois G. Por construção, $\varphi([A]) = \overline{z^p} = \overline{a}$, isto é, φ é sobrejetor. O teorema está demonstrado. □

A seguir, apresentamos a seqüência exata de L.Childs (construída em [9]). Como no teorema acima, sejam p um primo ímpar e regular em R, G um grupo cíclico de ordem p e $\varepsilon \in R$ raiz p-ésima primitiva da unidade.

Denotamos por $Pic(R)$ o grupo de Picard das classes $\overline{P}$ de isomorfismos dos R-módulos projetivos de posto constante 1, e por $Pic_p(R)$ o subgrupo de p-torsão. Observemos que, se G for um grupo abeliano, toda extensão galoisiana de R com grupo de Galois G é um $R[G]$-módulo projetivo de posto constante 1 [34]. Seja $\pi : T_p(R) \longrightarrow Pic(R[G])$ definida por $\pi([A]) = \overline{A}$ a aplicação canônica. Na realidade, π é um homomorfismo de grupos abelianos [14]. Claramente o núcleo de π é $H_p(R)$. Em [9], L. Childs mostrou que a

imagem de π é $PrimPic_p(R[G])$, o subgrupo dos elementos primitivos de p-torsão de $Pic(R[G])$, isto é, o subgrupo formados pelos elementos $P \in Pic(R[G])$, de p-torsão, tais que $P \otimes_R P \approx R[G \times G] \otimes^{\Delta}_{R[G]} P$ como $R[G \times G]$-módulos, onde $\Delta : R[G] \longrightarrow R[G \times G]$ é o homomorfismo de R-álgebras induzido por $\Delta(\sigma) = (\sigma, \sigma)$, para qualquer $\sigma \in G$.

Decorre daí, e do Teor 1.4.1 que a seqüência de L. Childs

$$1 \longrightarrow G_p(R) \xrightarrow{j} T_p(R) \xrightarrow{\pi} PrimPic_p(R[G]) \longrightarrow 1,$$

é exata, onde $G_p(R) = \dfrac{\mathcal{U}_{\lambda^p}(R)}{\left(\mathcal{U}_{\lambda}(R)\right)^p}$, $j(\overline{a}) = \left[\dfrac{R[X]}{\langle f(X)\rangle}; \sigma(x) = \varepsilon x + 1\right]$ para qualquer $\overline{a} \in G_p(R)$, com $x = X + \langle f(X)\rangle$, $\lambda = \varepsilon - 1$ e $f \in R[X]$ mônico dado pela equação $(\lambda X + 1)^p - a = \lambda^p f(X)$ (Corolário 1.2.5). É com esta seqüência que vamos trabalhar no próximo capítulo, para dar uma descrição dos grupos $T_p(R)$, $H_p(R)$ e $PrimPic_p(R[G])$, no caso em que p é um primo ímpar regular e R não possui uma raiz p-ésima primitiva da unidade.

1.5 Cohomologia galoisiana

O nosso objetivo nesta seção é a construção de uma determinada seqüência exata de grupos, de quatro termos, de forma análoga àquela construída por S. U. Chase, D. K. Harrison e A. Rosenberg em [6], Corollary 5.5 (ver também [11], Theorem IV.1.1). Faremos uso dessa seqüência e dos principais resultados deste trabalho, os quais serão tratados no próximo capítulo, para construir o isomorfismo $PrimPic_p(R[G]) \approx PrimPic_p(S[G])^{\Gamma}$ (ver secção 2.4).

Começamos considerando uma R-álgebra S e $\Gamma \subset Aut_R(S)$ um grupo finito de R-automorfismos de S. Sejam

$$Z^1(\Gamma, \mathcal{U}(S)) = \{ f : \Gamma \to \mathcal{U}(S) \mid f(\gamma\gamma') = f(\gamma)\gamma(f(\gamma')), \text{ para quaisquer } \gamma, \gamma' \in \Gamma\}$$

$$B^1(\Gamma, \mathcal{U}(S)) = \{ f \in Z^1(\Gamma, \mathcal{U}(S)) \mid \text{existe } u \in \mathcal{U}(S) \text{ tal que } f(\gamma) = \gamma(u)u^{-1} \text{ para qualquer } \gamma \in \Gamma\}$$

$$Z^2(\Gamma, \mathcal{U}(S)) = \{ f : \Gamma \times \Gamma \to \mathcal{U}(S) \mid f(\gamma\gamma', \gamma'')f(\gamma, \gamma') = f(\gamma, \gamma'\gamma'')\gamma(f(\gamma', \gamma'')), \text{ para quaisquer } \gamma, \gamma', \gamma'' \in \Gamma\}$$

$$B^2(\Gamma, \mathcal{U}(S)) = \{ f \in Z^2(\Gamma, \mathcal{U}(S)) \mid \text{existe } g : \Gamma \to \mathcal{U}(S) \text{ tal que } f(\gamma, \gamma') = g(\gamma\gamma')(g(\gamma)\gamma(g(\gamma')))^{-1}, \text{ para quaisquer } \gamma, \gamma' \in \Gamma\}.$$

Observemos que $Z^i(\Gamma, \mathcal{U}(S))$ é um grupo abeliano com a multiplicação pontual e $B^i(\Gamma, \mathcal{U}(S))$ é um subgrupo de $Z^i(\Gamma, \mathcal{U}(S))$, $i = 1, 2$. Seja $H^i(\Gamma, \mathcal{U}(S)) = Z^i(\Gamma, \mathcal{U}(S))/B^i(\Gamma, \mathcal{U}(S))$ o i-ésimo grupo de cohomologia de Γ com coeficientes em $\mathcal{U}(S)$, $i = 1, 2$. Se $f \in Z^i(\Gamma, \mathcal{U}(S))$ denotamos por $[f]$ a classe que f representa em $H^i(\Gamma, \mathcal{U}(S))$. Como antes, $Pic(R)$ (resp. $Pic(S)$) denota o grupo das classes de isomorfismo dos R (resp. S)-módulos projetivos de posto constante 1. Consideremos a ação de Γ sobre $Pic(S)$ dada por $\gamma \cdot \overline{P} = \overline{{}_\gamma P}$, onde ${}_\gamma P = P$ como grupos aditivos e $s \cdot x = \gamma(s)x$, para todo $s \in S$ e $x \in {}_\gamma P$. Denotamos por $Pic(S)^\Gamma$ o subgrupo dos elementos estáveis pela ação de Γ, isto é, o subgrupo dos elementos $\overline{P}$ de $Pic(S)$ tais que $\gamma \cdot \overline{P} = \overline{P}$, para todo $\gamma \in \Gamma$.

Agora já podemos enunciar o principal resultado desta seção.

1.5.1. Teorema

Sejam S uma R-álgebra fielmente projetiva e $\Gamma \subset Aut_R(S)$ um grupo finito de R-automorfismos de S tal que $S^\Gamma = R$. Suponhamos que exista $c \in S$ tal que $tr(c) = \sum_{\gamma\in\Gamma} \gamma(c) = 1$. Então existem homomorfismos naturais η_i para os quais a seqüência de grupos abaixo é exata:

$$1 \longrightarrow H^1(\Gamma, \mathcal{U}(S)) \xrightarrow{\eta_1} Pic(R) \xrightarrow{\eta_2} Pic(S)^\Gamma \xrightarrow{\eta_3} H^2(\Gamma, \mathcal{U}(S))$$

Para a demonstração desse teorema necessitamos de alguns resultados auxiliares. Para a demonstração desses resultados estaremos assumindo, na medida que for necessário, a existência do elemento $c \in S$ tal que $tr(c) = 1$ e o fato de S ser um R-módulo fiel e projetivo finitamente gerado.

Seja $D = \{ \sum_{\gamma\in\Gamma} \lambda_\gamma \gamma \,|\, \lambda_\gamma \in S\}$. É imediato que $D \subseteq \mathcal{E}nd_R(S)$ como subanel. Seja $T_S = tr(S\_) \subseteq D$, o S-submódulo à esquerda de D formado pelos elementos da forma $tr(s\_) = \sum_{\gamma\in\Gamma} \gamma \cdot (s\_)$, para todo $s \in S$. Claramente T_S é também um D-módulo à direita via a ação $tr(s'\_) \cdot s\gamma = tr(s's\gamma\_) = \sum_{\gamma'\in\Gamma} \gamma'(s's)\gamma'\gamma = \sum_{\rho\in\Gamma} \rho(\gamma^{-1}(s's))\rho = tr(\gamma^{-1}(s's)\_)$, para todo $s' \in S$ e $s\gamma \in D$.

Dado um D-módulo à esquerda M denotamos por M^Γ o R-submódulo de M estável pela ação de Γ, isto é, o R-submódulo de M formado pelos elementos $m \in M$ tais que $\gamma \cdot m = m$, para todo $\gamma \in \Gamma$. É imediato que $tr \cdot M \subseteq M^\Gamma$, onde $tr = \sum_{\gamma\Gamma} \gamma \in D$. Isto permite definir o homomorfismo de R-módulos $\varphi : T_S \otimes_D M \to M^\Gamma$, induzido por $\varphi(tr(s\_) \otimes m) = tr \cdot sm = \sum_{\gamma\in\Gamma} \gamma \cdot sm$ onde $s \in S$ e $m \in M$.

1.5.2. Lema

φ é um isomorfismo de R-módulos.

Demonstração : Claramente φ é sobrejetor pois $\varphi(tr(c\_)\otimes m) = tr\cdot cm = tr(c)m = m$, para todo $m \in M^{\Gamma}$, onde $c \in S$ é tal que $tr(c) = 1$. Como $tr(s\_)\otimes m = 1\otimes tr(s\_)\cdot m = 1\otimes tr\cdot sm = 1\otimes\varphi(tr(s\_)\otimes m)$, para quaisquer $s \in S$ e $m \in M$, segue que φ é injetor. □

Tomando $M = S$ no lema anterior, obtemos o

1.5.3. Corolário

$T_S \otimes_D S \approx S^{\Gamma} = R$ como R-módulos.

1.5.4. Lema

A aplicação $\psi : S \otimes_R T_S \to D$, induzida por $\psi(s' \otimes tr(s\_)) = s'tr(s\_)$, é um monomorfismo de S-módulos.

Demonstração : Claramente ψ é um homomorfismo de S-módulos. Para mostrar que ψ é injetor, usaremos o fato de que S é um R-módulo projetivo finitamente gerado. Neste caso existem $s_j \in S$ e $g_j \in \mathcal{H}om_R(S, R)$, $1 \leq j \leq n$, tais que $\sum_{j=1}^{n} g_j(s)s_j = s$, para todo $s \in S$. Logo, se

$\alpha = \sum_{i=1}^{m} s_i' \otimes tr((s_i)\_)$ está no núcleo de ψ então $\sum_{i=1}^{m} s_i'tr((s_i)\_) = 0$ e temos

$$\alpha = \sum_{i=1}^{m} s_i' \otimes tr((s_i)\_) = \sum_{i=1}^{m}\sum_{j=1}^{n} g_j(s_i')s_j \otimes tr((s_i)\_)$$

$$= \sum_{j=1}^{n} s_j \otimes \sum_{i=1}^{m} g_j(s_i')tr((s_i)\_) = \sum_{j=1}^{n} s_j \otimes g_j\Big(\sum_{i=1}^{m} s_i'tr((s_i)\_)\Big) = 0. \qquad \square$$

1.5.5. Lema

Seja M um D-módulo à esquerda plano. Então a aplicação

$$\mu : S \otimes_R M^\Gamma \to M, \quad \textit{induzida por } \mu(s \otimes m) = sm,$$

é um isomorfismo de D-módulos à esquerda.

Demonstração : É imediato que μ é um epimorfismo de D-módulos . Desde que M é plano, decorre do Lema 1.5.4 que $\psi \otimes 1 : (S \otimes_R T_S) \otimes_D M \to D \otimes_D M$ é um monomorfismo de S-módulos. Logo, a injetividade de μ decorre do fato de μ poder ser visto como a composição dos seguintes monomorfismos de S-módulos:

$$S \otimes_R M^\Gamma \approx S \otimes_R (T_S \otimes_D M) \approx (S \otimes_R T_S) \otimes_D M \xrightarrow{\psi \otimes 1} D \otimes_D M \approx M$$

com os monomorfismos acima induzidos por

$$s \otimes m \mapsto s \otimes (tr(c\_) \otimes m) \mapsto (s \otimes tr(c\_)) \otimes m \mapsto s\,tr(c\_) \otimes m \mapsto s\,tr(c\_) \cdot m$$

$= s\,tr \cdot cm = s\,tr(c)sm$, onde $c \in S$ é tal que $tr(c) = 1$. □

1.5.6. Lema

Todo $f \in Z^1(\Gamma, \mathcal{U}(S))$ define um S-automorfismo $\theta_f : D \to D$ tal que $\theta_f(\sum_{\gamma \in \Gamma} s_\gamma \gamma) = \sum_{\gamma \in \Gamma} s_\gamma f(\gamma)\gamma$.

Demonstração : Claramente θ_f é um homomorfismo de S-módulos e $\theta_f((s\gamma)(s'\gamma')) = \theta_f(s\gamma(s')\gamma\gamma') = s\gamma(s')f(\gamma\gamma')\gamma\gamma' = s\gamma(s')f(\gamma)\gamma(f(\gamma'))\gamma\gamma'$ $= (sf(\gamma)\gamma)(s'f(\gamma')\gamma') = \theta_f(s\gamma)\theta_f(s'\gamma')$, para quaisquer $s, s' \in S$ e $\gamma, \gamma' \in \Gamma$. Logo θ_f é um homomorfismo de S-álgebras. Além disso, para todo $s\gamma \in D$ temos $\theta_f(sf(\gamma)^{-1}\gamma) = sf(\gamma)^{-1}f(\gamma)\gamma = s\gamma$, ou seja, θ_f é sobrejetor. Como D é um R-módulo finitamente gerado, pois S o é, então θ_f é um isomorfismo

([27], I.2.4). □

1.5.7. Lema

A aplicação $\theta : Z^1(\Gamma, \mathcal{U}(S)) \to Aut_S(D)$, *dada por* $\theta(f) = \theta_f$, *é um monomorfismo de grupos.*

Demonstração : Para quaisquer $f, g \in Z^1(\Gamma, \mathcal{U}(S))$ e para todo $s\gamma \in D$ $\theta_{fg}(s\gamma) = s(fg)(\gamma)\gamma = sf(\gamma)g(\gamma)\gamma = sg(\gamma)f(\gamma)\gamma = \theta_f(sg(\gamma)\gamma) = \theta_f\theta_g(s\gamma)$, ou seja, $\theta(fg) = \theta_{fg} = \theta_f\theta_g = \theta(f)\theta(g)$, e portanto θ é um homomorfismo de grupos. Agora, se $\theta(f) = 1$, então $f(\gamma)\gamma = \theta_f(\gamma) = \gamma$ e, em particular, $f(\gamma) = f(\gamma)\gamma(1) = \gamma(1) = 1$, para qualquer $\gamma \in \Gamma$. Logo $f = 1$, isto é, θ é injetor. □

1.5.8. Lema

Para qualquer $f \in B^1(\Gamma, \mathcal{U}(S))$, $\theta(f)$ *é um automorfismo interno de* D.

Demonstração : Seja $f \in B^1(\Gamma, \mathcal{U}(S))$. Então, existe $u \in \mathcal{U}(S)$ tal que $f(\gamma) = u^{-1}\gamma(u)$ para todo $\gamma \in \Gamma$. Logo,
$\theta_f(s\gamma) = sf(\gamma)\gamma = su^{-1}\gamma(u)\gamma = u^{-1}(s\gamma)u$, para todo $s\gamma \in D$. □

Para cada $f \in Z^1(\Gamma, \mathcal{U}(S))$ denotamos por S_f o D-módulo à esquerda S dado pela ação $s\gamma \cdot x = \theta_f(s\gamma) \cdot x = sf(\gamma)\gamma \cdot x = sf(\gamma)\gamma(x)$, para quaisquer $x \in S_f$ e $s\gamma \in D$.

1.5.9. Lema

S_f é um D-módulo à esquerda projetivo finitamente gerado.

Demonstração : Pelo Lema 1.5.2 existem $s'_j \in S_f$ e $t_j = tr((s_j)_-) \in T_S$, $1 \leq j \leq n$, tais que $\sum_{j=1}^{n} t_j(s'_j) = 1$. Para cada $1 \leq j \leq n$ seja $t'_j : S_f \to D$ a aplicação dada por $t'_j : s \mapsto st_j$. Claramente, t'_j é um homomorfismo de R-módulos. Além disso, observemos que $t'_j(s'\gamma \cdot s)(x) = (s'\gamma \cdot s)t_j(x) = s'\gamma \cdot (st_j(x)) = (s'\gamma \cdot st_j)(x)$, para todo $x \in S_f$. Portanto $t'_j(s'\gamma \cdot s) = s'\gamma \cdot st_j = s'\gamma \cdot t'_j(s)$, para quaisquer $s \in S_f$ e $s'\gamma \in D$. Logo $t'_j \in \mathcal{H}om_D(S_f, D)$ e temos $s = 1s = \sum_{j=1}^{n} t_j(s'_j)s = \sum_{j=1}^{n} st_j(s'_j) = \sum_{j=1}^{n} t'_j(s) \cdot s'_j$, para todo $s \in S_f$, o que demonstra a afirmação do lema. □

O corolário a seguir é uma conseqüência imediata dos Lemas 1.5.5 e 1.5.9.

1.5.10. Corolário

$S \otimes_R S_f^{\Gamma} \approx S_f$, como D-módulos à esquerda.

Demonstração do Teorema 1.5.1: A demonstração deste teorema será feita em seis etapas.

Etapa 1: a definição de η_1

Observemos que S_f^{Γ} é um R-módulo projetivo de posto constante 1. De fato, note que $S_f = S$ como R-módulos e S é R-módulo fiel e projetivo finitamente gerado. A afirmação agora decorre, via localização, do Corolário 1.5.10 e do ([27] Lemme I.6.2). Isto permite definir uma aplicação $\eta : Z^1(\Gamma, \mathcal{U}(S)) \to Pic(R)$ dada por $\eta(f) = \overline{S_f^{\Gamma}}$. Mostremos inicialmente que η é um homomorfismo de grupos. De fato, dados $f, g \in Z^1(\Gamma, \mathcal{U}(S))$ temos a seguinte seqüência de S-isomorfismos

$$S \otimes_R (S_f^\Gamma \otimes_R S_g^\Gamma) \approx (S \otimes_R S_f^\Gamma) \otimes_S (S \otimes_R S_g^\Gamma) \approx S_f \otimes_S S_g \approx S_{fg} \approx S \otimes_R S_{fg}^\Gamma$$

cuja composição é um D-isomorfismo. Logo,

$$T_S \otimes_D (S \otimes_R (S_f^\Gamma \otimes_R S_g^\Gamma)) \approx T_S \otimes_D (S \otimes_R S_{fg}^\Gamma) \quad \text{de onde segue que}$$

$$(T_S \otimes_D S) \otimes_R (S_f^\Gamma \otimes_R S_g^\Gamma) \approx (T_S \otimes_D S) \otimes_R S_{fg}^\Gamma \quad \text{e portanto}$$

$$S_f^\Gamma \otimes_R S_g^\Gamma \approx R \otimes_R (S_f^\Gamma \otimes_R S_g^\Gamma) \approx R \otimes_R S_{fg}^\Gamma \approx S_{fg}^\Gamma \quad \text{ou seja,}$$

$$\eta(fg) = \overline{S_{fg}^\Gamma} = \overline{S_f^\Gamma \otimes_R S_g^\Gamma} = \overline{S_f^\Gamma}\,\overline{S_g^\Gamma} = \eta(f)\eta(g).$$

Agora, mostremos que $B^1(\Gamma, \mathcal{U}(S))$ está contido no núcleo $N(\eta)$ de η. De fato, se $f \in B^1(\Gamma, \mathcal{U}(S))$ então $f(\gamma) = u^{-1}\gamma(u)$, para algum $u \in \mathcal{U}(S)$ e para qualquer $\gamma \in \Gamma$. Logo, para todo $r \in R$ temos, em S_f, $\gamma.u^{-1}r = f(\gamma)\gamma(u)^{-1}r = u^{-1}\gamma(u)\gamma(u)^{-1}r = u^{-1}r$, para qualquer $\gamma \in \Gamma$, ou seja $u^{-1}r \in S_f^\Gamma$. Isto define um R-homomorfismo, claramente injetor, $\iota : R \to S_f^\Gamma$, dado por $\iota : r \mapsto u^{-1}r$. Além disso, ι é um isomorfismo, pois se $s \in S_f^\Gamma$ então $s = \gamma \cdot s = f(\gamma)\gamma(s) = u^{-1}\gamma(us)$, e portanto $\gamma(us) = us$, para todo $\gamma \in \Gamma$. Logo, $us \in S^\Gamma = R$ e $\iota(us) = u^{-1}(us) = s$, ou seja, ι é sobrejetor. Assim, $\eta(f) = \overline{S_f^\Gamma} = \overline{R}$ e $f \in N(\eta)$. Conseqüentemente η induz um homomorfismo de grupos $\eta_1 : H^1(\Gamma, \mathcal{U}(S)) \to Pic(R)$ dado por $\eta_1(f) = \overline{S_f^\Gamma}$.

Etapa 2: a exatidão em $H^1(\Gamma, \mathcal{U}(S))$

Seja $f \in Z^1(\Gamma, \mathcal{U}(S))$ tal que $\overline{S_f^\Gamma} = \overline{R}$. Então $S_f^\Gamma \approx R$ como R-módulos e temos a seguinte composição ω de D-isomorfismos $S \approx S \otimes_R R \approx S \otimes_R S_f^\Gamma \approx S_f$, dada por por $\omega : s \mapsto s \otimes 1 \mapsto s \otimes w \mapsto sw = ws$, para algum $w \in S_f^\Gamma \subset S_f$. Como ω é um isomorfismo, $w \in \mathcal{U}(S)$. Além disso, dado $v \in D$ temos $v \cdot (\omega s) = v \cdot \omega(s) = \theta_f(v) \cdot \omega(s) = \omega\big(\theta_f(v) \cdot s\big) = \omega(\theta_f(v) \cdot s)$, para todo

$s \in S$. Logo, $v \cdot w = w\theta_f(v)$, ou seja, $\theta_f(v) = w^{-1}v \cdot w$. Em particular, já que $w \in S_f^\Gamma$, $\theta_f(\gamma) = w^{-1}\gamma \cdot w = w^{-1}w = 1$, para qualquer $\gamma \in \Gamma$. Por outro lado, $\theta_f(\gamma) = w^{-1}\gamma.w = w^{-1}f(\gamma)\gamma(w)$. Assim, $f(\gamma) = w\gamma(w^{-1})$ para todo $\gamma \in \Gamma$, o que mostra que $f \in B^1(\Gamma, \mathcal{U}(S))$. Ou seja, $[f] = 1$ em $H^1(\Gamma, \mathcal{U}(S))$.

Etapa 3: a definição de η_2

Seja $\overline{P} \in Pic(R)$. Então $\gamma \otimes 1 : S \otimes_R P \to {}_\gamma(S \otimes_R P)$ é um S-isomorfismo, para todo $\gamma \in \Gamma$. É suficiente mostrar que $\gamma \otimes 1$ é um S-homomorfismo. De fato, $\gamma \otimes 1\big(s(s' \otimes x)\big) = \gamma \otimes 1(ss' \otimes x) = \gamma(ss') \otimes x = \gamma(s)\gamma(s') \otimes x = s \cdot (\gamma \otimes 1(s' \otimes x))$, para quaisquer $s, s' \in S$ e $x \in E$. Portanto $\gamma \cdot \overline{S \otimes_R P} = \overline{S \otimes_R P}$, para qualquer $\gamma \in \Gamma$, ou seja, $\overline{S \otimes_R P} \in Pic(S)^\Gamma$. Isto permite definir uma aplicação $\eta_2 : Pic(R) \to Pic(S)^\Gamma$ dada por $\eta_2 : \overline{P} \mapsto \overline{S \otimes_R P}$. Claramente η_2 é um homomorfismo de grupos.

Etapa 4: a exatidão em $Pic(R)$

Seja $f \in Z^1(\Gamma, \mathcal{U}(S))$. Então $\eta_2\eta_1([f]) = \eta_2\big(\overline{S_f^\Gamma}\big) = \overline{S \otimes_R S_f^\Gamma}$ e $S \otimes_R S_f^\Gamma \approx S_f$ como D-módulos e, em particular, como S-módulos. Mas $S_f \approx S$ como S-módulos e então $\eta_2\eta_1 = 1$. Ou seja, a imagem de η_1 está contida no núcleo de η_2.

Consideremos agora um elemento $\overline{P}$ do núcleo de η_2. Então existe um isomorfismo de S-módulo $\phi : S \otimes_R P \to S$. Observemos que $S \otimes_R P$ tem uma estrutura de D-módulo à esquerda, com D agindo na primeira componente. Seja $\theta : D \to D$ a aplicação dada por $\theta(v) \cdot s = \phi(v \cdot \phi^{-1}(s))$, para todo $v \in D$ e $s \in S$. É fácil verificar que θ é um homomorfismo de R-álgebras e de S-módulos. Logo $\theta(s) = s\theta(1) = s$ e θ é univocamente determinado

por sua ação nos elementos $\gamma \in \Gamma$. Seja $f : \Gamma \to S$ a aplicação dada por $f(\gamma) = \theta(\gamma) \cdot 1$, para qualquer $\gamma \in \Gamma$. Como $\theta(\gamma) = \phi(\gamma \cdot \phi^{-1}(\_))$ é claramente um isomorfismo e $\theta(\gamma) \cdot s = \phi\big(\gamma \cdot \phi^{-1}(s)\big) = \phi\Big(\gamma\big(s\phi^{-1}(1)\big)\Big) = \phi\Big(\gamma(s)\gamma\big(\phi^{-1}(1)\big)\Big) = \gamma(s)\phi\big(\gamma \cdot \phi^{-1}(1)\big) = \gamma(s)\theta(\gamma) \cdot 1 = \gamma(s)f(\gamma)$, para todo $s \in S$, então $f(\gamma) \in \mathcal{U}(S)$ e $\theta(\gamma) = f(\gamma)\gamma$, para qualquer $\gamma \in \Gamma$. Além disso, de $f(\gamma\gamma')\gamma\gamma' = \theta(\gamma\gamma') = \theta(\gamma)\theta(\gamma') = f(\gamma)\gamma \cdot f(\gamma')\gamma' = f(\gamma)\gamma\big(f(\gamma')\big)\gamma\gamma'$ decorre que $f(\gamma\gamma') = f(\gamma)\gamma\big(f(\gamma')\big)$, para quaisquer $\gamma, \gamma' \in \Gamma$, ou seja, $f \in Z^1\big(\Gamma, \mathcal{U}(S)\big)$. Para a conclusão da demonstração desta etapa basta exibir um R-isomorfismo de P em S_f^Γ, isto é, mostrar que P está na imagem de η_1. Para tanto, observemos que ϕ^{-1} é um S-isomorfismo de S em $S \otimes_R P$ e que $\phi\big(\gamma \cdot \phi^{-1}(\_)\big) = \theta(\gamma) = f(\gamma)\gamma$, para todo $\gamma \in \Gamma$. Logo, para quaisquer $s \in S_f$ e $s'\gamma \in D$ temos $\phi^{-1}(s'\gamma \cdot s) = \phi^{-1}(s'f(\gamma)\gamma \cdot s) = \phi^{-1}(\phi(s'\gamma \cdot \phi^{-1}(s))) = s'\gamma\phi^{-1}(s)$. Então, $\phi^{-1} : S_f \to S \otimes_R P$ é um isomorfismo de D-módulos à esquerda e

$$S_f^\Gamma \approx T_S \otimes_D S_f \xrightarrow{1\otimes\phi^{-1}} T_S \otimes_D (S \otimes_R P) \approx (T_S \otimes_D S) \otimes_R P \approx R \otimes_R P \approx P$$

é um isomorfismo de R-módulos.

Etapa 5: a definição de η_3

Seja $\overline{P} \in Pic(S)^\Gamma$. Então $\gamma \cdot \overline{P} = \overline{P}$, para cada $\gamma \in \Gamma$. Conseqüentemente, existe um R-isomorfismo $\psi_\gamma : P \to P$ tal que $\psi_\gamma(sx) = s \cdot \psi_\gamma(x) = \gamma(s)\psi_\gamma(x)$, para quaisquer $s \in S$ e $x \in P$. Logo $\psi_{\gamma\gamma'}\psi_{\gamma'}^{-1}\psi_\gamma^{-1} : P \to P$ é um isomorfismo de R-módulos e $\psi_{\gamma\gamma'}\psi_{\gamma'}^{-1}\psi_\gamma^{-1}(sx) = s\psi_{\gamma\gamma'}\psi_{\gamma'}^{-1}\psi_\gamma^{-1}(x)$, para quaisquer $s \in S$ e $x \in P$. Portanto, $\psi_{\gamma\gamma'}\psi_{\gamma'}^{-1}\psi_\gamma^{-1} \in \mathcal{E}nd_S(P)$. Por outro lado, já que P é um S-módulo projetivo de posto constante 1, é fácil verificar, via localização, que a aplicação $\iota : S \to \mathcal{E}nd_S(P)$, dada por $s :\mapsto (\iota_s : x \mapsto sx)$, para todo $s \in S$

e $x \in P$, é um isomorfismo de S-módulos. Conseqüentemente, $\psi_{\gamma\gamma'}\psi_{\gamma'}^{-1}\psi_{\gamma}^{-1}$ é a multiplicação por um elemento $f(\gamma,\gamma') \in \mathcal{U}(S)$, para quaisquer $\gamma,\gamma' \in \Gamma$. Desta forma, para cada S-módulo P tal que $\overline{P} \in Pic(S)^{\Gamma}$ existe uma função $f : \Gamma \times \Gamma \to \mathcal{U}(S)$. Além disso, da igualdade $\psi_{\gamma(\gamma'\gamma'')} = \psi_{(\gamma\gamma')\gamma''}$ obtemos que $f \in Z^2(\Gamma, \mathcal{U}(S))$.

Seja $\eta_3 : Pic(S)^{\Gamma} \to H^2(\Gamma, \mathcal{U}(S))$ a correspondência $\overline{P} \mapsto [f]$. Mostremos que η_3 está bem definida. Para isso, seja $\{\lambda_\gamma \,|\, \gamma \in \Gamma\}$ uma outra escolha de R-isomorfismos de P em P tais que $\lambda_\gamma(sx) = \gamma(s)\lambda_\gamma(x)$, para quaisquer $s \in S$ e $x \in P$. Pelo mesmo argumento utilizado acima, determinamos uma nova função $g : \Gamma \otimes \Gamma \to \mathcal{U}(S)$ tal que $g(\gamma,\gamma') = \lambda_{\gamma\gamma'}\lambda_{\gamma'}^{-1}\lambda_{\gamma}^{-1}$, para quaisquer $\gamma,\gamma' \in \Gamma$. Também como acima $g \in Z^2(\Gamma, \mathcal{U}(S))$. Como $\lambda_\gamma\psi_\gamma^{-1}$ é um S-isomorfismo de P em P, então $\lambda_\gamma\psi_\gamma^{-1}$ é também a multiplicação por um elemento $h(\gamma) \in \mathcal{U}(S)$. Temos:

$$\begin{aligned}
f(\gamma,\gamma')^{-1}g(\gamma,\gamma') &= (\psi_\gamma\psi_{\gamma'}\psi_{\gamma\gamma'}^{-1})(\lambda_{\gamma\gamma'}\lambda_{\gamma'}^{-1}\lambda_{\gamma}^{-1}) \\
&= (\psi_\gamma\lambda_\gamma^{-1})\lambda_\gamma(\psi_{\gamma'}\lambda_{\gamma'}^{-1})\lambda_{\gamma'}\psi_{\gamma\gamma'}^{-1}\lambda_{\gamma\gamma'}\lambda_{\gamma'}^{-1}\lambda_{\gamma}^{-1} \\
&= h(\gamma)^{-1}\lambda_\gamma h(\gamma')^{-1}\lambda_{\gamma'}\psi_{\gamma\gamma'}^{-1}\lambda_{\gamma\gamma'}\lambda_{\gamma'}^{-1}\lambda_{\gamma}^{-1} \\
&= (\gamma(h(\gamma'))h(\gamma))^{-1}(\lambda_\gamma\lambda_{\gamma'}\psi_{\gamma\gamma'}^{-1})(\lambda_{\gamma\gamma'}\lambda_{\gamma'}^{-1}\lambda_{\gamma}^{-1}) \\
&= (\gamma(h(\gamma'))h(\gamma))^{-1}(\lambda_{\gamma\gamma'}\lambda_{\gamma'}^{-1}\lambda_{\gamma}^{-1})(\lambda_\gamma\lambda_{\gamma'}\psi_{\gamma\gamma'}^{-1}) \\
&= (\gamma(h(\gamma'))h(\gamma))^{-1}h(\gamma\gamma').
\end{aligned}$$

Então, $[f] = [g] \in H^2(\Gamma, \mathcal{U}(S))$ e η_3 está bem definida.

Resta mostrar que η_3 é um homomorfismo de grupos. Sejam $\overline{P_1}, \overline{P_2} \in Pic(S)^{\Gamma}$ tais que $\eta_3(\overline{P_1}) = [f]$ e $\eta_3(\overline{P_2}) = [g]$. Para cada $\gamma \in \Gamma$, sejam $\psi_\gamma : P_1 \to P_1$ e $\theta_\gamma : P_2 \to P_2$ os R-isomorfismos que definem f e g

respectivamente. Logo $\psi_\gamma \otimes \theta_\gamma : P_1 \otimes_S P_2 \to P_1 \otimes_S P_2$ é um R-isomorfismo que define um novo elemento $h \in Z^1(\Gamma, \mathcal{U}(S))$. Portanto, para quaisquer $\gamma, \gamma' \in \Gamma$ temos

$$\begin{aligned} h(\gamma,\gamma') &= (\psi_{\gamma\gamma'} \otimes \theta_{\gamma\gamma'})(\psi_{\gamma'} \otimes \theta_{\gamma'})^{-1}(\psi_\gamma \otimes \theta_\gamma)^{-1} \\ &= \psi_{\gamma\gamma'}\psi_{\gamma'}^{-1}\psi_\gamma^{-1} \otimes \theta_{\gamma\gamma'}\theta_{\gamma'}^{-1}\theta_\gamma^{-1} \\ &= f(\gamma,\gamma')g(\gamma,\gamma'). \end{aligned}$$

Conseqüentemente, $\eta_3(\overline{P_1 \otimes_S P_2}) = [f][g] = \eta_3(\overline{P_1})\eta_3(\overline{P_2})$ e η_3 é um homomorfismo.

Etapa 6: a exatidão em $Pic(S)^\Gamma$

Observemos que se $\overline{P} \in \eta_2\big(Pic(R)\big)$, isto é, se $\overline{P} = \overline{S \otimes_R E}$, para algum $\overline{E} \in Pic(R)$, então $P \approx {}_\gamma P$ via o R-isomorfismo $\psi_\gamma = \gamma \otimes 1$, para todo $\gamma \in \Gamma$. Além disso, $\psi_\gamma\psi_{\gamma'} = \psi_{\gamma\gamma'}$. Então, $\eta_3(\overline{P}) = [f]$, com $f(\gamma,\gamma') = \psi_{\gamma\gamma'}\psi_{\gamma'}^{-1}\psi_\gamma^{-1} = 1$, para quaisquer $\gamma, \gamma' \in \Gamma$. Ou seja, $\overline{P}$ está no núcleo de η_3. Reciprocamente, se $\overline{P}$ está no núcleo de η_3 então, para cada $\gamma \in \Gamma$, existem um R-isomorfismo $\psi_\gamma : P \to P$ e um elemento $h(\gamma) \in \mathcal{U}(S)$ tais que $\psi_\gamma(sx) = \gamma(s)\psi_\gamma(x)$, para quaisquer $s \in S$, $x \in P$ e $\psi_{\gamma\gamma'}\psi_{\gamma'}^{-1}\psi_\gamma^{-1} = h(\gamma\gamma')(h(\gamma)\gamma(h(\gamma'))^{-1}$, para quaisquer $\gamma, \gamma' \in \Gamma$. Conseqüentemente, a ação $\gamma \cdot x = h(\gamma)^{-1}\psi_\gamma(x)$, para todo $x \in P$ e todo $\gamma \in \Gamma$, define sobre P uma estrutura de D-módulo à esquerda. De fato, para quaisquer $\gamma, \gamma' \in \Gamma$ e $x \in P$, temos

$$\gamma \cdot (\gamma' \cdot x) = \gamma \cdot \big(h(\gamma')\psi_{\gamma'}(x)\big) = h(\gamma)^{-1}\psi_\gamma\big(h(\gamma')\psi_{\gamma'}(x)\big)$$

$$= h(\gamma)^{-1}\gamma\big(h(\gamma')\big)^{-1}\psi_\gamma\psi_{\gamma'}(x) = h(\gamma\gamma')^{-1}\psi_{\gamma\gamma'}(x) = (\gamma\gamma') \cdot x.$$

Mas P e S são, respectivamente, S-módulo e D-módulo à esquerda projetivos finitamente gerados, então P é também um D-módulo à esquerda projetivo

finitamente gerado e, pelo Lema 1.5.5, $P \approx S \otimes_R P^\Gamma$. Como P é S-módulo projetivo de posto constante 1, pode-se ver facilmente, via localização, que P e S têm o mesmo posto como R-módulos projetivos. Portanto, ainda via localização e pelo Lemme I.6.1 de [27], obtemos que $\overline{P^\Gamma} \in Pic(R)$, ou seja, $\overline{P} = \eta_2(\overline{P^\Gamma})$. Com isto concluímos a demonstração do teorema. □

Capítulo 2: O Resultado Principal

Neste capítulo R continua denotando um anel comutativo com unidade. Seja $p \in \mathbb{Z}$ primo ímpar e regular em R. Em todo este capítulo, denotamos por S o anel $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle}$ e $\varepsilon = X + \langle \Phi_p(X) \rangle$. Pelo que vimos no primeiro capítulo ε é uma raiz primitiva p-ésima da unidade em $S = R[\varepsilon]$. Como antes, denotamos por $Pic(S)$ o grupo de Picard, das classes $\overline{P}$ de isomorfismos dos S-módulos projetivos P de posto constante 1, e por $Pic_p(S)$ o subgrupo de p-torsão.

Na primeira secção definimos uma ação de $\Gamma = \{\gamma_i \mid \gamma_i : \varepsilon \mapsto \varepsilon^i,\ 1 \leq i \leq p-1\}$, que é um subgrupo de R-automorfismos de S, sobre a seqüência exata de L. Childs e mostramos que a seqüência formada pelos subgrupos estáveis por Γ também é exata.

Nas secções seguintes vamos estender os resultados de C. Greither e R. Miranda [17], dando uma caracterização para os grupos $T_p(R)$, $H_p(R)$ e $PrimPic_p(R[G])$, onde G denota o grupo cíclico de ordem p.

2.1 A Γ-linearidade

Em [9], L. Childs mostrou que a seqüência de grupos abaixo é exata:

$$1 \longrightarrow G_p(S) \xrightarrow{j} T_p(S) \xrightarrow{\pi} PrimPic_p(S[G]) \longrightarrow 1$$

onde $G_p(S) = \dfrac{\mathcal{U}_{\lambda^p}(S)}{\left(\mathcal{U}_{\lambda}(S)\right)^p}$ com $\lambda = \varepsilon - 1$ e, para quaisquer $[A] \in T_p(S)$ e $\overline{a} \in G_p(S)$, $\pi([A;\sigma]) = \overline{A}$ e $j(\overline{a}) = \left[\dfrac{S[X]}{\langle f(X)\rangle}; \sigma(x) = \varepsilon x + 1\right]$

com $x = X + \langle f(X)\rangle$ e $f \in S[X]$ mônico dado pela equação $\left(\lambda X + 1\right)^p - a = \lambda^p f(X)$ (Corolário 1.2.5).

Consideremos agora o subgrupo de $\mathcal{A}ut_R(S)$, $\Gamma = \{id = \gamma_1, \gamma_2, \ldots, \gamma_{p-1}\}$ com $\gamma_i : \varepsilon \mapsto \varepsilon^i$, para todo $1 \leq i \leq p-1$. Como vimos no Capítulo anterior, Γ é cíclico. Para definir uma ação de Γ sobre a seqüência de L. Childs, precisamos do seguinte módulo: dados A um S-módulo e $\gamma \in \Gamma$, definimos o S-módulo ${}_{\gamma}A$ tal que ${}_{\gamma}A = A$ como grupo aditivo e S age sobre ${}_{\gamma}A$ via $s \cdot \alpha = \gamma(s)\alpha$, para quaisquer $s \in S$ e $\alpha \in A$. Então a ação de Γ sobre a seqüência de L. Childs é dada pela ação natural sobre os grupos $T_p(S)$ e $PrimPic_p(S[G])$ e pela *-ação sobre $G_p(S)$: para cada $\gamma_i \in \Gamma$ com $1 \leq i \leq p-1$,

$$\gamma_i * \overline{a} = \overline{\gamma_i^{-1}(a^i)}, \quad \text{para qualquer } \overline{a} \in G_p(S);$$

$$\gamma_i([A;\sigma]) = [{}_{\gamma_i}A;\sigma], \quad \text{para qualquer } [A;\sigma] \in T_p(S); \text{ e}$$

$$\gamma_i \cdot \overline{P} = \overline{{}_{\gamma_i}P}, \quad \text{para qualquer } \overline{P} \in PrimPic_p(S[G]).$$

Observemos que estas ações estendem as *-ações de C. Greither e R. Miranda [17]. Claramente, precisamos verificar esta afirmação somente so-

bre $PrimPic_p(S[G])$. Então, vamos supor que $p \in \mathcal{U}(S)$, e portanto, para qualquer classe $[A;\sigma] \in T_p(S)$, temos $A \approx S \oplus P \oplus \ldots \oplus P^{\otimes(p-1)}$ onde $P = P_A = \{a \in A \mid \sigma(a) = \varepsilon a\}$ ([3] e [14]). Sejam $\gamma_i \in \Gamma$ e $\overline{A} = \pi([A;\sigma]) \in PrimPic_p(S[G]) = \pi\big(T_p(S)\big)$. Logo,

$$\gamma_i * \overline{A} = \overline{{}_{\gamma_i}(S \oplus P \oplus \ldots \oplus P^{\otimes(p-1)})} = \overline{{}_{\gamma_i}S \oplus {}_{\gamma_i}P \oplus \ldots \oplus {}_{\gamma_i}P^{\otimes(p-1)}} \in Pic(S[G]).$$

Agora, trabalhando em $Pic_p(S)$ como C. Greither e R. Miranda, trabalhamos com $\overline{P_A}$ em vez de $\overline{A}$, e $\sigma(\alpha) = \varepsilon \cdot \alpha$ somente para os elementos de ${}_{\gamma_i}P^{\otimes^i}$. De fato, sejam $1 \leq i \leq p-1$ e $\alpha = \sum_{k=1}^{m} x_{1k} \otimes \ldots \otimes x_{ik} \in {}_{\gamma_i}P^{\otimes^i}$ com $x_{jk} \in P = \{a \in A \mid \sigma(a) = \varepsilon a\}$ para quaisquer $1 \leq j \leq i$ e $1 \leq k \leq m$. Então, $\sigma(\alpha) = \sum_{k=1}^{m} \varepsilon x_{1k} \otimes \ldots \otimes \varepsilon x_{ik} = \sum_{k=1}^{m} \varepsilon^i \big(x_{1k} \otimes \ldots \otimes x_{ik}\big)$ $= \varepsilon^i \Big(\sum_{k=1}^{m} x_{1k} \otimes \ldots \otimes x_{ik}\Big) = \gamma_i(\varepsilon)\alpha = \varepsilon \cdot \alpha$. É fácil ver que, para $k \neq i$ e $\beta \in {}_{\gamma_i}P^{\otimes^k}$, $\sigma(\beta) = \varepsilon^k \beta \neq \varepsilon \cdot \beta$. Conseqüentemente, $\gamma_i * \overline{A} = \overline{P_{\gamma_i A}} = \overline{{}_{\gamma_i}P^{\otimes^i}} = \gamma_i * \overline{P_A}$, o que mostra a afirmação.

A verificação de que o homomorfismo π comuta com a ação de Γ sobre os grupos $T_p(S)$ e $PrimPic_p(S[G])$ é imediata a partir das definições dadas.

Para a verificação de que o homomorfismo j também comuta com a ação de Γ sobre os grupos $G_p(S)$ e $T_p(S)$, necessitamos de algumas considerações preliminares.

Observemos que cada $\gamma \in \Gamma$ se estende de modo natural a um R-automorfismo de $S[X]$ via $\gamma\big(\sum_k s_k X^k\big) = \sum_\gamma (s_k) X^k$. Observemos também que a cada polinômio $h(X) = \sum_k s_k X^k$ em $S[X]$ corresponde o polinômio ${}_\gamma h(X) = \sum_k \gamma^{-1}(s_k) \cdot X^k$ em ${}_\gamma(S[X])$. Assim, ${}_\gamma\Big(\frac{S[X]}{\langle f(X)\rangle}\Big) = \frac{{}_\gamma S[X]}{\langle {}_\gamma f(X)\rangle} = {}_\gamma(S[x])$ onde $x = X + \langle f(X)\rangle$ e além disso, a aplicação ${}_\gamma(S[X]) \longrightarrow S[Z]$ dado por

$\sum_k s_k \cdot X^k) \mapsto \sum_k s_k Z^k$, induz um isomorfismo de S-álgebras

$$\varphi\colon {}_\gamma(S[x]) = \frac{\gamma(S[X])}{\langle {}_\gamma f(X)\rangle} \to \frac{S[Z]}{\langle \gamma^{-1}(f(Z))\rangle} = S[z] \quad \text{onde } z = Z + \langle \gamma^{-1}(f(Z))\rangle.$$

Agora, via φ estendemos a ação de σ sobre $S[z]$, isto é,

$$\sigma(z) = \varphi\Big(\sigma\big(\varphi^{-1}(z)\big)\Big) = \varphi(\sigma(x)) = \varphi(\gamma^{-1}(\varepsilon)\cdot x + 1) = \gamma^{-1}(\varepsilon)z + 1.$$

Assim, para cada $\gamma_i \in \Gamma$,

$$\gamma_i(j(\overline{a})) = \gamma_i\Big(\Big[\frac{S[X]}{\langle f(X)\rangle}; \sigma(x) = \varepsilon x + 1\Big]\Big) = \Big[{}_{\gamma_i}\Big(\frac{S[X]}{\langle f(X)\rangle}\Big); \sigma(x) = \varepsilon x + 1\Big]$$

$$= \Big[\frac{\gamma_i(S[X])}{\langle {}_{\gamma_i} f(X)\rangle}; \sigma(x) = \gamma_i^{-1}(\varepsilon)\cdot x + 1\Big] = \Big[\frac{S[Z]}{\langle \gamma_i^{-1}(f(Z))\rangle}; \sigma(z) = \gamma_i^{-1}(\varepsilon)z + 1\Big]$$

$$= \Big[\frac{S[Z]}{\langle \gamma_i^{-1}(f(Z))\rangle}; \sigma(z) = \varepsilon^t z + 1\Big] \quad \text{em } T_p(S), \text{ com } \quad it \equiv 1 (\mathrm{mod}\, p).$$

Por outro lado, seja $w = (\sigma(z) - z) \in S[z]$. Então, $w = (\varepsilon^t - 1)z + 1 = \gamma_i^{-1}(\lambda)z + 1$. Logo, $\sigma(w) = (\varepsilon^t - 1)\sigma(z) + 1 = (\varepsilon^t - 1)(w + z) + 1 = (\varepsilon^t - 1)z + 1 + (\varepsilon^t - 1)w = w + (\varepsilon^t - 1)w = \varepsilon^t w$ e $\sigma(\omega^p) = (\varepsilon^t)^p w^p = w^p$, ou seja, $b = w^p \in S$. Além disso, $w \in \mathcal{U}(S[z])$. De fato, suponhamos que exista $\mathcal{M} \in \mathcal{M}ax(S[z])$ tal que $w = (\sigma(z) - z) \in \mathcal{M}$. Conseqüentemente, $(\sigma(s) - s) \in \mathcal{M}$, para cada $s \in S[z]$, o que contradiz o fato de que $S[z]$ é extensão galoisiana de R (Teorema 1.1.1). Mas $\gamma_i^{-1}(\lambda) = (\varepsilon^t - 1) = \lambda(\varepsilon^{t-1} + \ldots + \varepsilon + 1) \in \lambda S$, isto é, $w = \gamma_i^{-1}(\lambda)z + 1 \in \mathcal{U}_\lambda(S[z])$ e portanto $b = w^p \in \mathcal{U}_{\lambda^p}(S)$.

Afirmamos que $b = \gamma_i^{-1}(a)$. De fato, $(\lambda X + 1)^p - a = \lambda^p f(X)$ em $S[X]$, significa que $\big(\gamma_i^{-1}(\lambda)X + 1\big)^p - \gamma_i^{-1}(a) = \gamma_i^{-1}(\lambda)^p {}_{\gamma_i} f(X)$ em ${}_{\gamma_i}(S[X])$. Conseqüentemente $\big(\gamma_i^{-1}(\lambda)Z + 1\big)^p - \gamma_i^{-1}(a) = \gamma_i^{-1}(\lambda)^p \gamma_i^{-1}\big(f(Z)\big)$, isto é, $\big((\varepsilon^t - 1)Z + 1\big)^p - \gamma_i^{-1}(a) = \gamma_i^{-1}(\lambda)^p \gamma_i^{-1}\big(f(Z)\big)$ em $S[Z]$. Agora, de $\gamma_i^{-1}\big(f(z)\big) = 0$ em $S[z]$, temos $\big((\varepsilon^t - 1)z + 1\big)^p - \gamma_i^{-1}(a) = 0$, ou seja, $b = w^p = \gamma_i^{-1}(a)$.

Finalmente, seja $v = w^i$. Então, $v^p = (w^i)^p = (w^p)^i = b^i = \gamma_i^{-1}(a^i)$ e $\sigma(v) = \sigma(w)^i = (\varepsilon^t w)^i = \varepsilon^{it} w^i = \varepsilon v$. Como $w = 1 + (\varepsilon^t - 1)z$ e $(\varepsilon^t - 1) = \lambda(\varepsilon^{t-1} + \ldots + \varepsilon + 1)$, $w = 1 + \lambda(\varepsilon^{t-1} + \ldots + \varepsilon + 1)z$. Logo, $v = w^i = 1 + \lambda y$ para certo $y \in S[z]$. Assim, $\varepsilon + \varepsilon\lambda y = \varepsilon v = \sigma(v) = \sigma(1 + \lambda y) = 1 + \lambda\sigma(y)$, isto é, $\varepsilon - 1 + \varepsilon\lambda y = \lambda\sigma(y)$, ou $\lambda(1 + \varepsilon y) = \lambda\sigma(y)$. Mas λ é regular e portanto $\sigma(y) = \varepsilon y + 1$. Segue da igualdade $v^p = \gamma_i^{-1}(a^i)$ que $(1+\lambda y)^p - \gamma_i^{-1}(a^i) = 0$. Conseqüentemente, existe um polinômio mônico $g(Y) \in S[Y]$ satisfazendo $(\lambda Y + 1)^p - \gamma_i^{-1}(a^i) = \lambda^p g(Y)$, com $g(y) = 0$. Pelo Teorema 1.3.5, $S[z] = S[y]$. Já que y é raiz de $g(Y)$, segue do teorema do homomorfismo e da comparação dos postos que existe um isomorfismo de S-álgebras $S[y] \xrightarrow{\psi} \dfrac{S[Y]}{\langle g(Y)\rangle}$. Além disso, ψ é um isomorfismo de extensões de Galois, pois $\psi\big(\sigma(y)\big) = \psi(\varepsilon y + 1) = \varepsilon\overline{Y} + 1 = \sigma(\overline{Y}) = \sigma\big(\psi(y)\big)$. Portanto, $\left[\dfrac{S[Z]}{\langle\gamma_i^{-1}(f(Z))\rangle}; \sigma(z) = \varepsilon^t z + 1\right] = \left[\dfrac{S[Y]}{g(Y)}; \sigma(y) = \varepsilon y + 1\right]$, onde $g \in S[Y]$ é o polinômio mônico dado pela equação $(\lambda Y + 1)^p - \gamma_i^{-1}(a^i) = \lambda^p g(Y)$ e $\left[\dfrac{S[Y]}{g(Y)}; \sigma(y) = \varepsilon y + 1\right] = j\Big(\overline{\gamma_i^{-1}(a^i)}\Big) = j(\gamma_i * \overline{a})$. Com isto, mostramos que $\gamma_i\big(j(\overline{a})\big) = j\big(\gamma_i * \overline{a}\big)$.

Finalizamos esta secção, mostrando que a seqüência formada pelos grupos estáveis pela ação de Γ sobre a seqüência exata de de L. Childs também é exata.

2.1.1. Teorema

Sejam $p \in \mathbb{Z}$ *primo,* $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle} = R[\varepsilon]$ *com* $\varepsilon = X + \langle \Phi_p(X) \rangle$ *e* $\Gamma = \{\gamma_i \mid \gamma_i : \varepsilon \mapsto \varepsilon^i, 1 \leq i \leq p-1\}$ *subgrupo de* $Aut_R(S)$. *Então, a seqüência*

$$1 \longrightarrow G_p(S)^{*\Gamma} \xrightarrow{j} T_p(S)^{\Gamma} \xrightarrow{\pi} \Big(PrimPic_p(S[G])\Big)^{\Gamma} \longrightarrow 1$$

é exata, onde $j(\overline{a}) = \Big[\dfrac{S[X]}{\langle f(X) \rangle}; \sigma(x) = \varepsilon x + 1\Big]$ *com* $x = X + \langle f(X) \rangle$ *e* $f \in S[X]$ *mônico dado pela equação* $(\lambda X + 1)^p - a = \lambda^p f(X)$ *e* $\pi([A;\sigma]) = \overline{A}$, *para quaisquer* $[A] \in T_p(S)$ *e* $\overline{a} \in G_p(S)$.

Demonstração : Claramente a seqüência é exata à esquerda, pois j é a restrição à $G_p(S)^{*\Gamma}$ de um monomorfismo. Então, decorre do Lema da Serpente ([42] Theorem 6.5) que a seqüência abaixo é exata:

$$1 \longrightarrow G_p(S)^{*\Gamma} \xrightarrow{j} T_p(S)^{\Gamma} \xrightarrow{\pi} \Big(PrimPic_p(S[G])\Big)^{\Gamma} \xrightarrow{\partial}$$

$$\xrightarrow{\partial} H^1(\Gamma, G_p(S)) \xrightarrow{j_1} H^1(\Gamma, T_p(S)) \xrightarrow{\pi_1} H^1\Big(\Gamma, \big(PrimPic_p(S[G])\big)^{\Gamma}\Big).$$

Por outro lado $\mathcal{U}_{\lambda^p}(S) \subseteq \mathcal{U}_{\lambda}(S)$, e portanto $G_p(S) = \dfrac{\mathcal{U}_{\lambda^p}(S)}{\mathcal{U}_{\lambda}(S)^p}$ é de p-torsão. Então, $\Big(H^1\big(\Gamma, G_p(S)\big)\Big)^p = \{\overline{1}\}$ ([42] Theorem 10.26). Além disso, $\Gamma \approx \mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ e, em particular, $|\Gamma| = p-1$. Logo, segue que (novamente por [42] Theorem 10.26) $\Big(H^1\big(\Gamma, G_p(S)\big)\Big)^{(p-1)} = \{\overline{1}\}$. Assim, dado $\overline{\theta} \in H^1(\Gamma, G_p(S))$, $\overline{1} = \overline{\theta}^p = \overline{\theta}\,\overline{\theta}^{(p-1)} = \overline{\theta}$, e portanto $H^1\big(\Gamma, G_p(S)\big) = \{\overline{1}\}$. O que conclui a demonstração. □

2.2 O isomorfismo $T_p(R) \approx T_p(S)^{\Gamma}$

Para obter o isomorfismo desejado, vamos exibir, para cada A, extensão galoisiana de S com grupo de Galois G, uma extensão galoisiana A_0 de R com mesmo grupo de Galois G, tal que $[A] = [S \otimes_R A_0]$ em $T_p(S)$. Fazemos isto, aplicando técnicas da teoria de "descente" galoisiana, observando o fato de que, em geral, S não é uma extensão galoisiana de R pois, para p não invertível em R, $S = R[\varepsilon]$ não é R-separável. Então, usamos o conceito de *extensão Γ-normal* (ver secção 1.3). Para o caso em que $[A] \in H_p(S)$, isto é, A possui S-base normal, A_0 (que possui R-base normal) é obtida no próximo lema. Para isso, consideremos novamente o subgrupo cíclico de $\mathcal{A}ut_R(S)$, $\Gamma = \{id = \gamma_1, \gamma_2, \ldots, \gamma_{p-1}\}$ com $\gamma_i : \varepsilon \mapsto \varepsilon^i$, para todo $1 \leq i \leq p-1$.

2.2.1. Lema

Sejam $p \in \mathbb{Z}$ primo ímpar, $G = \langle \sigma \rangle$ grupo de ordem p e A uma extensão Γ-normal de S com grupo de Galois G que possui S-base normal, isto é, $[A] \in H_p(S)$ tal que γ se estende à $\tilde{\gamma} \in \mathcal{A}ut_R(A)$ com ordem $p-1$ satisfazendo $\sigma\tilde{\gamma} = \tilde{\gamma}\sigma$, onde $\Gamma = \langle \gamma \rangle$. Sejam $\tilde{\Gamma} = \langle \tilde{\gamma} \rangle$ e $A_0 = A^{\tilde{\Gamma}}$. Então, $[A_0] \in H_p(R)$ e $[A] = [S \otimes_R A_0]$.

Demonstração : Como $\tilde{\gamma}$ comuta com σ temos $\sigma(A_0) \subseteq A_0$ e portanto G age naturalmente (via restrição) sobre A_0. Assim, a ação de G sobre $S \otimes_R A_0$ é dada via $1 \otimes G$. Então, como $\sigma\tilde{\gamma} = \tilde{\gamma}\sigma$ e $\tilde{\gamma}\,|_S = \gamma$, segue que

$$(S \otimes_R A_0)^G = S \otimes_R A_0^G = S \otimes_R \left(A^G\right)^{\tilde{\Gamma}} = S \otimes_R S^{\tilde{\Gamma}} = S \otimes_R S^{\Gamma} = S \otimes_R R = S.$$

Mas, $[A] \in H_p(S)$, isto é, A possui S-base normal. Seja $\{\alpha_i = \sigma^i(\alpha_0) \mid 0 \leq i \leq p-1\}$ uma S-base normal de A. Pelo Corolário 1.3.2,

$$\alpha = \sum_{i=0}^{p-1} \alpha_i \sigma^{-i} \in \mathcal{U}(A[G]) \quad \text{e} \quad \sigma(\alpha) = \alpha\sigma.$$

Por outro lado, $\tilde{\gamma}$ age sobre $A[G]$ via $\tilde{\gamma}(\sum_{i=0}^{p-1} a_i\sigma^{-i}) = \sum_{i=0}^{p-1} \tilde{\gamma}(a_i)\sigma^{-i}$.

Seja $\beta = \prod_{k=1}^{p-1} \tilde{\gamma}^k(\alpha^{-1}) = \sum_{i=0}^{p-1} \beta_i\sigma^{-i} \in \mathcal{U}(A[G])$. Então,

$\beta = \tilde{\gamma}(\beta) = \tilde{\gamma}(\sum_{i=0}^{p-1} \beta_i\sigma^{-i}) = \sum_{i=0}^{p-1} \tilde{\gamma}(\beta_i)\sigma^{-i}$ e portanto, $\beta_i = \tilde{\gamma}(\beta_i)$, para todo $1 \leq i \leq p-1$. Logo, $\beta \in \mathcal{U}(A_0[G])$. Além disso,

$$\sigma(\beta) = \sigma\Big(\prod_{k=1}^{p-1} \tilde{\gamma}^k(\alpha^{-1})\Big) = \prod_{k=1}^{p-1} \tilde{\gamma}^k\Big(\sigma(\alpha^{-1})\Big)$$

$$= \prod_{k=1}^{p-1} \tilde{\gamma}^k(\alpha^{-1}\sigma^{-1}) = \prod_{k=1}^{p-1} \tilde{\gamma}^k(\alpha^{-1})\tilde{\gamma}^k(\sigma^{-1}) = \beta \cdot \prod_{k=1}^{p-1} \tilde{\gamma}^k(\sigma^{-1}) = \beta(\sigma^{-1})^{p-1} = \beta\sigma.$$

Novamente pelo corolário 1.3.2, $\{\beta_i = \sigma^i(\beta_0)\}_{i=0}^{p-1} \subseteq A_0$ é S-base normal de A. Claramente $\{\beta_i\}_{i=0}^{p-1}$ é também uma R-base de A_0.

Consideremos agora o homomorfismo de S-álgebras $S \otimes_R A_0 \xrightarrow{\mu} A$ dado por $\mu\Big(\sum_{i=0}^{p-1} s_i \otimes b_i\Big) = \sum_{i=0}^{p-1} s_i b_i$. Então μ comuta com a ação de G. De fato,

$$\mu\sigma \sum_{i=0}^{p-1} s_i \otimes b_i = \sum_{i=0}^{p-1} s_i\sigma(b_i) = \sigma\Big(\sum_{i=0}^{p-1} s_i b_i\Big) = \Big(\sigma\mu \sum_{i=0}^{p-1} s_i \otimes b_i\Big).$$

Já que a imagem da S-base $\{1 \otimes \beta_i\}_{i=0}^{p-1}$ de $S \otimes_R A_0$ é $\{\beta_i\}_{i=0}^{p-1}$, que é uma S-base de A, obtemos que μ é um isomorfismo de S-álgebras. Segue que $S \otimes_R A_0$ também é uma extensão galoisiana de S com grupo de Galois G. De fato, sejam $x_i, y_i \in A$ $(1 \leq i \leq m)$ coordenadas de Galois da extensão A. Claramente, $\mu^{-1}(x_i), \mu^{-1}(y_i) \in S \otimes_R A_0$ $(1 \leq i \leq m)$, são coordenadas

de Galois da extensão $S \otimes_R A_0$. Logo, em $T_p(S)$, $[A] = [S \otimes_R A_0]$.

Agora, S é uma R-álgebra fielmente plana ([4], pg.46), pois $S = R[\varepsilon]$ é livre. Então, segue do Lema 1.1.8 que A_0 é extensão galoisiana de R com grupo de Galois G. □

No próximo lema, mostramos que, para cada extensão galoisiana A de R com grupo de Galois G, ao "subir" do anel A para o anel $S \otimes_R A$ com $S = R[\varepsilon]$, preservamos as operações dos grupos $T(G;R)$ e $T(G;S)$. Observemos que não precisamos da hipótese $|G| = p$ prima.

2.2.2. Lema

Sejam $R \subseteq S$, com S uma R-álgebra comutativa e G um grupo abeliano finito. Sejam $[A] = [S \otimes_R A_0]$ e $[B] = [S \otimes_R B_0]$ em $T(G;S)$, com $[A_0], [B_0] \in T(G;R)$. Então, $[A] * [B] = [S \otimes_R (A_0 \otimes_R B_0)^{\delta G}] \in T(G;S)$.

Demonstração : Da hipótese, existem isomorfismos de extensões de Galois $A \overset{f}{\approx} S \otimes_R A_0$ e $B \overset{g}{\approx} S \otimes_R B_0$ satisfazendo $f\sigma = (1 \otimes \sigma)f$ e $g\sigma = (1 \otimes \sigma)g$ para qualquer $\sigma \in G$. Portanto $A \otimes_S B \overset{f \otimes g}{\approx} (S \otimes_R A_0) \otimes_S (S \otimes_R B_0)$ com $f \otimes g(\sigma \otimes \tau) = (1 \otimes \sigma)f \otimes (1 \otimes \tau)g$ para quaisquer $\sigma, \tau \in G$.

Como A_0 e B_0 são extensões galoisianas de R com grupo de Galois G então $A_0 \otimes_R B_0$ é uma extensão galoisiana de R com grupo de Galois $G \otimes G = \{\sigma \otimes \tau \mid \sigma, \tau \in G\}$ e $S \otimes_R A_0 \otimes_R B_0$ é extensão galoisiana de S (Lema 1.1.6), com grupo de Galois $G \otimes G \approx 1 \otimes G \otimes G$ ($G \otimes G$ age sobre $A_0 \otimes_R B_0$ via $\sigma \otimes \tau$ e sobre $S \otimes_R A_0 \otimes_R B_0$ via $1 \otimes \sigma \otimes \tau$, para quaisquer $\sigma, \tau \in G$). Assim, definimos

$\psi : A \otimes_S B \longrightarrow S \otimes_R A_0 \otimes_R B_0$ por $\psi(a \otimes b) = \sum_{i,j} s_i(a;f)t_j(b;g) \otimes a_i \otimes b_j$

onde $f(a) = \sum_{i=1}^{n(a;f)} s_i(a;f) \otimes a_i$ e $g(b) = \sum_{j=1}^{m(b;g)} t_j(b;g) \otimes b_j$. Como f e g estão fixos, escrevemos $n(a) = n(a;f)$, $s_i(a) = s_i(a;f)$, $m(b) = m(b;g)$ e $t_j(b) = t_j(b;g)$, para quaisquer $1 \leq i \leq n(a)$ e $1 \leq j \leq m(b)$. Além disso, para qualquer $\sigma \in G$, $f\sigma = (1 \otimes \sigma)f$ e $g\sigma = (1 \otimes \sigma)g$. Então, dado $\sigma \in G$,

$$\sum_{i=1}^{n(a)} s_i(a) \otimes \sigma(a_i) = (1 \otimes \sigma)f(a) = f\sigma(a) = \sum_{i=1}^{n\left(\sigma(a)\right)} s_i\big(\sigma(a)\big) \otimes \sigma(a)_i$$

e

$$\sum_{j=1}^{m(b)} t_j(b) \otimes \tau(b_j) = (1 \otimes \tau)g(b) = g\tau(b) = \sum_{j=1}^{m\left(\tau(b)\right)} t_j\big(\tau(b)\big) \otimes \tau(b)_j$$

Logo, $\psi(\sigma \otimes \tau) = (1 \otimes \sigma \otimes \tau)\psi$, para quaisquer $\sigma, \tau \in G$. De fato, dados $(a \otimes b) \in A \otimes_S B$ e $\sigma, \tau \in G$,

$$\psi\Big((\sigma \otimes \tau)(a \otimes b)\Big) = \psi\Big(\sigma(a) \otimes \tau(b)\Big) = \sum_{\substack{1 \leq i \leq n(\sigma(a)) \\ 1 \leq j \leq m(\tau(b))}} s_i\Big(\sigma(a)\Big)t_j\Big(\tau(b)\Big) \otimes \sigma(a)_i \otimes \tau(b)_j$$

$$= \left(\sum_{i=1}^{n\left(\sigma(a)\right)} s_i\Big(\sigma(a)\Big) \otimes \sigma(a)_i \otimes 1\right)\left(\sum_{j=1}^{m\left(\tau(b)\right)} t_j\Big(\tau(b)\Big) \otimes 1 \otimes \tau(b)_j\right)$$

$$= \left(\sum_{i=1}^{n(a)} s_i(a) \otimes \sigma(a_i) \otimes 1\right)\left(\sum_{j=1}^{m(b)} t_j(b) \otimes 1 \otimes \tau(b_j)\right)$$

$$= \sum_{\substack{1 \leq i \leq n(a) \\ 1 \leq j \leq m(b)}} s_i(a)t_j(b) \otimes \sigma(a_i) \otimes \tau(b_j) = (1 \otimes \sigma \otimes \tau)\psi(a \otimes b).$$

Conseqüentemente,

$$(A \otimes_S B)^{\delta G} \overset{\psi}{\approx} (S \otimes_R A_0 \otimes_R B_0)^{1 \otimes \delta G} = S \otimes_R (A_0 \otimes_R B_0)^{\delta G}$$

Pelo Teorema Fundamental da Teoria de Galois, $(A_0 \otimes_R B_0)^{\delta G}$ é extensão galoisiana de R com grupo de Galois $G \approx \dfrac{G \otimes G}{\delta G}$, ou seja, em $T(G;S)$, $[A] * [B] = [S \otimes (A_0 \otimes_R B_0)^{\delta G}]$. □

Podemos agora mostrar o isomorfismo desejado

2.2.3. Teorema

Sejam $p \in \mathbb{Z}$ *primo,* $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle} = R[\varepsilon]$ *onde* $\varepsilon = X + \langle \Phi_p(X) \rangle$, $\Gamma = \{\gamma_i \mid \gamma_i : \varepsilon \mapsto \varepsilon^i, 1 \leq i \leq p-1\}$ *subgrupo de* $Aut_R(S)$ *e* $\Phi_p(X)$ *o p-ésimo polinômio ciclotômico em* $R[X]$. *Então,*

$$\begin{array}{rccc} \varphi : & T_p(R) & \longrightarrow & T_p(S)^\Gamma \\ & [A;\sigma] & \longmapsto & [S \otimes_R A; 1 \otimes \sigma] \end{array}$$ *é um isomorfismo de grupos.*

Demonstração : A ação de Γ sobre $S \otimes_R A$ é via primeira coordenada. Logo, para cada $\gamma \in \Gamma$, $\gamma\varphi[A;\sigma] = \gamma[S \otimes A; 1 \otimes \sigma] = [{}_\gamma S \otimes A; 1 \otimes \sigma] = [S \otimes A; 1 \otimes \sigma] = \varphi[A;\sigma]$, isto é, $\varphi[A;\sigma] \in T_p(S)^\Gamma$. Consideremos agora $[A_1;\sigma_1] = [A_2;\sigma_2]$ em $T_p(R)$, e seja $f : A_1 \longrightarrow A_2$ isomorfismo de R-álgebras tal que $f\sigma_1 = \sigma_2 f$. Conseqüentemente, $1 \otimes f : S \otimes_R A_1 \longrightarrow S \otimes_R A_2$ é um isomorfismo de extensões de Galois. Logo, φ está bem definida, e segue do Lema anterior que φ é um homomorfismo de grupos. Mostremos que φ é bijetor.

Seja $[A;\sigma] \in Ker(\varphi)$, isto é, $[S \otimes_R A; 1 \otimes \sigma] = [S^p;\tau]$ onde $\tau(s_1, \ldots, s_p) = (s_p, s_1, \ldots, s_{p-1})$. Logo, existe $\beta : S \otimes_R A \longrightarrow S^p$ isomorfismo de S-álgebras tal que $\beta(1 \otimes \sigma) = \tau\beta$.

Para cada $\delta \in \Gamma$, definimos $\theta_\delta = \beta\delta\beta^{-1}\delta^{-1}$. Claramente $\theta_\delta \in \mathcal{A}ut_R(S^p)$. Observemos que Γ age sobre S^p via $\delta \cdot (s_1, \ldots, s_p) = (\delta(s_1), \ldots, \delta(s_p))$. Logo, para quaisquer $s \in S$ e $z \in S^p$,

$\theta_\delta(sz) = \beta\delta\beta^{-1}\delta^{-1}(sz) = \beta\delta\beta^{-1}(\delta^{-1}(s)\delta^{-1}(z)) = \beta\delta\Big(\delta^{-1}(s)\beta^{-1}\delta^{-1}(z)\Big) = s\,\theta_\delta(z)$,

isto é, $\theta_\delta \in \mathcal{A}ut_S(S^p)$. Por outro lado, a ação de Γ sobre $\mathcal{A}ut_S(S^p)$ é via conjugação: $\delta(\rho) = \delta\rho\delta^{-1}$, para quaisquer $\delta \in \Gamma$ e $\rho \in \mathcal{A}ut_S(S^p)$. Assim,

$\theta_{\delta_1\delta_2} = \beta\delta_1\delta_2\beta^{-1}\delta_2^{-1}\delta_1^{-1} = (\beta\delta_1\beta^{-1}\delta_1^{-1})\delta_1(\beta\delta_2\beta^{-1}\delta_2^{-1})\delta_1^{-1} = \theta_{\delta_1}\delta_1(\theta_{\delta_2})$

$= \theta(\delta_1)\delta_1\big(\theta(\delta_2)\big)$, para quaisquer $\delta_1, \delta_2 \in \Gamma = <\gamma>$. Portanto, a aplicação $\theta : \Gamma \longrightarrow \mathcal{A}ut_S(S^p)$, dada por $\theta(\delta) = \theta_\delta$ é um 1-cociclo.

Por outro lado, a ação de Γ comuta com a ação de τ. De fato:

$$\delta\tau(s_1, \ldots, s_p) = \delta(s_p, s_1, \ldots, s_{p-1}) = (\delta(s_p), \delta(s_1), \ldots, \delta(s_{p-1}))$$

$= \tau(\delta(s_1), \ldots, \delta(s_p)) = \tau\delta(s_1, \ldots, s_p)$, para qualquer $(s_1, \ldots, s_p) \in S^p$.

Além disso, para cada $\delta \in \Gamma$, $\theta_\delta\tau = \beta\delta\beta^{-1}\delta^{-1}\tau = \beta\delta\beta^{-1}\tau\delta^{-1}$

$= \beta\delta(\tau^{-1}\beta)^{-1}\delta^{-1} = \beta\delta\Big(\beta(1\otimes\sigma^{-1})\Big)^{-1}\delta^{-1} = \beta\delta(1\otimes\sigma)\beta^{-1}\delta^{-1}$

$= \beta(1\otimes\sigma)\delta\beta^{-1}\delta^{-1} = \tau\beta\delta\beta^{-1}\delta^{-1} = \tau\theta_\delta$, ou seja,

$$\theta_\delta \in \Delta = \{w \in \mathcal{A}ut_S(S^p) \mid w\tau = \tau w\}.$$

Observemos que $\Delta \subseteq \mathcal{U}(S < \tau >)$. De fato, por ([6], Theorem 3.1), para cada $w \in \Delta$, existem $e_{i,w} \in S^p$, $0 \leq i \leq p-1$ idempotentes ortogonais com soma 1, tais que $w = \sum_{i=0}^{p-1} e_{i,w}\tau^i$. Já que $w\tau = \tau w$, segue que $\sum_{i=0}^{p-1} e_{i,w}\tau^{i+1} = \sum_{i=0}^{p-1} \tau(e_{i,w})\tau^{i+1}$. Então, $e_{i,w} = \tau(e_{i,w})$, isto é, $e_{i,w} \in (S^p)^{\langle\tau\rangle} = S$, para todo $0 \leq i \leq p-1$. Assim, mostramos que

$\Delta = \{w = \sum_{i=0}^{p-1} e_{i,w}\tau^i \mid \{e_{i,w}\}_{i=0}^{p-1}$ *é uma família de idempotentes de* S *dois a dois ortogonais e com soma 1*$\}$. Como S e $\langle\tau\rangle$ são comutativos, segue

que Δ é comutativo. Além disso, Δ é Γ-módulo via a conjugação.

Já vimos que $\theta : \Gamma \longrightarrow \Delta$, $\delta \mapsto \theta_\delta$ é 1-cociclo. Logo $\overline{\theta} \in H^1(\Gamma, \Delta)$, e portanto $\overline{\theta}^{p-1} = \overline{1}$, onde $1 : \Gamma \longrightarrow \Delta$ associa a cada $\delta \in \Gamma$ a identidade id_{S^p} ([42], Theorem 10.26). Por outro lado, para qualquer $\theta_\delta \in \Delta$, $\theta_\delta = \sum_{i=0}^{p-1} e_{i,\delta}\tau^i$ onde $\{e_{i,\delta}\}_{i=0}^{p-1}$ é uma família de idempotentes de S dois a dois ortogonais com soma 1, para todo $0 \leq i \leq p-1$. Então,

$$\theta_\delta^p = \left(\sum_{i=0}^{p-1} e_{i,\delta}\tau^i\right)^p = \sum_{i=0}^{p-1} e_{i,\delta}\tau^{ip} = \left(\sum_{i=0}^{p-1} e_{i,\delta}\right) id_{S^p} = 1 \cdot id_{S^p} = id_{S^p},$$

ou ainda, para cada $\delta \in \Gamma$, $\theta^p(\delta) = \theta_\delta^p = id_{S^p}$. Logo, $\overline{\theta^p} = \overline{1}$ e portanto, $\overline{1} = \overline{\theta}^p = \overline{\theta}^{p-1}\overline{\theta} = \overline{\theta}$. Conseqüentemente, $\overline{\theta} = \overline{1}$ em $H^1(\Gamma, \Delta)$, ou seja, θ é um 1-cobordo. Logo existe $w \in \Delta$ tal que $\theta(\delta) = \delta(w) \cdot w^{-1}$, para qualquer $\delta \in \Gamma$. Então, $\theta(\delta) = \beta\delta^{-1}\beta^{-1}\delta^{-1} = \delta(w)w^{-1} = \delta w\delta^{-1} \cdot w^{-1} = w^{-1}\delta w\delta^{-1}$, e portanto obtemos que $\beta\delta\beta^{-1} = w^{-1}\delta w$, ou seja, $(w\beta)\delta = \delta(w\beta)$, para cada $\delta \in \Gamma$. Assim, o isomorfismo $w\beta : S \otimes_R A \xrightarrow{\beta} S^p \xrightarrow{w} S^p$ nos mostra que

$$A \overset{\mu}{=} R \otimes_R A = S^\Gamma \otimes_R A = (S \otimes_R A)^\Gamma \overset{w\beta}{\approx} (S^p)^\Gamma = R^p,$$

isto é, $A \overset{w\beta}{\approx} R^p$. Além disso, $w\beta \cdot 1 \otimes \sigma = w\tau\beta = \tau w\beta$, e portanto $[A] = [R^p] = e_G(R)$. Conseqüentemente, φ é injetor.

Para mostrar a sobrejetividade de φ é suficiente verificar que $[A;\sigma]^{(p-1)} \in \varphi\big(T_p(R)\big)$, pois $h : T_p(S)^\Gamma \longrightarrow T_p(S)^\Gamma$ dado por $h([A;\sigma]) = [A;\sigma]^{(p-1)} = [A;\sigma]^{-1}$ é um isomorfismo de grupos. Observemos que

$$h([A;\sigma]) = [A;\sigma]^{(p-1)} = \prod_{i=1}^{p-1} \gamma_i\big([A;\sigma]\big), \quad \text{pois } [A;\sigma] \in T_p(S)^\Gamma.$$

Seja $B = \prod_{i=1}^{p-1} \gamma_i\big([A;\sigma]\big) = \prod_{i=1}^{p-1} [\gamma_i A;\sigma]$. Então,

$B = [(\otimes_{i=1}^{p-1}{}_{\gamma_i}A)^N; \sigma \otimes 1 \otimes \ldots \otimes 1]$, onde N é o núcleo da multiplicação $m : \prod_{i=1}^{p-1} \frac{\mathbb{Z}}{p\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{p\mathbb{Z}}$ definida por $m(\overline{z_1}, \ldots, \overline{z_{p-1}}) = \overline{\prod_{i=1}^{p-1} z_i}$ e $\prod_{i=1}^{p-1} \frac{\mathbb{Z}}{p\mathbb{Z}}$ age sobre $\left(\otimes_{i=1}^{p-1} A\right)$ coordenada a coordenada. Para simplificar a notação, também denotamos por B a S-álgebra $\left(\otimes_{i=1}^{p-1}{}_{\gamma_i}A\right)^N$.

Agora, para cada $\gamma_i \in \Gamma$, $1 \leq i \leq p-1$, definimos $\tilde{\gamma}_i : B \longrightarrow B$ do seguinte modo: $\tilde{\gamma}_i|_S = \gamma_i$ e $\tilde{\gamma}_i(b) = \otimes_{j=1}^{p-1} a_{ij(\mathrm{mod}\, p)}$, para todo elemento básico $b = \otimes_{j=1}^{p-1} a_j \in B$. Assim, $\tilde{\gamma}_i$ permuta as coordenadas de b: na j-ésima posição temos $a_{ij(\mathrm{mod}\, p)}$ substituindo a_j. Claramente, dado $r \in R$, temos que $\tilde{\gamma}_i(r) = \gamma_i(r) = r$, e então $\tilde{\gamma}_i \in \mathcal{A}ut_R(B)$, para todo $1 \leq i \leq p-1$. Da definição de B, segue que $\sigma \otimes 1 \otimes \ldots \otimes 1$ age identicamente a $1 \otimes \ldots \otimes 1 \otimes \sigma \otimes 1 \otimes \ldots \otimes 1$, e conseqüentemente, $\sigma\tilde{\gamma}_i = \tilde{\gamma}_i\sigma$, para todo $1 \leq i \leq p-1$.

Além disso, $\tilde{\Gamma} = \{\tilde{\gamma}_i \mid 1 \leq i \leq p-1\}$ é um grupo cíclico de ordem $p-1$. Sejam $\tilde{\Gamma} =< \tilde{\gamma} >$ e $B_0 = B^{\tilde{\Gamma}}$. Mostremos que $[B_0] \in T(G;R)$ e $[B] = [S \otimes_R B_0]$. Seja $\mathcal{M} \in \mathcal{M}ax(R)$. Então, segue de ([1], Proposition 5.6) que $S_{\mathcal{M}}$ é uma extensão inteira de $R_{\mathcal{M}}$. Mas Γ é um subgrupo finito de $\mathcal{A}ut_{R_{\mathcal{M}}}(S_{\mathcal{M}})$, e $S_{\mathcal{M}}^{\Gamma} \approx R_{\mathcal{M}}$. Assim, como $R_{\mathcal{M}}$ é local, $S_{\mathcal{M}}$ é um anel semi-local (Lema 1.2.6).

Conseqüentemente, pelo teorema ([6], Theorem 4.2-c), $B_{\mathcal{M}}$ tem $S_{\mathcal{M}}$-base normal. Consideremos o homomorfismo de S-álgebras induzido pela multiplicação $\mu : S \otimes_R B_0 \longrightarrow B$. Pelo Lema 2.2.1, $\mu_{\mathcal{M}} : S_{\mathcal{M}} \otimes_{R_{\mathcal{M}}} \left(B_{\mathcal{M}}\right)_0 \longrightarrow B_{\mathcal{M}}$ é um $R_{\mathcal{M}}$-isomorfismo de álgebras para qualquer $\mathcal{M} \in \mathcal{M}ax(R)$. Por outro lado, para todo $\mathcal{M} \in \mathcal{M}ax(R)$,

$$B_{\mathcal{M}} \overset{\mu_{\mathcal{M}}}{\approx} S_{\mathcal{M}} \otimes_{R_{\mathcal{M}}} \left(B_{\mathcal{M}}\right)_0 = S_{\mathcal{M}} \otimes_{R_{\mathcal{M}}} \left(B_0\right)_{\mathcal{M}} \approx \left(S \otimes_R B_0\right)_{\mathcal{M}}.$$

Então, pelo Princípio Local-Global ([31], corol. iv.7 pg. 261)

$\mu : S \otimes_R B_0 \longrightarrow B$, induzido pela multiplicação $\mu(s \otimes b) = sb$, para qualquer $(s \otimes b)$ elemento básico de $S \otimes B_0$, é um isomorfismo de R-álgebras. Já que μ é S-linear e que $\mu\sigma = \sigma\mu$, $[B] = [S \otimes_R B_0]$ em $T_p(S)$. Mas S é um R-módulo fielmente plano e portanto $[B_0] \in T_p(R)$ (Lema 1.1.8). Ou seja, $[B] = \varphi([B_0])$. Logo φ é um isomorfismo de grupos. □

2.3 O isomorfismo $H_p(R) \approx H_p(S)^{\Gamma}$

Dados M um grupo abeliano e H um grupo finito agindo sobre M, a norma em M relativa a H (ver [10]) $\eta_{H,M} : M \longrightarrow M$ é definida por $\eta_{H,M}(m) = \prod_{h \in H} h \cdot m$, para qualquer $m \in M$. O próximo lema descreve $M^H = \{m \in M \mid h \cdot m = m, \text{ para qualquer } h \in H\}$ em função de η. Na verdade, fazemos uma restrição sobre a torsão de M, mas observamos que a hipótese assumida é claramente satisfeita pelos grupos com os quais vamos trabalhar.

2.3.1. Lema

Sejam M um grupo abeliano e H um grupo finito agindo sobre M. Se M é de torsão $n = |H|+1$, então $\eta_{H,M}\left(M\right) = M^H$.

Demonstração : Claramente, $\eta_{H,M}\left(M\right) \subseteq M^H$. Reciprocamente, dado $m \in M^H$, temos que $\eta_{H,M}(m) = m^{|H|} = m^{n-1}$, e portanto,

$(\eta_{H,M})^2(m) = m^{(n-1)^2} = m$, desde $m^n = 1$. Logo, $m \in \eta_{H,M}\Big(M\Big)$. □

Para mostrar que $H_p(R) \approx H_p(S)^\Gamma$, observemos que o monomorfismo $j : G_p(S) \longrightarrow T_p(S)$ da seqüência de L. Childs é Γ-linear (secção 2.1). Mas $j = \theta$, onde $G_p(S) \overset{\theta}{\approx} H_p(S)$ é o isomorfismo dado no Teorema 1.4.1. Conseqüentemente, $G_p(S)^{*\Gamma} \overset{\theta|}{\approx} H_p(S)^\Gamma$. Assim, vamos mostrar que os grupos $H_p(R)$ e $G_p(S)^{*\Gamma}$ são isomorfos. Para isso, consideremos a norma em $G_p(S)$ relativa a Γ, $\eta = \eta_{\Gamma,G_p(S)} : G_p(S) \longrightarrow G_p(S)$ dada por

$\eta(\overline{a}) = \prod_{i=0}^{p-2} \gamma_i * \overline{a} = \prod_{i=0}^{p-2} \overline{\gamma_i^{-1}(a^i)}$ para todo $\overline{a} \in G_p(S)$, conhecida como a norma de Stickelberger. Recordemos que $\Gamma = \langle\gamma\rangle$ com $\gamma = \gamma_t$ e $1 \leq t, l \leq p-1$ tais que $tl \equiv 1 (\mathrm{mod}\, p)$. É fácil ver que, para cada $\overline{a} \in G_p(S)$, $\eta(\overline{a}) = \prod_{i=0}^{p-2} \overline{\gamma^{-i}(a^{t^i})}$.

O corolário a seguir é imediato:

2.3.2. Corolário

$\eta\Big(G_p(S)\Big) = G_p(S)^{*\Gamma}$

A partir deste corolário e do próximo lema, podemos construir o isomorfismo proposto nesta secção.

Denotaremos por $E_p(S)$ o subgrupo $\varphi(H_p(R))$ de $T_p(S)^\Gamma$, onde φ é o isomorfismo dado pelo Teorema 2.2.3. Vamos mostrar que $E_p(S)$ é um grupo isomorfo à $\eta\big(G_p(S)\big)$.

2.3.3. Lema

Seja p um primo ímpar. Então $\eta\big(G_p(S)\big) \approx E_p(S)$

Demonstração : Observemos que $H_p(S) \overset{\theta^{-1}}{\approx} G_p(S)$, onde θ é o isomorfismo dado pelo Teorema 1.4.1. Assim, basta verificar que $\theta^{-1}(E_p(S)) = \eta\big(G_p(S)\big)$.

Seja $[A] \in E_p(S)$. Então existe $A_0 \in H_p(R)$ tal que $[A] = [S \otimes_R A_0]$. Além disso, se $\{\alpha_i = \sigma^i(\alpha_0)\}_{i=0}^{p-1}$ é uma R-base normal de A_0, então $\{1 \otimes \alpha_i\}_{i=0}^{p-1}$ é uma S-base normal de $S \otimes_R A_0$ e conseqüentemente A possui S-base normal. Assim, temos $[A] \in E_p(S) \cap H_p(S) \subseteq T_p(S)^\Gamma \cap H_p(S) = H_p(S)^\Gamma$. Por outro lado, $H_p(S) = \theta(G_p(S)) = j(G_p(S))$ (Teorema 1.4.1) e, como j é Γ-linear (ver secção 2.1), temos $H_p(S)^\Gamma \overset{\theta^{-1}}{\approx} G_p(S)^{*\Gamma}$. Agora, segue do Corolário 2.3.2 que $\theta^{-1}([A]) \in G_p(S)^{*\Gamma} = \eta(G_p(S))$.

Reciprocamente, dado $\overline{a} \in \eta\big(G_p(S)\big) = G_p(S)^{*\Gamma}$, seja $A = \dfrac{S[X]}{\langle f(X)\rangle} = S[x]$, com $f(X) \in S[X]$ mônico tal que $(\lambda X + 1)^p - a = \lambda^p f(X)$ (Corolário 1.2.5) e $x = X + \langle f(X)\rangle$. A ação de G sobre A é dada por $\sigma(x) = \varepsilon x + 1$. Como $\lambda^p f\big(\sigma(x)\big) = (\lambda\sigma(x) + 1)^p - a = \big(\lambda(\varepsilon x + 1) + 1\big)^p = (\lambda\varepsilon x + \lambda + 1)^p = (\lambda\varepsilon x + \varepsilon)^p = \varepsilon(\lambda x + 1)^p = (\lambda x + 1)^p - a = \lambda^p f(x) = 0$, isto é, $f\big(\sigma(x)\big) = 0$, obtemos que a ação está bem definida. Seja $z = 1 + \lambda x$. Então, $z^p = (1 + \lambda x)^p = \lambda^p f(x) + a = a$, isto é, $z^p = a \in \mathcal{U}_{\lambda^p}(S)$ e portanto $\theta^{-1}([A]) = \overline{a}$. Pelo Teorema 1.4.1, $[A] \in H_p(S)$. Mostremos que $[A] \in E_p(S)$. Como $\overline{a} \in \eta\big(G_p(S)\big)$, existe $d \in \mathcal{U}_{\lambda^p}(S)$ tal que $\eta(\overline{d}) = \overline{\prod_{k=0}^{p-2} \gamma^{-k}\Big(d^{t^k}\Big)} = \overline{a}$,

onde t satisfaz $tl \equiv 1 (\mathrm{mod}\, p)$ com $1 \leq t, l \leq p-1$. Conseqüentemente, existe $u \in \mathcal{U}_\lambda(S)$ satisfazendo $a = \prod_{k=0}^{p-2} \gamma^{-k}(d)^{t^k} u^p$, ou seja, $au^{-p} = \prod_{k=0}^{p-2} \gamma^{-k}(d)^{t^k}$.

Assim, substituindo a por au^{-p}, podemos supor que $a = \prod_{k=0}^{p-2} \gamma^{-k}(d)^{t^k}$. Então,

$$\gamma(a)a^{-t} = \gamma\left(\prod_{k=0}^{p-2}\gamma^{-k}(d)^{t^k}\right)\left(\prod_{k=0}^{p-2}\gamma^{-k}(d)^{t^k}\right)^{-t} = d^{\left(\sum_{k=0}^{p-2} t^k\gamma^{-k}\right)\left(\gamma-t\right)}$$

$$= d^{\gamma\left(1-t^{(p-1)}\right)} = \gamma\left(d^{1-t^{(p-1)}}\right). \quad \text{Já que } t^{(p-1)} = p(-r)+1 \quad \text{para algum}$$

$r \in \mathbb{Z}$, temos $\dfrac{1-t^{(p-1)}}{p} = r \in \mathbb{Z}$. Seja $c = d^r$. Assim,

$$\gamma(a)a^{-t} = \gamma\left(d^{rp}\right) = \gamma(c^p) = \gamma(c)^p, \quad \text{e portanto,} \quad \gamma(a) = a^t\gamma(c)^p.$$

Definimos $\tilde{\gamma} : A \longrightarrow A$ satisfazendo $\tilde{\gamma}(s) = \gamma(s)$, para qualquer $s \in S$ e $\tilde{\gamma}(z) = \gamma(c)z^t$. De $\tilde{\gamma}(z)^p = \gamma(c^p)z^{p^t} = \gamma(c^p)a^t = \gamma(a) = \tilde{\gamma}(z^p)$, segue que $\tilde{\gamma}$ está bem definido com respeito a z. Para obtermos a boa definição de $\tilde{\gamma}$ com respeito a x, precisamos primeiramente verificar que $c = d^r \in \mathcal{U}_\lambda(S)$. Mas $d \in \mathcal{U}_{\lambda^p}(S)$. Logo $d \in \mathcal{U}(S)$ e existe $d_0 \in S$ tal que $d = 1 + \lambda^p d_0$. Conseqüentemente, $d^r \in \mathcal{U}(S)$ e $c = d^r = (1+\lambda^p d_0)^r = 1 + \sum_{k=1}^{r}\binom{r}{k}\lambda^{p^k}d_0^k$

$$= 1 + \lambda\left(\sum_{k=1}^{r}\binom{r}{k}\lambda^{(p^k-1)}d_0^k\right) \in \mathcal{U}_\lambda(S). \text{ Agora, observemos que } c = 1+\lambda c_0,$$

com $c_0 \in S$ e

$$\tilde{\gamma}(1+\lambda x) = \tilde{\gamma}(z) = \gamma(c)z^t = \gamma(1+\lambda c_0)(1+\lambda x)^t$$

$$= (1+\gamma(\lambda)\gamma(c_0))(1+\lambda b) = 1 + \gamma(\lambda)\Big(\gamma(c_0) + \gamma(c_0)\lambda b\Big) + \lambda b,$$

onde $b \in A$ é dado por $b = \sum_{k=1}^{t}\binom{t}{k}\lambda^{(k-1)}x^k$. Mas, pelo Lema 1.2.3, existe $s \in S$ tal que $\lambda = \gamma(\lambda)s$, isto é,

$$1 + \gamma(\lambda)\tilde{\gamma}(x) = 1 + \gamma(\lambda)\Big(\gamma(c_0) + \gamma(c_0)\lambda b + sb\Big)$$

e obtemos que $\tilde{\gamma}(x) = \gamma(c_0) + \gamma(c_0)\lambda b + sb$, ou seja, $\tilde{\gamma}(x) = \gamma(c_0)z^t + sb$. Isto nos dá a boa definição de $\tilde{\gamma}$ com respeito a x. Mostremos que $\tilde{\gamma} \in \mathcal{A}ut_R(A)$ e que $\sigma\tilde{\gamma} = \tilde{\gamma}\sigma$. Temos $\tilde{\gamma}^{(p-1)}(z) = \beta z$, com $\beta \in \mathcal{U}_\lambda(S)$ ou, equivalentemente, $\tilde{\gamma}^{(p-1)}(z)\beta^{-1} = z$. Logo,

$\beta^{-1}\Big(1 + \gamma^{(p-1)}(\lambda)\tilde{\gamma}^{(p-1)}(x)\Big) = \beta^{-1}\tilde{\gamma}^{(p-1)}(z) = z = 1 + \lambda x$, isto é,

$\beta^{-1}\Big(1 + \lambda\tilde{\gamma}^{(p-1)}(x)\Big) = 1 + \lambda x = \beta^{-1}(\beta + \lambda\beta x)$, ou ainda,

$1 + \lambda\tilde{\gamma}^{(p-1)}(x) = \beta + \lambda\beta x$. Seja $\beta_0 \in S$ tal que $\beta = 1 + \lambda\beta_0$. Então, $1 + \lambda\tilde{\gamma}^{(p-1)}(x) = (1 + \lambda\beta_0) + \lambda\beta x = 1 + \lambda(\beta_0 + \beta x)$. Como $\lambda \in R^\times$, $\tilde{\gamma}^{(p-1)}(x) = \beta_0 + \beta x$. Conseqüentemente, $x = \beta^{-1}\tilde{\gamma}^{(p-1)}(x) - \beta^{-1}\beta_0 = \tilde{\gamma}\Big(\gamma^{-1}(\beta^{-1})\tilde{\gamma}^{(p-2)}(x) - \gamma^{-1}(\beta^{-1}\beta_0)\Big)$, e portanto $\tilde{\gamma}$ é sobrejetor. Segue que $\tilde{\gamma}$ é bijetor ([27], I.2.4). Claramente, $\tilde{\gamma}$ é R-linear, e então $\tilde{\gamma} \in \mathcal{A}ut_R(A)$.

Finalmente, $z^{-1}\tilde{\gamma}^{(p-1)}(z) = z^{t^{(p-1)}-1} \cdot \prod_{k=0}^{p-2} \gamma^{-k}(c)^{t^k} = a^{-r}c^{(\sum_{k=0}^{p-2} t^k\gamma^{-k})}$

$= d^{(\sum_{k=0}^{p-2} t^k\gamma^{-k})(-r)} \cdot d^{r(\sum_{k=0}^{p-2} t^k\gamma^{-k})} = d^0 = 1,$

e portanto $\tilde{\gamma}^{(p-1)}(z) = z$. Agora,

$$1 + \lambda x = z = \tilde{\gamma}^{(p-1)}(z) = \tilde{\gamma}^{(p-1)}(1 + \lambda x)$$
$$= 1 + \gamma^{(p-1)}(\lambda)\tilde{\gamma}^{(p-1)}(x) = 1 + \lambda\tilde{\gamma}^{(p-1)}(x),$$

e então $x = \tilde{\gamma}^{(p-1)}(x)$, ou seja, $\tilde{\gamma}$ tem ordem $p - 1$. Pelo Lema 2.2.1, segue que $[A] \in E_p(S)$. □

Do Corolário 2.3.2 e Lema 2.3.3 temos o

2.3.4. Teorema

Sejam $p \in \mathbb{Z}$ primo, $S = \dfrac{R[X]}{\langle\Phi_p(X)\rangle} = R[\varepsilon]$ onde $\Phi_p(X)$ é o p-ésimo polinômio ciclotômico em $R[X]$, $\varepsilon = X + \langle\Phi_p(X)\rangle$ é uma raiz primitiva

p-ésima da unidade em S *e* $\Gamma = \{\gamma_i \mid \gamma_i : \varepsilon \mapsto \varepsilon^i, 1 \leq i \leq p-1\}$ *subgrupo de* $Aut_R(S)$. *Então,*

$$H_p(R) \approx G_p(S)^{*\Gamma} \approx H_p(S)^{\Gamma}.$$

2.4 O isomorfismo $PrimPic_p(R[G]) \approx \Big(PrimPic_p(S[G])\Big)^{\Gamma}$

Para obter o isomorfismo desejado, utilizamos a seqüência cohomológica construída na secção 1.5 e os isomorfismos construídos nas duas secções anteriores. O lema a seguir, é uma conseqüência imediata do Lema 2.3.1.

2.4.1. Lema

Seja $\eta = \eta_{\Gamma, PrimPic_p(S[G])}$ *a norma em* $PrimPic_p(S[G])$ *relativa a* Γ. *Então,* $\eta\Big(PrimPic_p(S[G])\Big) = \Big(PrimPic_p(S[G])\Big)^{\Gamma}$

Observemos que $S[G] \approx S \otimes_R R[G]$ é uma $R[G]$-álgebra fielmente projetiva, pois S é uma R-álgebra fielmente projetiva. Por outro lado, como $1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{p-1} = 0$ segue que $tr(-\varepsilon) = \sum_{\gamma \in \Gamma} \gamma(-\varepsilon) = 1$, isto é, tomando $c = -\varepsilon$ no Teorema 1.5.1 obtemos, para os anéis $R[G] \subseteq S[G]$, que a seqüência abaixo é exata:

$$1 \longrightarrow H^1\Big(\Gamma, \mathcal{U}(S[G])\Big) \xrightarrow{\eta_1} Pic(R[G]) \xrightarrow{\eta_2} Pic(S[G])^{\Gamma} \xrightarrow{\eta_3} H^2\Big(\Gamma, \mathcal{U}(S[G])\Big)$$

onde, em particular, $\eta_2(\overline{P}) = \overline{S \otimes_R P}$.

Vamos verificar que a restrição de η_2 ao subgrupo $PrimPic_p(R[G])$ nos dá o isomorfismo de grupos proposto. Denotemos esta restrição de η_2 por η_2', e mostremos que

$$\eta_2'(PrimPic_p(R[G])) = PrimPic_p(S[G])^\Gamma \quad \text{e} \quad Ker\eta_2' = 1.$$

2.4.2. Lema

A aplicação de grupos $Pic(R[G]) \longrightarrow Pic(S[G])$ *dada por* $\overline{P} \mapsto \overline{S \otimes_R P}$ *induz um homomorfismo de grupos* $PrimPic_p(R[G]) \longrightarrow PrimPic_p(S[G])^\Gamma$

Demonstração : É suficiente verificar que, para cada elemento primitivo $\overline{P}$ em $Pic(R[G])$, $\overline{S \otimes_R P}$ é um elemento primitivo de p-torsão em $Pic(S[G])$.

Seja $\overline{P} \in PrimPic_p(R[G])$. Então, segue da definição de um elemento primitivo (ver [9]) que existe um isomorfismo de $R[G \times G]$-módulos $\phi : P \otimes_R P \longrightarrow R[G \times G] \otimes^{\Delta}_{R[G]} P$, onde $R[G]$ age sobre $R[G \times G]$ via $\Delta : R[G] \longrightarrow R[G \times G]$ com $\Delta(\sigma) = (\sigma, \sigma)$.

Assim, $\Psi : (S \otimes_R P) \otimes_S (S \otimes_R P) \longrightarrow S[G \times G] \otimes^{\Delta}_{S[G]} (S \otimes_R P)$ induzido por $\Psi(s \otimes m \otimes t \otimes n) = \sum_i sr_i(\sigma_i, \tau_i) \otimes t \otimes a_i$ é um homomorfismo de $S[G \times G]$-módulos, onde $\left(\sum_i r_i(\sigma_i, \tau_i) \otimes a_i\right) \in R[G \times G] \otimes^{\Delta}_{R[G]} P$ é univocamente determinado por ϕ. De fato, como a aplicação definida do produto cartesiano $(S \otimes_R P) \times (S \otimes_R P)$ no produto tensorial $S[G \times G] \otimes^{\Delta}_{S[G]} (S \otimes_R P)$ que associa a cada $(s \otimes m, t \otimes n)$ o elemento $\sum_i sr_i(\sigma_i, \tau_i) \otimes t \otimes a_i$ é aditiva nas duas coordenadas e S-balanceada, Ψ está bem definido. Além disso, é fácil verificar que Ψ é um homomorfismo de $S[G \times G]$-módulos. Por outro lado,

$1 \otimes \Psi : S \otimes_R (S \otimes_R P) \otimes_S (S \otimes_R P) \longrightarrow S \otimes_R S[G \times G] \otimes^{\Delta}_{S[G]} (S \otimes_R P)$ induzida por $(1 \otimes \Psi)\big(\alpha \otimes (s \otimes m) \otimes (t \otimes n)\big) = \alpha \otimes \big(sr(\sigma, \tau)\big) \otimes \big(t \otimes a\big)$ para quaisquer $\alpha, s, t \in S$ e $m, n \in P$ onde $\phi(m \otimes n) = r(\sigma, \tau) \otimes a$ com $r \in R$, $\sigma, \tau \in G$ e $a \in P$ é um isomorfismo de $S[G \times G]$-módulos. De fato,

usando as propriedades associativa e comutativa do produto tensorial, segue que

$$S \otimes_R (S \otimes_R P) \otimes_S (S \otimes_R P) \approx (S \otimes_R P) \otimes_R S \otimes_S (S \otimes_R P)$$
$$\alpha \otimes (s \otimes m) \otimes (t \otimes n) \longmapsto s \otimes m \otimes \alpha \otimes t \otimes n$$

$$(S \otimes_R P) \otimes_R S \otimes_S (S \otimes_R P) \approx P \otimes_R S \otimes_R S \otimes_S P \otimes_R S$$
$$s \otimes m \otimes \alpha \otimes t \otimes n \longmapsto m \otimes s \otimes \alpha \otimes n \otimes t$$

$$P \otimes_R S \otimes_R S \otimes_S P \otimes_R S \approx (P \otimes_R P) \otimes_R (S \otimes_S S \otimes_R S)$$
$$m \otimes s \otimes \alpha \otimes n \otimes t \longmapsto m \otimes n \otimes t \otimes s \otimes \alpha$$

$$(P \otimes_R P) \otimes_R (S \otimes_S S \otimes_R S) \overset{\phi \otimes 1}{\approx} R[G \times G] \otimes^{\Delta}_{R[G]} P \otimes_R (S \otimes_S S \otimes_R S)$$
$$m \otimes n \otimes t \otimes s \otimes \alpha \longmapsto \phi(m \otimes n) \otimes t \otimes s \otimes \alpha$$

$$R[G \times G] \otimes^{\Delta}_{R[G]} P \otimes_R (S \otimes_S S \otimes_R S) \approx R[G \times G] \otimes^{\Delta}_{R[G]} (S \otimes_R P) \otimes_S S \otimes_R S$$
$$\Big(\sum_i r_i(\sigma_i, \tau_i) \otimes a_i\Big) \otimes t \otimes s \otimes \alpha \longmapsto \sum_i r_i(\sigma_i, \tau_i) \otimes t \otimes a_i \otimes s \otimes \alpha$$

$$R[G \times G] \otimes^{\Delta}_{R[G]} (S \otimes_R P) \otimes_S S \otimes_R S \approx S \otimes_S R[G \times G] \otimes^{\Delta}_{R[G]} (S \otimes_R P) \otimes_R S$$
$$\sum_i r_i(\sigma_i, \tau_i) \otimes t \otimes a_i \otimes s \otimes \alpha \longmapsto s \otimes \sum_i r_i(\sigma_i, \tau_i) \otimes t \otimes a_i \otimes \alpha$$

$$S \otimes_S R[G \times G] \otimes^{\Delta}_{R[G]} (S \otimes_R P) \otimes_R S \approx S \otimes_S S \otimes_R R[G \times G] \otimes^{\Delta}_{R[G]} (S \otimes_R P)$$
$$s \otimes \sum_i r_i(\sigma_i, \tau_i) \otimes t \otimes a_i \otimes \alpha \longmapsto \alpha \otimes s \otimes \sum_i r_i(\sigma_i, \tau_i) \otimes t \otimes a_i$$

Agora, aplicando as fórmulas associativas do produto tensorial ([5], Proposition IX.2.1) obtemos

$$S \underset{R \otimes_R S}{\otimes} (S \otimes_R R[G \times G]) \overset{\Delta}{\underset{R[G]}{\otimes}} (S \otimes_R P) \approx S \otimes_R (S \otimes_R R[G \times G]) \overset{\Delta}{\underset{S \otimes_R R[G]}{\otimes}} (S \otimes_R P)$$
$$\Big(\alpha \otimes s \otimes \sum_i r_i(\sigma_i, \tau_i)\Big) \otimes (t \otimes a_i) \longmapsto \alpha \otimes s \otimes \sum_i r_i(\sigma_i, \tau_i) \otimes t \otimes a_i$$

$$\Big(S \otimes_R S \otimes_R R[G\times G]\Big) \overset{\Delta}{\underset{S\otimes_R R[G]}{\otimes}} (S\otimes_R P) \;\approx\; S\otimes_R S[G\times G]\otimes^{\Delta}_{S[G]} (S\otimes_R P)$$

$$\alpha\otimes s\otimes \sum_i r_i(\sigma_i,\tau_i)\otimes t\otimes a_i \longmapsto \alpha\otimes\Big(\sum_i sr_i(\sigma_i,\tau_i)\Big)\otimes\big(t\otimes a_i\big)$$

Mas $\alpha\otimes\Big(\sum_i sr_i(\sigma_i,\tau_i)\Big)\otimes\big(t\otimes a_i\big) = (1\otimes\Psi)\big(\alpha\otimes s\otimes m\otimes t\otimes n\big)$, e portanto $1\otimes\Psi$ é a composição dos isomorfismos acima, o que mostra a afirmação. Como S é um R-módulo fielmente plano, pois $S = R[\varepsilon]$ é um R-módulo livre, segue que Ψ é um isomorfismo de $S[G\times G]$-módulos. Ou seja, $S\otimes_R P$ é um elemento primitivo em $Pic(S[G])$ (ver [9]). Já que P é de p-torsão, $\overline{S\otimes_R P} = \eta_2'(\overline{P}) \in PrimPic_p(S[G])^{\Gamma}$. □

É imediato que $\eta_2'\big(PrimPic_p(R[G])\big) \subseteq PrimPic_p(S[G])^{\Gamma}$. Reciprocamente, seja $\overline{P}$ um elemento primitivo em $Pic_p(S[G])^{\Gamma}$. Como $\pi : T_p(S)^{\Gamma} \longrightarrow PrimPic_p(S[G])^{\Gamma}$, que a cada extensão galoisiana de S com grupo de Galois G estável pela ação de Γ associa a sua classe em $Pic_p(S[G])$, é sobrejetora, podemos supor que P é uma extensão galoisiana de S com grupo de Galois G estável pela ação de Γ. Assim, existe $[P_0] \in T_p(R)$ tal que $S\otimes_R P_0 \approx P$ (Teorema 2.2.3). Em particular, P_0 é uma extensão galoisiana de R com grupo de Galois G. Portanto, $\overline{P_0}$ é um elemento primitivo em $Pic_p(R[G])$ ([9], Corollary 1.3), isto é, $\overline{P_0} \in PrimPic_p(R[G])$. Logo, $\overline{P} = \eta_2'(\overline{P_0})$, ou seja, $\eta_2'\big(PrimPic_p(R[G])\big) = PrimPic_p(S[G])^{\Gamma}$.

Por outro lado, $H^1(\Gamma, \mathcal{U}(S))$ é de (p-1)-torsão, pois $|\Gamma| = p-1$ e

$PrimPic_p(R[G])$ é de p-torsão. Portanto,

$$ker\eta_2' \subseteq \eta_1\big(H^1(\Gamma, \mathcal{U}(S[G]))\big) \cap PrimPic_p(R[G]) = 1,$$

isto é, η_2' é injetor. Conseqüentemente, η_2' é um isomorfismo. Desta forma, temos o

2.4.3. Teorema

Sejam $p \in \mathbb{Z}$ *primo,* $S = \dfrac{R[X]}{\langle \Phi_p(X) \rangle} = R[\varepsilon]$ *onde* $\Phi_p(X)$ *é o p-ésimo polinômio ciclotômico em* $R[X]$, $\varepsilon = X + \langle \Phi_p(X) \rangle$ *é uma raiz primitiva p-ésima da unidade em* S *e* $\Gamma = \{\gamma_i \mid \gamma_i : \varepsilon \mapsto \varepsilon^i, 1 \leq i \leq p-1\}$ *subgrupo de* $Aut_R(S)$. *Então,*

$$\begin{array}{rccc} \Psi : & PrimPic_p(R[G]) & \longrightarrow & PrimPic_p(S[G])^\Gamma \\ & \overline{P} & \longmapsto & \overline{S \otimes_R P} \end{array}$$

é um isomorfismo de grupos.

Finalmente, como conseqüência dos isomorfismos construídos nestas três últimas secções e da seqüência exata dada pelo Teorema 2.1.1, obtemos o

2.4.4. Teorema

Sejam R *um anel comutativo com unidade e* $p \in \mathbb{Z}$ *primo regular em* R. *Então, a seqüência abaixo é exata*

$$1 \longrightarrow H_p(R) \hookrightarrow T_p(R) \xrightarrow{\pi} PrimPic_p(R[G]) \longrightarrow 1$$

onde $\pi([A;\sigma]) = \overline{A}$.

Capítulo 3: Aplicação ao caso Cúbico

3.1 O grupo $G_3(S)^{*\Gamma}$

Nesta secção, damos uma descrição do grupo $G_3(S)^{*\Gamma}$ independente da *-ação de Γ. Seja, como antes, $\Gamma = \{id = \gamma_1, \gamma_2, \ldots, \gamma_{p-1} \mid \gamma_i : \varepsilon \mapsto \varepsilon^i$, para qualquer $1 \leq i \leq p-1\}$. Definimos a norma associada à Γ em $G_p(S)$ por $\mathcal{N}_\Gamma(\overline{a}) = \prod_{\gamma\in\Gamma} \overline{\gamma(a)}$, para cada $\overline{a} \in G_p(S)$. Então, como $G_p(S)$ é de p-torsão, $G_p(S)^{*\Gamma} \subseteq ker(\mathcal{N}_\Gamma)$. De fato, seja $\overline{a} \in G_p(S)^{*\Gamma}$. Para cada $1 \leq i \leq p-1$, $\overline{a} = \gamma_i * \overline{a} = \overline{\gamma_i^{-1}(a^i)}$. Conseqüentemente,

$$\mathcal{N}_\Gamma(\overline{a}) = \prod_{i=1}^{p-1} \gamma_i(\overline{a}) = \prod_{i=1}^{p-1} \overline{\gamma_i(\gamma_i^{-1}(a^i))} = \prod_{i=1}^{p-1} \overline{a^i} = \overline{a}^{1+2+\ldots+(p-1)} = \overline{a}^{\frac{p(p-1)}{2}} = \overline{1}.$$

Agora, para o caso cúbico vale a igualdade, isto é, $p = 3$ e $\Gamma = \{id, \gamma\}$ onde $\gamma : \varepsilon \mapsto \varepsilon^2$ e $\mathcal{N}_\Gamma(\overline{a}) = \overline{a}\gamma(\overline{a})$, para qualquer $\overline{a} \in G_3(S)$. Vemos isso no próximo lema:

3.1.1. Lema

$G_3(S)^{*\Gamma} = ker(\mathcal{N}_\Gamma)$.

Demonstração : Seja $\overline{a} \in G_3(S)$ tal que $\overline{a\gamma(a)} = \overline{1}$. Segue que $\overline{a^2\gamma(a^2)} = \overline{1}$. Aplicando γ^{-1} a esta igualdade, obtemos que $\overline{\gamma^{-1}(a^2)a^2} = \overline{1}$. Logo, $\overline{\gamma^{-1}(a^2)} =$

$(\overline{a}^2)^{-1} = \overline{a}$, ou equivalentemente, $\gamma * \overline{a} = \overline{a}$, isto é, $\overline{a} \in G_3(S)^{*\Gamma}$. □

Seja $D_\Gamma : G_3(S) \longrightarrow G_3(S)$ definida por $D_\Gamma(\overline{a}) = \overline{a/\gamma(a)}$. Claramente, $D_\Gamma\big(G_3(S)\big) \subseteq ker(\mathcal{N}_\Gamma)$. Reciprocamente, seja $\overline{a} \in G_3(S)$ tal que $\mathcal{N}_\Gamma(\overline{a}) = \overline{1}$. Assim, $\overline{a} = \overline{1/\gamma(a)} = \overline{\gamma(a^{-1})}$. Segue que $\overline{a} = \overline{a^2/a} = \overline{a^{-1}/\gamma(a^{-1})} = D_\Gamma(\overline{a^{-1}}) \in D_\Gamma\big(G_3(S)\big)$. Pelo Lema anterior $D_\Gamma\big(G_3(S)\big) = ker(\mathcal{N}_\Gamma) = G_3(S)^{*\Gamma}$. Conseqüentemente, D_Γ induz a função $D : \mathcal{U}_{\lambda^3}(S) \longrightarrow ker(\mathcal{N}_\Gamma) \subseteq G_3(S)$ dada por $D(a) = D_\Gamma(\overline{a}) = \overline{a/\gamma(a)}$.

Como $G_3(S)$ é de 3-torsão, $\Big(\mathcal{U}_\lambda(S)\Big)^3 \subseteq ker(D)$. Além disso, $\mathcal{U}_{\lambda^3}(R) \subseteq ker(D)$, pois γ é R-linear. Então, D é fatorada pela função $\pi : \dfrac{\mathcal{U}_{\lambda^3}(S)}{\mathcal{U}_{\lambda^3}(R)\cdot\Big(\mathcal{U}_\lambda(S)\Big)^3} \longrightarrow ker(\mathcal{N}_\Gamma) = D_\Gamma\big(G_3(S)\big) = G_3(S)^{*\Gamma}$ dada por $\pi(\overline{a}) = D(a) = \overline{a/\gamma(a)}$. Claramente, π é um homomorfismo de grupos.

3.1.2. Lema

π é um isomorfismo de grupos.

Demonstração : Dado $\overline{b} \in ker(\mathcal{N}_\Gamma) = D_\Gamma\big(G_3(S)\big)$, existe $a \in \mathcal{U}_{\lambda^3}(S)$ satisfazendo $\overline{b} = \overline{a/\gamma(a)} = D(a) = \pi(\overline{a})$, ou seja, π é sobrejetor.

Agora, seja $a \in \mathcal{U}_{\lambda^3}(S)$ tal que $\pi(\overline{a}) = \overline{1}$, isto é, $\pi(\overline{a})$ tem norma 1 relativa à Γ. Por outro lado, $\dfrac{a}{\gamma(a)} = t^3$ para algum $t \in \mathcal{U}_\lambda(S)$, ou seja, $\gamma(a) = \frac{a}{t^3}$. Mas t define uma classe $[t^3] \in H^1\Big(\Gamma, \big(\mathcal{U}_\lambda(S)\big)^3\Big)$. Seja $\mu_3 = \mu_3\Big(\mathcal{U}_\lambda(S)\Big) = \{a \in \mathcal{U}_\lambda(S) \mid a^3 = 1\}$, e consideremos a seqüência exata

$$1 \longrightarrow \mu_3\Big(\mathcal{U}_\lambda(S)\Big) \longrightarrow \mathcal{U}_\lambda(S) \longrightarrow \Big(\mathcal{U}_\lambda(S)\Big)^3 \longrightarrow 1,$$

que induz a seqüência exata (Lema da Serpente)

$$H^1\Big(\Gamma, \mu_3(\mathcal{U}_\lambda(S))\Big) \longrightarrow H^1\Big(\Gamma, \mathcal{U}_\lambda(S)\Big) \longrightarrow H^1\Big(\Gamma, (\mathcal{U}_\lambda(S))^3\Big) \xrightarrow{\partial} H^2\Big(\Gamma, \mu_3(S)\Big).$$

Mas, $H^1\Big(\Gamma, \mu_3(\mathcal{U}_\lambda(S))\Big) = 1$, pois $|\,\Gamma\,| = 2$ e μ_3 é de 3-torsão. Além disso, $2H^1\Big(\Gamma, (\mathcal{U}_\lambda(S))^3\Big) = 1$ ([42] Theorem 10.26). Logo, $2[t^3] = [t^6] = [1]$,

isto é, t^6 é um cobordo, e portanto, existe $u \in \mathcal{U}_\lambda(S)$ tal que $t^6 = \dfrac{u^3}{\gamma(u^3)}$.

Seja $z = \dfrac{a^2}{u^3} \in \mathcal{U}_{\lambda^3}(S)$. Então,

$$\gamma(z) = \frac{\gamma(a^2)}{\gamma(u^3)} = \frac{a^2}{t^6} \cdot \frac{1}{\gamma(u^3)} = \frac{a^2\,\gamma(u^3)}{u^3} \cdot \frac{1}{\gamma(u^3)} = \frac{a^2}{u^3} = z.$$

Conseqüentemente, $z \in \mathcal{U}_{\lambda^3}(S) \cap R = \mathcal{U}_{\lambda^3}(R)$. Assim,

$$a^2 = z\,u^3 \in \mathcal{U}_{\lambda^3}(R) \cdot \Big(\mathcal{U}_\lambda(S)\Big)^3,$$

ou seja, a classe de a^2 é a identidade em $\dfrac{\mathcal{U}_{\lambda^3}(S)}{\mathcal{U}_{\lambda^3}(R) \cdot \Big(\mathcal{U}_\lambda(S)\Big)^3}$. Segue que

$\overline{a} = \overline{a}\,\overline{1} = \overline{a}\,\overline{a}^2 = \overline{a}^3 = \overline{1}$, pois o grupo é de 3-torsão. Logo π é injetor.

□

Como conseqüência do Teorema 2.3.4 e dos dois Lemas acima obtemos o seguinte isomorfismo de grupos:

3.1.3. Teorema

$$H_3(R) \approx G_3(S)^{*\Gamma} \overset{\pi^{-1}}{\approx} \frac{\mathcal{U}_{\lambda^3}(S)}{\mathcal{U}_{\lambda^3}(R) \cdot \Big(\mathcal{U}_\lambda(S)\Big)^3}$$

Bibliografia

[1] M. F. Atiyah e I. G. MacDonald "Introduction to commutative algebra", Addison-Wesley, Massachusetts, 1969.

[2] M. Auslander e O. Goldman "The Brauer group of a commutative ring", Trans. AMS, 97 (1960) pg. 367-409.

[3] A. Borevich "Kummer extensions of rings", J.Soviet Math., 11 (1979) pg. 514-534.

[4] N. Bourbaki "Algèbre commutative", chapters I-II, Hermann, Paris, 1962, (Actualités Sci. Ind., nro. 1290).

[5] H. Cartan e S. Eilenberg "Homological Algebra", Princeton Univ. Press, Princeton, 1956.

[6] S. U. Chase, D. K. Harrison e A. Rosenberg "Galois theory and Galois cohomology of commutative rings", Mem. AMS, 52 (1965) pg. 1-19.

[7] S. U. Chase e A. Rosenberg "Amitsur cohomology and the Brauer group", Mem. AMS, 52 (1965) pg. 34-77.

[8] L. N. Childs "Abelian Galois extensions of rings containing roots of unity", Illionois J. Math., 15 (1971) pg. 273-280.

[9] L. N. Childs "The group of unramified Kummer extensions of prime degree", Proc. London Math. Soc., (3) 35 (1977) pg. 407-422.

[10] L. N. Childs "Cyclic Stickelberger cohomology and descent of Kummer extensions", Proc. AMS, (4) 90 (1984) pg. 505-510.

[11] F. DeMeyer e E. Ingraham "Separable algebras over commutative rings", Lecture Notes in Math., 181, Springer-Verlag, Berlin/N.Y., 1971.

[12] M. Ferrero, A. Paques, A. Solecki "On $\mathbb{Z}_p$-extensions of commutative rings", J. Pure and Appl. Algebra 72 (1991), 5-22.

[13] M. Ferrero e A. Paques "Galois theory of commutative rings revisited", Beiträge zur Algebra e Geometrie, (2) 38 (1997) pg. 399-410.

[14] G. Garfinkel e M. Orzech "Galois extensions as modules over the group ring", Canadian J. Math., 22 (1970) pg. 242-248.

[15] C. Greither, R. Haggenmüller "Abelsche Galoiserweiterungen von $R[X]$", Manuscripta Math. 38 (1982), 239-256.

[16] C. Greither "Cyclic Galois extensions of commutative rings", Lecture Notes in Math., 1534, Springer-Verlag, Berlin, 1992.

[17] C. Greither e R. Miranda "Galois extensions of prime degree", J. of Algebra, 124 (1989) pg. 354-366.

[18] R. Haggenmüller "Über Invarianten separabler Galoiserweiterungen kommutativer Ringe", Dissertation, Univ. München, 1979.

[19] R. Haggenmüller "Über die Gruppe der Galoiserweiterungen von Primahlgrad", Habilitationsschrift Univ. München, 1985.

[20] D. K. Harrison "Abelian extensions of commutative rings", Mem. AMS, 52 (1968) pg. 66-79.

[21] H. Hasse "Die Multiplikations gruppe der abelschen Korper mit fester Galoisgruppe", Abh. Math. Sem. Univ. Hamburg 16 (1949), 29-40.

[22] G. J. Januz "Separable algebras over commutative rings", Trans. AMS 122 (1966), 461-479.

[23] I. Kersten, J. Michaliček "Kummer theory without roots of unity", J. Pure and Appl. Algebra 50 (1988), 21-72.

[24] I. Kersten e J. Michaliček "$\mathbb{Z}_p$-extensions of complex multiplication fields", J. Number Theory, 32 (2) (1989) pg. 131-150.

[25] I. Kersten e J. Michaliček "On Vandiver's conjecture and $\mathbb{Z}_p$-extensions of $Q(\zeta_{p^n})$", J. Number Theory, 32 (3) (1989) pg. 371-386.

[26] H. F. Kreimer e M. Takeuchi "Hopf algebras and Galois extensions of an algebra", Indian Univ. Math. J. 30 (1981), 675-692.

[27] M. A. Knus e M. Ojanguren "Théorie de la descente et algèbres d'Azumaya", Lecture Notes in Math., 389, Springer-Verlag, Berlin/N.Y., 1974.

[28] D. A. Marcus "Number Fields", Springer-Verlag, N.Y., 1977.

[29] D. Maurer "Stickelberger's criterion, Galois algebras, and tame ramification in algebraic number fields", J. of Pure and Applied Algebra, 33 (1984) pg. 281-293.

[30] P. J. McCarthy "Algebraic extensions of fields", Blaisdel Pub., 1966.

[31] B. R. McDonald "Linear Algebra over Commutative Rings", Marcel Dekker, Inc., N.Y., 1984.

[32] T. Nagahara, A. Nakajima "On cyclic extensions of commutative rings", Math. J. Okayama Univ. 15 (1971), 81-90.

[33] A. Nakajima "On a group of cyclic extensions over commutative rings", Math. J. Okayama Univ. 16 (1972), 163-172.

[34] M. Orzech "A cohomological description of abelian Galois extensions", Trans. AMS, 137 (1969) pg. 481-499.

[35] M. Orzech "A cohomology theory for commutative Galois extensions", Math. Z., 105 (1978) 128-140.

[36] A. Paques e A. Micali "Sur le groupe des extensions cycliques", J. of Algebra, 63 (1980) pg. 268-278.

[37] A. Paques "On the primitive element and normal basis theorems", Communications in Algebra, 16(3) (1988) pg.443-455.

[38] A. Paques e A. Micali "Sur L'existence d'element primitif et base normale", Bull. Soc. Math. Belg. - Tijdschr. Belg. Wisk. Gen., 40 (1988), 2, serie A, pg. 289-295.

[39] A. Paques "On primitive element and normal basis for Galois p-extensions of a commutative ring", $3^{\text{ème}}$ Contact Franco-Belge en Algèbre, Montpellier 88, France, Cahiers Math. 39, Univ. Montpellier, (1992), 231-236.

[40] A. Paques "Teoría de Galois sobre anillos conmutativos", Universidad de Los Andes, Mérida, 1999.

[41] R. S. Pierce "Associative Algebras", Springer-Verlag, N.Y., 1982.

[42] J. J. Rotman "An introduction to homological algebra", Academic Press, Inc., Orlando, 1979.

[43] Ch. Small "The group of quadratic extensions". J. Pure Appl. Algebra 2 (1972), 83-105.

[44] C. A. Weibel "An introduction to homological algebra", Univ. Press, N.Y., 1995.

[45] T. Wyler "Torsors under abelian p-groups", J. Pure and Appl. Algebra 45 (1987), 273-286.