Universidade Federal do Rio Grande do Sul
Instituto de Matemática

EXTENSÕES DE GALOIS DE ANÉIS COMUTATIVOS DE CARACTERÍSTICA p.

por
ALVERI ALVES SANT' ANA

Dissertação submetida ao curso de Pós-Graduação em Matemática como requisito parcial para a obtensão do grau de Mestre.

Orientador
Prof. Dr. Miguel Angel Alberto Ferrero

Porto Alegre, Setembro de 1991

Dedico este trabalho à Marília e ao Filipe.

Agradecimentos

Quero agradecer ao meu orientador Prof. Dr. Miguel Angel Alberto Ferrero por sua dedicação e empenho com que sempre me atendeu.

Quero agradecer também à Marília e ao Filipe, por terem tido enorme paciência comigo enquanto me dedicava a este trabalho.

Resumo:

Nesta dissertação estudamos extensões p^n– cíclicas de um anel comutativo R de característica p, com p primo, via vetores de Witt. Além disso, damos uma descrição do $\mathbb{Z}/p^n\mathbb{Z}$–módulo $T_n(\mathbb{Z}/p^n\mathbb{Z}, R)$ das classes de isomorfismos de extensões p^n– cíclicas de R.

Abstract:

In this dissertation we study cyclic p^n–extensions of a commutative ring R of characteristic p, where p is a prime integer, via Witt vectors. Moreover, we give a description of the $\mathbb{Z}/p^n\mathbb{Z}$–module $T_n(\mathbb{Z}/p^n\mathbb{Z}, R)$ of the isomorphism classes of cyclic p^n–extensions of R.

Índice

INTRODUÇÃO

Em [3], M. Auslander e O. Goldman introduziram a definição de extensão de Galois de anéis comutativos. Posteriormente, S. U. Chase, D. K. Harrison e A. Rosenberg [5] desenvolveram uma teoria de Galois para anéis comutativos. Neste trabalho eles obtém várias condições equivalentes que definem o conceito de extensões de Galois de anéis e obtém ainda um "teorema fundamental" (teorema II.3.4), o qual generaliza, para anéis, a clássica correspondência de Galois conhecida para corpos.

Ao mesmo tempo,D. K. Harrison [12] mostrou que conjunto das classes de isomorfismos de extensões de Galois de um anel R, cujo grupo de Galois é um grupo abeliano fixo G, é também um grupo abeliano, chamado grupo de Harrison $T(G,R)$.

A partir destes primeiros trabalhos mencionados acima, muitas pesquisas foram desenvolvidas com o objetivo de estudar as extensões de Galois, suas propriedades, sua estrutura, o grupo de Harrison de um anel. Em particular, mostrou-se que o grupo de Harrison $T(G,R)$ é determinado completamente se é conhecido o grupo de Harrison $T(H,R)$, para cada grupo cíclico finito H. Este fato motiva o estudo das extensões "cíclicas", isto é, extensões de Galois cujo grupo de Galois é cíclico.

O objetivo desta dissertação é o de estudar extensões de Galois de um anel comutativo de característica p com grupo de Galois cíclico de ordem p^n, para $n \geq 1$. O caso $n = 1$, foi considerado por T. Nagahara e A. Nakajima em [15]. Neste trabalho eles determinaram completamente a estrutura das extensões de Galois com grupo de Galois cíclico de ordem p, de um anel comutativo de característica p. Posteriormente, o próprio Nakajima [16] aproveitou estes resultados para obter o grupo de Harrison para este caso.

O caso geral, isto é, extensões de Galois cíclicas com grupo de Galois de ordem p^n de um anel de característica p, foi estudado inicialmente por T. Wyller [21] e C. Greither [9]. Mas só resultados parciais foram obtidos. Ainda, os métodos utilizados por estes autores são métodos cohomológicos, o que torna a leitura do trabalho fundamental de Wyller uma tarefa muito difícil.

Os resultados gerais sobre estrutura e classificação das extensões de Galois cíclicas de ordem p^n de um anel de característica p foram obtidas por M. Ferrero, A. Paques e A. Solecki, em [7] e [8]. Estes trabalhos tem ainda a vantagem de serem desenvolvidos através de métodos mais diretos que os de Wyller e Greither.

Nestes últimos trabalhos citados, mostra-se que toda extensão de Galois cíclica de ordem p^n é um certo quociente de um anel de polinômios a várias indeterminadas, e re-

ciprocamente. Estes resultados são aproveitados para descrever completamente o grupo de Harrison em tais casos. Uma descrição de tal grupo é obtida em [8], utilizando vetores de Witt, generalizando assim a teoria clássica de Artin-Schreier-Witt, para corpos de caraterística p.

No capítulo I apresentamos alguns resultados que são pré-requisitos para a leitura do que segue, tais como módulos, álgebras, produtos tensoriais, etc.

No capítulo II são apresentados os resultados de Chase, Harrison e Rosenberg, fundamentais em todo trabalho sobre teoria de Galois de anéis. O §1 contém o teorema que caracteriza as distintas formas equivalentes da definição de extensões de Galois de um anel comutativo(teorema II.1.6), a qual generaliza a definição para o caso de corpos. No §2 apresentamos alguns exemplos de extensões de Galois. O §3 é dedicado ao teorema fundamental(teorema II.3.4.), o qual mostra que existe correspondência biunívoca entre subgrupos do grupo de Galois e certas subálgebras da extensão. O §4 é destinado a algumas propriedades dos homomorfismos e automorfismos de extensões de Galois. Finalmente, no §5 introduzimos o grupo de Harrison de um anel comutativo R sobre um grupo abeliano G. Neste caso, por simplicidade, optamos por provar o teorema principal desta sessão (teorema II.5.2) somente para grupos cíclicos, pois este é o caso considerado em nosso trabalho.

O capítulo III expõe os resultados fundamentais desta dissertação, segundo [7] e [8], considerando extensões de Galois cíclicas de ordem p^n de um anel de característica p. No §1 estudamos , como introdução, as extensões cíclicas de ordem p, de acordo com [15]. No §2 provamos que toda extensão de Galois de um anel comutativo de característica p com grupo de Galois cíclico de ordem p^n é um certo quociente de um anel de polinômios $R[X_0, \ldots, X_{n-1}]$ e reciprocamente. No §3 obtemos uma representação do grupo de Harrison $T(\mathbb{Z}/p^n\mathbb{Z}, R)$ como um quociente do grupo abeliano $(W_n(R), +)$, onde $W_n(R)$ é o anel de vetores de Witt sobre R. Desta representação segue que $T(\mathbb{Z}/p^n\mathbb{Z}, R)$ é um $\mathbb{Z}/p^n\mathbb{Z}$-módulo livre, determinado basicamente pela estrutura de um grupo quociente de R, isto é, por $(R/\wp R, +)$, onde $\wp R = \{r^p - r : r \in R\}$ (Corolário III.3.3). No §4 alguns exemplos, complementos e algumas aplicações são apresentados.

Em um apêndice, apresentamos os vetores de Witt e suas principais propriedades, fundamentais para a compreensão dos resultados apresentados no capítulo III.

Finalmente, observamos que uma citação do tipo I.3.2 significa o segundo resultado do §3 do capítulo I, enquanto que uma citação do tipo 3.2 significa o segundo resultado do §3 do capítulo que está sendo lido.

CAPÍTULO I - PRELIMINARES

Neste capítulo apresentaremos uma série de resultados da teoria de módulos e álgebras, que serão necessários a compreensão deste trabalho. Alguns resultados não serão seguidos da respectiva prova, para não nos alongarmos em demasia e por serem resultados suficientemente conhecidos. No entanto, o leitor interessado poderá recorrer a bibliografia indicada oportunamente.

Todos os anéis aqui considerados possuem unidade e não serão necessariamente comutativos. Se $R \subseteq S$ é uma extansão de anéis então vamos sempre supor que R e S tem a mesma unidade. Suporemos ainda que todo homomorfismo de anéis envia a unidade na unidade.

§1. MÓDULOS

Seja R um anel. Um R–MÓDULO À ESQUERDA M é um grupo abeliano aditivo, no qual está definido uma aplicação $R \times M \to M$, por $(r, m) \mapsto rm$, para cada $(r, m) \in R \times M$, chamada operação externa do R–módulo, satisfazendo as seguintes condições:

(i) $r(r'm) = (rr')m$;

(ii) $r(m + m') = rm + rm'$;

(iii) $(r + r')m = rm + r'm$;

(iv) $1_R m = m$.

para todo $r, r' \in R$, $m, m' \in M$.

De forma análoga, podemos definir um R–módulo M à direita, se considerarmos a operação externa $M \times R \to M$, dada por $(m, r) \mapsto mr$, para todo $(m, r) \in M \times R$. Porém, escreveremos M é um R-módulo para dizer que M é um R–módulo à esquerda, salvo mensão explícita em contrário.

Vejamos agora alguns exemplos:

(a): Se R é um corpo, então um R– módulo não é nada mais que um espaço vetorial sobre R.

(b): Todo grupo abeliano G é um $\mathbb{Z}$- -módulo, definindo-se a operação externa de maneira natural, como segue: Para cada $n \in \mathbb{Z}$, $g \in G$, temos:

$ng = g + \cdots + g$ (n vezes) se $n > 0$;

$ng = (-g) + \cdots + (-g)$ (n vezes) se $n < 0$;

$0g = 0$.

(c): Qualquer anel R é um módulo sobre si mesmo (à esquerda ou à direita) considerando-se a própria multiplicação do anel como operação externa. Mais ainda, todo ideal de R é um módulo sobre R.

Seja M um R–módulo qualquer. Dizemos que $N \subseteq M$ é um R–SUBMÓDULO de M, se N é um R–módulo com as mesmas operações de M, isto é, N é um subgrupo aditivo de $(M, +)$ e $rn \in N$, para cada $r \in R$ e $n \in N$.

Se N_1 e N_2 são dois submódulos de M, então o conjunto $N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1, n_2 \in N_2\}$ é também um R–submódulo de M, denominado SUBMÓDULO SOMA de N_1 e N_2.

Seja N_1 um R–submódulo de M. Se existir um R–submódulo N_2 de M tal que $N_1 + N_2 = M$ e $N_1 \cap N_2 = \{0\}$, dizemos que M é uma SOMA DIRETA de N_1 e N_2, e representamos por $M = N_1 \oplus N_2$. Neste caso, dizemos também que N_1 e N_2 são R–somandos diretos de M.

Se M e M' são dois R–módulos e $f : M \to M'$ é uma aplicação tal que $f(m_1 + m_2) = f(m_1) + f(m_2)$ e $f(rm) = rf(m)$, para todos $m_1, m_2, m \in M$ e $r \in R$, então dizemos que f é um R–HOMOMORFISMO de M em M'. Se $Imf = M'$, dizemos que f é um R– EPIMORFISMO, se $kerf = \{0\}$, dizemos que f úm R–MONOMORFISMO e, dizemos que f é um R–ISOMORFISMO, se $kerf = \{0\}$ e $Imf = M'$ simultaneamente.

Notaremos por $Hom_R(M, M')$, o conjunto de todos os R–homomorfismos de M em M'. Este é um grupo abeliano aditivo com a soma usual de funções. Se definimos uma operação externa da forma $(rf)(m) = rf(m)$, para cada $r \in R$, $m \in M$ e $f \in Hom_R(M, M')$, então $Hom_R(M, M')$ adquire uma extrutura de R–módulo, como é facil verificar.

Seja N um R–submódulo de M. Então o conjunto M/N é um R–módulo com as operações $\bar{x} + \bar{y} = \overline{x + y}$ e $r\bar{x} = \overline{rx}$, para todos $\bar{x} = x + N$, $\bar{y} = y + N \in M/N$ e $r \in R$, chamado módulo quociente de M por N.

A aplicação $\pi : M \to M/N$ dada por $\pi(x) = x + N$, para todo $x \in M$, é chamada projeção canônica e é um R–epimorfismo cujo núcleo é N. Esta aplicação estabelece uma correspondência biunívoca preservando inclusões, entre os R– submódulos de M que contém N e os R– submódulos de M/N, como é facil verificar.

Com relação à homomorfismos de R–módulos, temos o seguinte teorema, cuja prova

pode ser encontrada em [14].

TEOREMA 1.1: (Teorema de homomorfismos para módulos) Sejam M, M' dois R–módulos, $f : M \to M'$ um R–epimorfismo. Se N é um R–módulo tal que $N \subseteq kerf$, então existe um único R–monomorfismo $\bar{f} : M/N \to M'$, tal que $f = \bar{f} \circ \pi$, onde $\pi : M \to M/N$ é a projeção canônica. Em particular, se $N = kerf$, então $M/N \simeq M'$.

Dados três R–módulos M_1, M_2, M_3 e $f : M_1 \to M_2$, $g : M_2 \to M_3$, dois R–homomorfismos, dizemos que $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ é uma sequência exata em M_2, se $Imf = kerg$. Mais ainda, se $\{M_i\}_{i \in I}$ é uma família de R–módulos, onde I é um conjunto enumerável de índices, então $\ldots M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \ldots$ onde $f_i \in Hom_R(M_i, M_{i+1})$, para todo $i \in I$, é uma sequência exata se é exata em M_i, para cada $i \in I$, ou seja, se $Imf_{i-1} = kerf_i$.

Dada uma sequência exata $0 \longrightarrow N_1 \xrightarrow{f} M \xrightarrow{g} N_2 \longrightarrow 0$ de R–módulos e R–homomorfismos, dizemos que ela CINDE, se o R–submódulo $Imf = kerg$ é um R–somando direto de M. Temos então o seguinte resultado, cuja prova pode ser encontrada em [14] ou [19].

TEOREMA 1.2: Seja $0 \longrightarrow N_1 \xrightarrow{f} M \xrightarrow{g} N_2 \longrightarrow 0$ uma sequência exata de R–módulos e R–homomorfismos. Então as seguintes condições são equivalentes:

(i) A sequência exata $0 \longrightarrow N_1 \xrightarrow{f} M \xrightarrow{g} N_2 \longrightarrow 0$ cinde;

(ii) Existe um R–homomorfismo $\psi : M \to N_1$, tal que $\psi \circ f = id_{N_1}$;

(iii) Existe um R–homomorfismo $\phi : N_2 \to M$, tal que $g \circ \phi = id_{N_2}$;

(iv) Existem R–homomorfismos $\psi : M \to N_1$ e $\phi : N_2 \to M$, tais que $\psi \circ f = id_{N_1}$, $g \circ \phi = id_{N_2}$ e $f \circ \psi + \phi \circ g = id_M$. Nestas condições $M \simeq N_1 \oplus N_2$ como R–módulos.

§2. MÓDULOS FINITAMENTE GERADOS, MÓDULOS LIVRES E MÓDULOS PROJETIVOS

Seja M um R–módulo e $S \subseteq M$ um conjunto qualquer. É fácil ver que a intersecção de todos os R–submódulos de M que contém S é o R– submódulo de M, notado por $[S]$, cujos elementos são todas as somas finitas do tipo $\sum_{i=1}^{n} r_i s_i$, onde $n \geq 1$, $r_i \in R$ e $s_i \in S$, para todo $1 \leq i \leq n$. Este submódulo é chamado SUBMÓDULO GERADO POR S. Se $[S] = M$, dizemos que S gera M ou que S é um sistema de geradores de

M. Ainda, dizemos que M é um R- MÓDULO FINITAMENTE GERADO, se existir um conjunto finito $S \subseteq M$ tal que $[S] = M$. Nesta caso, temos $M = Rm_1 + \cdots + Rm_n$, para alguns $m_1, \ldots, m_n \in M$.

Um conjunto S é uma base de M, se S é linearmente independente e $[S] = M$. Se M é um R–módulo que possui uma base, então dizemos que M é um R–MÓDULO LIVRE. Neste caso, cada elemento $m \in M$ pode ser escrito de uma única maneira como uma soma finita $m = \sum_{s \in S} r_s s$.

Todo espaço vetorial sobre um corpo K é um K– módulo livre. Todo anel com unidade R é um R– módulo livre cuja base é $\{1_R\}$. Mais ainda, dado um anel R, consideremos a soma direta $R^{(I)} = \bigoplus_{i \in I} R_i$, com $R_i \simeq R$, para todo $i \in I$, e indiquemos por $e_j = (\delta_{i,j})$, onde $\delta_{j,j} = 1$ e $\delta_{i,j} = 0$, se $i \neq j$. Então $R^{(I)}$ é um R– módulo livre com base $\{e_j\}_{j \in I}$. Esta base é chamada base canônica do R–módulo $R^{(I)}$. Ainda, se $I = \{1, \ldots, n\}$, então notamos $R^{(n)}$ em lugar de $R^{(I)}$.

Seja G um grupo abeliano finito não nulo. Então G é um $\mathbb{Z}$–módulo que não é livre. De fato, pelo teorema de Lagrange, se $n \geq 0$ é tal que $|\, G \,| = n$, então $ng = 0$, para todo $g \in G$ e, portanto, não existe nenhum subconjunto não vazio de G linearmente independente. Assim, G não possui uma base como $\mathbb{Z}$–módulo.

Temos as seguintes propriedades para módulos livres:

PROPOSIÇÃO 2.1:

(i) Se L é um R–módulo livre com base S e $f : S \longrightarrow N$ é qualquer aplicação de S em um R–módulo N, então existe um único R–homomorfismo $\bar{f} : L \longrightarrow N$, o qual extende f.

(ii) Se L é um R–módulo livre com base $\{x_i\}_{i \in I}$, então $L \simeq R^{(I)}$.

(iii) Todo R–módulo M é isomorfo a um quociente de um R–módulo livre.

(iv) Sejam L um R–módulo livre, M, N dois R–módulos, $f : M \longrightarrow N$ um R–epimorfismo e $g : L \longrightarrow N$ um R–homomorfismo. Então existe um R–homomorfismo $\bar{h} : L \longrightarrow M$, tal que $f \circ \bar{h} = g$.

Prova:

(i) Por hipótese, para cada $m \in M$, $m = \sum_{s \in S} r_s s$ com $r_s \in R$, para todo $s \in S$. Definindo-se $\bar{f} : L \longrightarrow N$, por $\bar{f}(m) = \sum_{s \in S} r_s f(s)$, pode-se verificar facilmente que $\bar{f}$ é o único R–homomorfismo nas condições requeridas.

(ii) Para provar (ii), basta definir uma aplicação $f : \{x_i\}_{i \in I} \longrightarrow R^{(I)}$, por $f(x_i) = e_i$,

para todo $i \in I$, onde $\{e_i\}_{i\in I}$ é a base canônica de $R^{(I)}$, e considerar sua única extensão $\bar{f} : L \longrightarrow R^{(I)}$, obtida de (i). Pode-se ver facilmente que $\bar{f}$ é um isomorfismo.

(iii) Seja M um R–módulo e $\{m_i\}_{i\in I}$ um conjunto de geradores de M (o qual sempre existe, pois o próprio M o é). Definindo então $f : R^{(I)} \longrightarrow M$ por $f(e_i) = m_i$, para todo $i \in I$ e extendendo a um R–homomorfismo $\bar{f} : R^{(I)} \longrightarrow M$, resulta facilmente que $\bar{f}$ é um epimorfismo e segue de 1.1 que $M \simeq R^{(I)}/ker\bar{f}$

(iv) Seja S uma base de L como R– módulo. Sendo $f : M \longrightarrow N$ um epimorfismo, então para cada $s \in S$, existe um elemento $m_s \in M$, tal que $g(s) = f(m_s)$. Definimos $h : S \longrightarrow M$, por $h(s) = m_s$, para cada $s \in S$. Por (i), existe um único R–homomorfimo $\bar{h} : L \longrightarrow M$, o qual extende h. Daí, como $l = \sum_{s\in S} r_s s$, para cada $l \in L$, onde $r_s \in R$, para todo $s \in S$, temos $(f \circ \bar{h})(l) = f(\bar{h}(\sum_{s\in S} r_s s)) = f(\sum_{s\in S} r_s h(s)) = \sum_{s\in S} r_s f(m_s) = \sum_{s\in S} r_s g(s) = g(\sum_{s\in S} r_s s) = g(l)$, isto é, $f \circ \bar{h} = g$. Isto finaliza a prova de (iv).

Em outras palavras, (iv) mostra que dado o diagrama de flexas contínuas abaixo, existe um R– homomorfismo $\bar{h}$ tal que o diagrama completo se torna comutativo.

$$\begin{array}{ccccc} & & L & & \\ & \overset{\bar{h}}{\swarrow} & \downarrow g & & \\ M & \xrightarrow{f} & N & \longrightarrow & 0 \end{array}$$

Apropriedade (iv) é válida não somente para módulos livres. De fato, ela dá origem à definição dos módulos projetivos, a qual faremos agora.

DEFINIÇÃO 2.2: Seja R um anel. Dizemos que um R–módulo P é PROJETIVO se, para quaisquer dois R–módulos M, N, um epimorfismo $f : M \longrightarrow N$ e um homomorfismo $g : P \longrightarrow N$, sempre existe um homomorfismo $\bar{g} : P \longrightarrow M$ tal que $f \circ \bar{g} = g$.

Claramente todo R–módulo livre é projetivo, mas a recíproca não é verdadeira. Mostraremos um exemplo neste sentido, após o próximo resultado o qual dá uma caracterização dos módulos projetivos.

PROPOSIÇÃO 2.3: Seja P um R– módulo. As seguintes afirmações são equivalentes:

(i) P é projetivo;

(ii) P é isomorfo a um R– somando direto de algum R–módulo livre;

(iii) Toda seqüência exata de R– módulos e R–homomorfismos

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

cinde;

(iv) Existe um conjunto de elementos $x_i \in P$ e de R–homomorfismos $f_i : P \longrightarrow R$, onde $i \in I$ (I um conjunto de índices) tais que:

(a) $\forall x \in P$, $f_i(x) = 0$ exceto para um número finito de índices $i \in I$;

(b) $\sum_{i \in I} f_i(x)x_i = x$, $\forall x \in P$.

Além disso, o conjunto de índices I pode ser tomado finito se e somente se P é um R–módulo finitamente gerado.

Prova: A equivalência (i) $\Leftrightarrow$ (iii) é imediata. Mostemos agora a equivalência (i) $\Leftrightarrow$ (ii).

Seja P um R–módulo projetivo. Então existe um R–módulo livre L e um epimorfismo $\varphi : L \longrightarrow P$ ($P \simeq L/ker\varphi$). Consideremos então o seguinte diagrama:

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow id & & \\ L & \xrightarrow{\varphi} & P & \longrightarrow & 0 \end{array}$$

Então existe um homomorfismo $h : P \longrightarrow L$ tal que $h \circ \varphi = id_P$. Portanto, P é um R– somando direto de L.

Reciprocamente, seja L um R–módulo livre tal que $L = P \oplus Q$. Seja $f : M \longrightarrow N$ um R–epimorfismo de módulos e $g : P \longrightarrow N$ um R–homomorfismo. Definimos $g' : L \longrightarrow N$ por $g'(x) = x$, se $x \in P$ e $g'(x) = 0$, se $x \in Q$. Então existe um homomorfismo $h : L \longrightarrow M$ tal que $f \circ h = g'$. Assim, tomando $\bar{g} = h \circ j$ onde j é a inclusão canônica $P \hookrightarrow L$. Temos então $\bar{g} \circ f = g$ e portanto P é projetivo.

Para finalizar a prova, mostraremos (i) $\Leftrightarrow$ (iv). Seja P um R–módulo projetivo. Existem um conjunto de índices I e R–homomorfismos $\varphi : P \longrightarrow R^{(I)}$ e $\pi : R^{(I)} \longrightarrow P$ tais que $\pi \circ \varphi = id_P$. Pensando $R^{(I)}$ como um conjunto de funções de I em R, seja $\pi_i : R^{(I)} \longrightarrow R$ dada por $\pi_i(f) = f(i)$ para todo $f \in R^{(I)}$. Então para todo $f \in R^{(I)}$, temos $\sum_{i \in I} \pi_i(f)e_i = f$, uma vez que $[\sum_{i \in I} \pi_i(f)e_i](j) = \pi_j(f) = f(j)$. (lembramos que $e_i \in R^{(I)}$ é tal que $e_i(j) = \delta_{i,j}$). Assim, $\{\pi, e_i\}$ satisfazem as condições (a) e (b) de (iv), para $R^{(I)}$. Agora seja $x_i = \pi(e_i)$ e $f_i = \pi_i \circ \varphi$. Claramente, $f_i(x) = 0$ para todos $x \in P$, $i \in I$ e $\sum_{i \in I} f_i(x)x_i = \sum_{i \in I} \pi_i(\varphi(x))\pi(e_i) = \pi(\sum_{i \in I} \pi_i(\varphi(x))e_i) = \pi(\varphi(x)) = x$, para todo $x \in P$. Assim, $\{f_i, x_i\}$ satisfazem (a) e (b) de (iv), para o R–módulo P.

Reciprocamente, se $\{f_i, x_i\}_{i\in I}$ são tais que vale (a) e (b) de (iv), definimos $\varphi : P \longrightarrow R^{(I)}$ por $\varphi(x)(i) = f_i(x)$ e $\pi : R^{(I)} \longrightarrow P$ por $\pi(f) = \sum_{i\in I} f(i)x_i$. É fácil verificar que φ e π são homomorfismos de R–módulos e $\pi(\varphi(x)) = \sum_{i\in I} f_i(x)x_i = x$, para todo $x \in P$. Assim, $\pi \circ \varphi = id_P$, de onde segue que P é isomorfo a um somando direto de $R^{(I)}$ e portanto projetivo.

COROLÁRIO 2.4: Seja P um R–módulo e seja N um R–somando direto de P.

(i) Se P é projetivo, então N também é projetivo.

(ii) Se P é finitamente gerado, então N também é finitamente gerado.

Citamos agora um exemplo de um módulo projetivo que não é livre. Seja K um corpo e $A = \mathcal{M}_2(K)$ o anel das matrizes quadradas sobre K. É fácil ver que $I_1 = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in K\right\}$, $I_2 = \left\{\begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} : c, d \in K\right\}$ são ideais à esquerda de A. Assim eles possuem uma estrutura de A–módulo à esquerda. Ainda, $A = I_1 \oplus I_2$ como A–módulos. Agora, o anel A considerado como A–módulo é livre. Segue então da proposição anterior que I_1 e I_2 são projetivos. Mas $\begin{pmatrix} b & -a \\ b & -a \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Logo, I_1 não possui uma base como A–módulo e portanto não é livre. Analogamente, I_2 não é livre.

Consideremos agora R e S anéis não necessariamente comutativos e $f : R \longrightarrow S$ um homomorfismo de anéis. Então S pode ser visto como um R–módulo com a operação $rs = f(r)s$, para cada $r \in R$, $s \in S$. Isto induz, naturalmente, uma estrutura de R–módulo sobre qualquer S–módulo. Isto acontece, por exemplo, quando R é um subanel de S e f é a identidade.

Feitas estas considerações, podemos falar em transitividade de módulo projetivos e módulos finitamente gerados, e assim, obter o seguinte resultado cuja prova pode ser encontrada em [6], [14] ou [4].

PROPOSIÇÃO 2.5: Sejam R e S anéis, $f : R \longrightarrow S$ um homomorfismo de anéis e P um S–módulo. Então:

(i) Se P é projetivo sobre S e S é projetivo sobre R, então P é projetivo sobre R.

(ii) Se P é finitamente gerado sobre S e S é finitamente gerado sobre R, então P é finitamente gerado sobre R.

(iii) Se P é finitamente gerado como R–módulo então P é finitamente gerado

como S–módulo.

§3. MÓDULOS GERADORES

Para qualquer R–módulo M, consideremos o subconjunto $T_R(M) = \{\sum_{i\in I} f_i(m_i) : f_i \in Hom_R(M,R),\ m_i \in M,\ I$ conjunto de índices $\}$. Como $Hom_R(M,R)$ é um R–módulo à direita, com a operação externa de finida por $(fr)(m) = f(m)r$, para cada $r \in R$, $f \in Hom_R(M,R)$ e $m \in M$, segue que $r(\sum_{i\in I} f_i(m_i)) = \sum_{i\in I} f_i(rm_i) \in T_R(M)$ e $(\sum_{i\in I} f_i(m_i))r = \sum_{i\in I}(f_i r)(m_i) \in T_R(M)$. Assim, $T_R(M)$ é um ideal bilateral de R, chamado IDEAL TRAÇO de M.

O R–módulo M é dito um R–MÓDULO GERADOR, ou simplesmente um R–GERADOR, se $T_R(M) = R$. Portanto, M é um R–gerador se e somente se existirem $f_1,\ldots,f_n \in Hom_R(M,R)$ e $m_1,\ldots,m_n \in M$ tais que $\sum_{i=1}^{n} f_i(m_i) = 1$.

Aqui vale também a propriedade da transitividade de módulos geradores, como mostra a seguinte proposição:

PROPOSIÇÃO 3.1: Sejam R e S anéis e $\phi : R \longrightarrow S$ um homomorfismo de anéis tal que S é um R–gerador quando considerado como um R–módulo. Seja ainda M um S–módulo. Se M é um S–gerador, então M é também um R– gerador.

Prova: Da hipótese segue que existem $f_1,\ldots,f_n \in Hom_S(M,S)$, $m_1,\ldots,m_n \in M$, $g_1,\ldots,g_m \in Hom_R(S,R)$ e $s_1,\ldots,s_m \in S$ tais que $\sum_{i=1}^{n} f_i(m_i) = 1 = \sum_{j=1}^{m} g_j(s_j)$. Então, $g_j f_i \in Hom_R(M,R)$, $s_j m_i \in M$ e $\sum_{j=1}^{m}\sum_{i=1}^{n} g_j f_i(s_j m_i) = \sum_{j=1}^{m}\sum_{i=1}^{n} g_j(s_j f_i(m_i)) = \sum_{j=1}^{m} g_j(s_j \sum_{i=1}^{n} f_i(m_i)) = 1$. Assim, M é R– gerador, como queríamos mostrar.

Um R–módulo M é dito um R–PROGERADOR se M é finitamente gerado,projetivo e gerador sobre R. Observemos que da transitividade de módulos finitamente gerados, projetivos e geradores, decorre a seguinte

PROPOSIÇÃO 3.2: Sejam R, S anéis e $\phi : R \longrightarrow S$ um homomorfismo de anéis tais que S é um R–progerador quando considerado como R– módulo. Então qualquer S–módulo M que é progerador sobre S é também R–progerador.

Lembremos neste momento que se M é um R-módulo, então o anulador de M em R é o ideal de R definido por $An_R(M) = \{r \in R : rm = 0,\ \forall m \in M\}$. Se $An_R(M) = \{0\}$ então dizemos que M é um R-MÓDULO FIEL.

LEMA 3.3: (Lema de Nakayama generalizado)

Sejam R um anel comutativo e M um R-módulo finitamente gerado. Então um ideal I de R verifica a propriedade $IM = M$ se e somente se $I + An_R(M) = R$.

Prova: Suponhamos $M = Rm_1 + \cdots + Rm_n$, onde $m_1, \ldots, m_n \in M$, e que I seja um ideal de R satisfazendo $IM = M$. Como $An_R(M)$ é um ideal de R, para obtermos $I + An_R(M) = R$, basta mostrarmos que $1 \in I + An_R(M)$.

Consideremos os submódulos $M_i = Rm_i + \cdots + Rm_n$, para cada $1 \leq i \leq n$ e tomamos $M_{n+1} = \{0\}$. É suficiente mostrarmos que, para todo $i \in \{1, 2, \ldots, n+1\}$, existe $a_i \in I$ tal que $(1 - a_i)M \subseteq M_i$. De fato, neste caso podemos concluir que existe $a_{n+1} \in I$, com $(1 - a_{n+1})M \subseteq M_{n+1} = 0$, ou seja, $1 - a_{n+1} \in An_R(M)$, ou ainda, $1 \in I + An_R(M)$. Faremos isto por indução em i.

Tomando $a_1 = 0$, claramente $(1 - a_1)M = M = M_1$. Seja agora $k \in \{1, 2, \ldots, n\}$ e suponhamos que exista $a_k \in I$ tal que $(1 - a_k)M \subseteq M_k$. Então, $(1 - a_k)M = (1 - a_k)IM = I(1 - a_k)M \subseteq IM_k = Im_k + \cdots + Im_n$. Assim existem elementos $a_{kj} \in I$, para cada $j = k, \ldots, n$, tais que $(1 - a_k)m_k = \sum_{j=k}^{n} a_{kj}m_j = a_{kk}m_k + \sum_{j=k+1}^{n} a_{kj}m_j$. Portanto, $(1 - a_k - a_{kk})m_k = \sum_{j=k+1}^{n} a_{kj}m_j \in M_{k+1}$, de onde segue que $(1 - a_k)(1 - a_k - a_{kk})M \subseteq (1 - a_k - a_{kk})M_k \subseteq M_{k+1}$. Tomando então $a_{k+1} = 2a_k + a_{kk} - a_k^2 - a_k a_{kk}$, obtemos $a_{k+1} \in I$ e $(1 - a_{k+1}) = (1 - a_k)(1 - a_k - a_{kk})$, e conseqüentemente $(1 - a_{k+1})M \subseteq M_{k+1}$. Isto completa a prova da indução e a primeira parte do lema.

Reciprocamente, suponhamos que $I + An_R(M) = R$, e mostremos que $IM = M$. Claramente $IM \subseteq M$. Seja $a \in I$ e $r \in An_R(M)$, tais que $1 = a + r$. Para cada $m \in M$, $m = 1m = (a + r)m = am + rm = am \in IM$, já que $r \in An_R(M)$. Logo $IM = M$ o que completa a prova do lema.

COROLÁRIO 3.4: Seja R um anel comutativo e M um R-módulo finitamente gerado. Se $\mathcal{M}M = M$, para todo ideal maximal $\mathcal{M}$ de R, então $M = 0$.

Prova: Suponhamos que M é tal que $\mathcal{M}M = M$, para todo ideal maximal $\mathcal{M}$ de R. Mostraremos que, nestas condições, $An_R(M) = R$. Assim obtemos $M = 1M = 0$,

pois $1 \in An_R(M)$

Suponhamos, por absurdo, que $An_R(M) \neq R$. Então existe algum ideal maximal $\mathcal{M}$ de R com $An_R(M) \subseteq \mathcal{M}$. Portanto, $An_R(M) + \mathcal{M} \neq R$, o que é uma contradição com o lema 3.3.

É frequentemente difícil distinguir se um módulo finitamente gerado e projetivo é um gerador. Porém, no caso de anéis comutativos, temos um critério fácil, com auxílio do lema anterior.

PROPOSIÇÃO 3.5: Seja R um anel comutativo e M um R–módulo finitamente gerado e projetivo. Então $T_R(M) \oplus An_R(M) = R$.

Prova: Sejam $f_1, \ldots, f_n \in Hom_R(M, R)$ e $m_1, \ldots, m_n \in M$, coordenadas projetivas de M sobre R. Então $m = \sum_{i=1}^{n} f_i(m)m_i$, para cada $m \in M$, e $f_i(m)$ está em $T_R(M)$. Assim $T_R(M)M = M$ e segue do lema de Nakayama que $T_R(M) + An_R(M) = R$. Mas $T_R(M)An_R(M) = 0$, já que, para qualquer $\alpha \in An_R(M)$, $f \in Hom_R(M, R)$ e $m \in M$, temos $\alpha f(m) = f(\alpha m) = 0$. Segue daí que $T_R(M) \cap An_R(M) = 0$. De fato, seja $1 = \alpha + \beta$ com $\alpha \in T_R(M)$ e $\beta \in An_R(M)$. Se $x \in T_R(M) \cap An_R(M)$, então $x = 1x = \alpha x + \beta x = 0$. Consequentemente $T_R \oplus An_R(M) = R$.

COROLÁRIO 3.6: Seja R um anel comutativo. Um R–módulo M é R–progerador se e somente se M é finitamente gerado, projetivo e fiel.

§4. PRODUTO TENSORIAL DE MÓDULOS

Sejam R e S dois anéis. Suponhamos que M seja um R–módulo e um S–módulo simultaneamente. Se a multiplicação de elementos de M por elementos de R comuta com a multiplicação por elementos de S, dizemos que M é um (R, S)–BIMÓDULO. Os bimódulos podem ser de vários tipos, dependendo de qual o lado que os anéis operam. Se, por exemplo, R opera pela esquerda e S pela direita, indicaremos este fato escrevendo ${}_RM_S$. Neste caso, $(rm)s = r(ms)$, para todos $r \in R$, $m \in M$ e $s \in S$.

Durante este parágrafo, com a finalidade de simplificar notações, escreveremos ${}_RM$, para dizer que M é um R–módulo à esquerda e ecreveremos M_R para dizer que M é um R–módulo à direita.

Começaremos com a seguinte

DEFINIÇÃO 4.1: Sejam M_R e ${}_RN$ R- -módulos. Dado um grupo abeliano G, dizemos que uma aplicação $\phi : M \times N \longrightarrow G$ é R–bilinear, se:

(i) $\phi(m_1 + m_2, n) = \phi(m_1, n) + \phi(m_2, n)$;

(ii) $\phi(m, n_1 + n_2) = \phi(m, n_1) + \phi(m, n_2)$;

(iii) $\phi(mr, n) = \phi(m, rn)$.

para todos $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ e $r \in R$.

Com as mesmas notações acima, um par (T, τ) constituido de um grupo abeliano T e uma aplicação R–bilinear $\tau : M \times N \longrightarrow T$ é chamado PRODUTO TENSORIAL de M e N sobre R, se para cada grupo abeliano G e para cada aplicação R– bilinear $\phi : M \times N \longrightarrow G$ existe um único homomorfismo de grupos $f : T \longrightarrow G$ tal que o seguinte diagrama comuta

$$\begin{array}{ccc} & M \times N & \\ {\scriptstyle\tau}\swarrow & & \searrow{\scriptstyle\phi} \\ T & \xrightarrow{f} & G \end{array}$$

Se (T, τ) é um produto tensorial de M e N, então claramente $f \circ \tau$ é R–bilinear, para cada homomorfismo $f : T \longrightarrow G$. Assim, (T, τ) é um produto tensorial de M e N sobre R se e somente se, para cada grupo abeliano G, a correspondência $f \longmapsto f \circ \tau$ define uma correspondência biunívoca entre $Hom_{\mathbb{Z}}(T, G)$ e o conjunto de todas as aplicações R–bilineares $\phi : M \times N \longrightarrow G$.

A seguir mostraremos que um tal produto tensorial existe e é único, a menos de isomorfismos. A unicidade é particularmente fácil

PROPOSIÇÃO 4.2: Se (T, τ) e (T', τ') são dois produtos tensoriais de M e N sobre R, então existe um único homomorfismo de grupos $f : T \longrightarrow T'$ tal que $\tau' = f \circ \tau$.

Prova: A hipótese implica a existência de homomorfismos f e g tais que os seguintes diagramas são comutativos

$$\begin{array}{ccc} & M \times N & \\ {\scriptstyle\tau}\swarrow & & \searrow{\scriptstyle\tau'} \\ T & \xrightarrow{f} & T' \end{array} \qquad \text{e} \qquad \begin{array}{ccc} & M \times N & \\ {\scriptstyle\tau'}\swarrow & & \searrow{\scriptstyle\tau} \\ T' & \xrightarrow{g} & T \end{array}$$

Então a comutatividade dos diagramas

$$\begin{array}{ccc} & M \times N & \\ {\scriptstyle\tau}\swarrow & & \searrow{\scriptstyle\tau} \\ T & \xrightarrow{g \circ f} & T \end{array} \qquad \text{e} \qquad \begin{array}{ccc} & M \times N & \\ {\scriptstyle\tau}\swarrow & & \searrow{\scriptstyle\tau} \\ T & \xrightarrow{id_T} & T \end{array}$$

juntamente com a unicidade da aplicação na definição, faz com que tenhamos $g \circ f = id_T$. Analogamente, mostra-se que $f \circ g = id_T$. Portanto, f é um isomorfismo como queríamos mostrar.

Consideremos agora um grupo abeliano G livremente gerado por $M \times N$, como $\mathbb{Z}$–módulo. Então G possui uma base $(x_a)_{a \in M \times N}$. Por simplicidade de notação escreveremos (m,n) em lugar de $x_{(m,n)}$. Assim, temos $G = \bigoplus_{M \times N} \mathbb{Z}(m,n)$. Seja agora H o subgrupo de G gerado por todos os elementos da forma

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$

$$(mr, n) - (m, rn)$$

para todos $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $r \in R$. Tomamos $T = G/H$ e definimos $\tau : M \times N \longrightarrow T$, por $\tau(m,n) = (m,n) + H$.

PROPOSIÇÃO 4.3: Com as mesmas notações acima, (T, τ) é um produto tensorial de M e N sobre R.

Prova: Seja $\phi : M \times N \longrightarrow F$ uma aplicação R–bilinear, onde F é um grupo abeliano qualquer. Sendo $G = \bigoplus_{M \times N} \mathbb{Z}(m,n)$, existe um homomorfismo de grupos $f' : G \longrightarrow F$ tal que o diagrama comuta

$$\begin{array}{ccc} & M \times N & \\ {\scriptstyle \tau}\swarrow & & \searrow{\scriptstyle \phi} \\ G & \xrightarrow{f'} & F \end{array}$$

Do fato que ϕ é R–bilinear, segue que H é um subgrupo de $ker f'$. Logo existe um homomorfismo de grupos $f : T \longrightarrow F$, tal que

$$\begin{array}{ccc} & M \times N & \\ {\scriptstyle id}\swarrow & & \searrow{\scriptstyle \phi} \\ G & \xrightarrow{f} & F \end{array}$$

é um diagrama comutativo. Finalmente, como $\tau(M \times N)$ gera T, segue que f é unicamente determinado por este diagrama. Assim está demonstrada a proposição.

O produto tensorial (T, τ) construído acima será denotado por $M \otimes_R N$ e, para cada $(m,n) \in M \times N$, escreveremos $\tau(m,n) = m \otimes n$.

Considerando-se os resultados obtidos até agora, temos que $M \otimes_R N$ é o único (a menos de isomorfismos) grupo abeliano que contém o gerado por $\{m \otimes n : m \in M, n \in N\}$, satisfazendo a seguinte

PROPOSIÇÃO 4.4: (Propriedade Universal do Produto Tensorial).

Para cada aplicação R–bilinear $\phi : M \times N \longrightarrow G$, existe um único homomorfismo de grupos abelianos $f : M \otimes_R N \longrightarrow G$ tal que $f(m \times n) = \phi(m,n)$, para cada $m \in M$, $n \in N$.

COROLÁRIO 4.5: Suponhamos $f : M \longrightarrow M'$ e $g : N \longrightarrow N'$ homomorfismos de R–módulos à direita e à esquerda, respectivamente. Então existe um único homomorfismo de grupos $f \otimes g : M \otimes_R N \longrightarrow M' \otimes_R N'$ tal que $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$, para todos $m \otimes n \in M \otimes_R N$.

Prova: Seja $\varphi : M \times N \longrightarrow M' \otimes_R N'$ definida por $\varphi(m,n) = f(m) \otimes g(n)$. Assim, φ é R–bilinear, como é fácil ver. Pela proposição anterior, existe um único homomorfismo de grupos $\bar{\varphi} : M \otimes_R N \longrightarrow M' \otimes N'$ tal que $\bar{\varphi}(m \otimes n) = \varphi(m,n) = f(m) \otimes g(n)$. Basta então tomar $f \otimes g = \bar{\varphi}$.

Em geral, o produto tensorial $M \otimes_R N$ não é um R–módulo. Porém, estruturas de bimódulos sobre M e N induzem uma estrutura de R–módulo em $M \otimes_R N$. Mais precisamente, temos a seguinte

PROPOSIÇÃO 4.6: Sejam R e S anéis e ${}_RM_S$, ${}_SN$ módulos. Então $M \otimes_R N$ é um R–módulo com a multiplicação externa dada por $r(m \otimes n) = rm \otimes n$. Ainda, se $f : M \longrightarrow M'$ e $g : N \longrightarrow N'$ são homomorfismos de (R,S)–bimódulos e S–módulos, respectivamente, então $f \otimes g$ é um homomorfismo de R–módulos.

Prova: Primeiro mostraremos que uma tal multiplicação externa está bem definida. Seja $\rho_r : M \longrightarrow M$ dada por $\rho_r(m) = rm$, para cada $m \in M$. Assim, ρ_r é um homomorfismo de R– módulos, para cada $r \in R$. Agora, observemos que $rm \otimes n = (\rho_r \otimes id_N)(m \otimes n)$. A boa definição segue.

É fácil ver que esta operação tem as propriedades desejadas.

Para ver que $f \otimes g$ é um homomorfismo de R– módulos, observemos que $(f \otimes g)(r(m \otimes n)) = (f \otimes g)(rm \otimes n) = f(rm) \otimes g(n) = rf(m) \otimes g(n) = r(f \otimes g)(m \otimes n)$. Isto completa a prova da proposição.

Analogamente, se $N =_S N_S$, então $M \otimes_S N$ pode ser visto como um S–módulo à

direita via $(m \otimes n)s = m \otimes ns$.

Está claro portanto, que se R é um anel comutativo, então o produto tensorial $M \otimes_R N$ é um R– módulo à esquerda e à direita. De fato, neste caso cada R–módulo é um módulo bilateral.

Listamos agora algumas propriedades dos produtos tensoriais. Uma prova para tais propriedades pode ser encontrada em [1] ou [6]

1: O produto tensorial é associativo no seguinte sentido: Sejam R e S dois anéis. Consideremos os módulos L_R, ${}_RM_S$ e ${}_SN$. Então $(L \otimes_R M) \otimes_S N$ e $L \otimes_R (M \otimes_S N)$ são isomorfos, via o isomorfismo $(l \otimes m) \otimes n \mapsto l \otimes (m \otimes n)$, para cada $(l \otimes m) \otimes n \in (L \otimes_R M) \otimes_S N$.

2. Se R é um anel comutativo e M, N são R–módulos, então $M \otimes_R N \simeq N \otimes_R M$, via o isomorfismo $m \otimes n \mapsto n \otimes m$, para cada $m \otimes n \in M \otimes_R N$.

3. O produto tensorial se distribui em relação à soma direta: Sejam $\{M_i\}_{i \in I}$, $\{N_j\}_{j \in J}$ famílias de R–módulos à esquerda e à direita, respectivamente, onde I e J são conjuntos de índices. Então temos

$$(\bigoplus_{i \in I} M_i) \bigotimes_R (\bigoplus_{j \in J} N_j) \simeq \bigoplus_{\substack{i \in I \\ j \in J}} M_i \bigotimes_R N_j$$

via o isomorfismo $(\sum_{i \in I} m_i) \otimes (\sum_{j \in J} n_j) \mapsto \sum_{\substack{i \in I \\ j \in J}} m_i \otimes n_j$.

4: Dado um anel qualquer R e um R–módulo ${}_RM$, então $M \simeq R \otimes_R M$, como R– módulos, via o isomorfismo $r \otimes m \mapsto rm$, para cada $r \otimes m \in R \otimes_R M$, tendo como aplicação inversa $m \mapsto 1 \otimes m$, para cada $m \in M$.

Consideremos agora ${}_RN$ um R–módulo livre com base $\{n_i : i \in I\}$. Consequentemente, $N = \bigoplus_{i \in I} Rn_i$. Nesta situação, temos a seguinte

PROPOSIÇÃO 4.7: Todo elemento de $M \otimes_R N$ possui uma única representação como uma soma finita do tipo $\sum_{i \in I} m_i \otimes n_i$, onde $m_i \in M$ e $m_i = 0$ exceto para um número finito de índices $i \in I$.

Prova: Sejam $m \in M$, $n \in N$. Então $n = \sum_{i \in I} r_i n_i$, onde $r_i \in R$ e $r_i = 0$ exceto para um número finito de índices de $i \in I$. Portanto, $m \otimes n = m \otimes \sum_{i \in I} r_i n_i =$

$\sum_{i\in I} m \otimes r_i n_i = \sum_{i\in I} mr_i \otimes n_i = \sum_{i\in I} m_i \otimes n_i$, onde $m_i = mr_i \in M$.

Para ver a unicidade de tal escrita, consideremos $\sum_{i\in I} m_i \otimes n_i \in M \bigotimes_R N$ tal que $\sum_{i\in I} m_i \otimes n_i = 0$. Como $N = \bigoplus_{i\in I} Rn_i$, temos $M \otimes_R N = M \otimes_R (\bigoplus_{i\in I} Rn_i) \simeq \bigoplus_{i\in I} M \bigotimes_R Rn_i$. Seja ϕ este isomorfismo. Então $\phi(\sum_{i\in I} m_i \otimes n_i) = 0$ em $\bigoplus_{i\in I} M \bigotimes_R Rn_i$, e portanto, para cada $i \in I$, $m_i \otimes n_i = 0$, visto como elemento de $\bigoplus_{i\in I} M \bigotimes_R Rn_i$.

Fixemos agora, $k \in I$. Como $R \simeq Rn_k$, segue que $M \simeq M \otimes_R R \simeq M \otimes_R Rn_k$ e assim, a imagem de m_k por este isomorfismo é $m_k \otimes n_k$, o qual é zero. Portanto, $m_k = 0$. Isto completa a prova.

PROPOSIÇÃO 4.8: Sejam R um anel comutativo e M um R–módulo livre. Então toda base de M como R–módulo tem a mesma cardinalidade.

Prova: Seja M um R–módulo livre e seja $\mathcal{M}$ um ideal maximal de R. Então, $R/\mathcal{M}$ é corpo. Consideremos $\pi : R \longrightarrow R/\mathcal{M}$ a projeção canônica. Assim, $R/\mathcal{M}$ é um R– módulo e podemos considerar o produto tensorial $R/\mathcal{M} \otimes_R M$, o qual é também um $R/\mathcal{M}$–espaço vetorial, via a operação externa $\bar{x}(\bar{r} \otimes m) = \overline{xr} \otimes m$, para todos $\bar{x} \in R/\mathcal{M}$, $\bar{r} \otimes m \in R/\mathcal{M} \otimes_R M$. Da proposição anterior segue que se $\{m_i\}_{i\in I}$ é uma base de M como R–módulo, então $\{\bar{1} \otimes m_i\}_{i\in I}$ é uma base de $R/\mathcal{M} \otimes_R M$ como $R/\mathcal{M}$–espaço vetorial. A recíproca é clara. Logo existe uma correspondência biunívoca entre os elementos de uma base de M e os elementos de uma base de $R/\mathcal{M} \otimes_R M$ como $R/\mathcal{M}$–espaço vetorial. Do fato que duas bases de um espaço vetorial tem a mesma cardinalidade, o resultado segue.

Neste caso, o cardinal de uma base de M como R– módulo é dito o posto do R–módulo M.

A seguinte proposição é de fácil verificação.

PROPOSIÇÃO 4.9:

(i) Se a sequência

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

é uma sequência exata de R–módulos à esquerda, então a sequência

$$N \bigotimes_R M' \xrightarrow{id_N \otimes f} N \bigotimes_R M \xrightarrow{id_N \otimes g} N \bigotimes_R M'' \longrightarrow 0$$

é também exata, para qualquer R–módulo à direita N.

(ii) Se a sequência

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

é uma sequência exata de R–módulos à direita, então a sequência

$$M' \underset{R}{\otimes} N \xrightarrow{f\otimes id_N} M \underset{R}{\otimes} N \xrightarrow{g\otimes id_N} M'' \underset{R}{\otimes} N \longrightarrow 0$$

também é exata, para qualquer R–módulo à esquerda N.

(iii) Se

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

é uma sequência exata que cinde, então a sequência

$$0 \longrightarrow M' \underset{R}{\otimes} N \xrightarrow{f\otimes id_N} M \underset{R}{\otimes} N \xrightarrow{g\otimes id_N} M'' \underset{R}{\otimes} N \longrightarrow 0$$

é também uma sequência exata que cinde, para qualquer R–módulo à esquerda N.

Dado um R–módulo ${}_RM$ e um epimorfismo $f : A_R \longrightarrow B_R$, segue de (ii) da proposição anterior que $f \otimes id_M : A \otimes_R M \longrightarrow B \otimes_R M$ é também um epimorfismo. Para alguns R–módulos vale uma propriedade análoga, no caso em que f é um monomorfismo. Este é o caso dos módulos projetivos, como veremos adiante. De fato esta última propriedade nos dá a seguinte

DEFINIÇÃO 4.10: Seja ${}_RM$ um R– módulo. ${}_RM$ é dito um módulo plano se, para todo monomorfismo $f : A_R \longrightarrow B_R$, $f \otimes id_M : A \otimes_R M \longrightarrow B \otimes_R M$ é também um monomorfismo.

Observemos que se tem uma definição análoga de módulos planos, para o caso de M ser um R–módulo à direita.

Provaremos agora um resultado sobre módulos planos.

TEOREMA 4.11: Seja ${}_RM = \bigoplus_{i\in I} M_i$. Então M é plano se e somente se M_i é plano, para cada $i \in I$.

Prova: Seja $f : A_R \longrightarrow B_R$ um monomorfismo de R–módulos. Consideremos o seguinte diagrama comutativo:

$$\begin{array}{ccc} A \otimes_R M = A \otimes_R (\bigoplus_{i\in I} M_i) & \xrightarrow{f\otimes id_M} & B \otimes_R (\bigoplus_{i\in I} M_i) = B \underset{R}{\otimes} M \\ \simeq \downarrow & & \downarrow \simeq \\ \bigoplus_{I\in I} (A \underset{R}{\otimes} M_i) & \xrightarrow{\sum_{i\in I}(f\otimes id_{M_i})} & \bigoplus_{i\in I} (B \underset{R}{\otimes} M_i) \end{array}$$

onde as setas verticais são os isomorfismos dados na propriedade 3 acima. Segue daí que $f \otimes id_M$ é um monomorfismo se e somente se $(f \otimes id_{M_i})$ é um monomorfismo, para cada $i \in I$. Assim, o teorema está provado.

Estamos agora em condições de provar o seguinte

TEOREMA 4.12: Todo R–módulo projetivo é plano.

Prova: Seja ${}_RM$ um R–módulo projetivo. Como todo módulo projetivo é isomorfo a um somando direto de um módulo livre, pelo teorema 4.11 é suficiente mostrarmos este teorema para o caso ${}_RM = {}_RR$. Isto segue da comutatividade do seguinte diagrama:

$$\begin{array}{ccc} A \otimes_R R & \xrightarrow{f \otimes id_R} & B \otimes_R R \\ \simeq \downarrow & & \downarrow \simeq \\ A & \xrightarrow{f} & B \end{array}$$

onde $f : A \longrightarrow B$ é um monomoirfismo de R– módulos à direita.

Finalizaremos este parágrafo apresentando o seguinte resultado, cuja prova pode ser encontrada em [6].

PROPOSIÇÃO 4.13: Seja R um anel comutativo e M, N dois R–módulos.

(i) Se M e N são finitamente gerados sobre R, então $M \otimes_R N$ é também um R–módulo finitamente gerado.

(ii) Se M e N são R– módulos projetivos, então $M \otimes_R N$ é também um R–módulo projetivo.

(iii) Se M e N são R– geradores, então $M \otimes_R N$ é também R– gerador.

(iv) Se M e N são R– progeradores, então $M \otimes_R N$ é também R– progerador.

§5. ÁLGEBRAS

Seja A um anel. Chamamos centro de A, e notamos por $Z(A)$, ao conjunto $Z(A) = \{a \in A : ax = xa, \forall x \in A\}$. Facilmente se vê que $Z(A)$ é um subanel de A e que A é comutativo se e somente se $Z(A) = A$.

Seja agora R um anel comutativo. Dizemos que um anel A é uma ÁLGEBRA SOBRE R (ou uma R-ÁLGEBRA) se existir um homomorfismo de anéis $\phi : R \longrightarrow Z(A)$. Se $A = Z(A)$, dizemos que A é uma R– ÁLGEBRA COMUTATIVA.

No que segue, sempre consideraremos R um anel comutativo com unidade, salvo mensão em contrário.

Dado uma R–álgebra A podemos dotá-la de uma estrutura de R–módulo à esquerda e à direita da seguinte forma: Se $\phi : R \longrightarrow Z(A)$ é o homomorfismo que caracteriza A como R–álgebra, então definimos a multiplicacão externa por $ra = \phi(r)a$ e $ar = a\phi(r)$, para cada $a \in A$, $r \in R$.

Observemos que esta definição equivale a dizer que A é um R–módulo satisfazendo $r(a_1a_2) = (ra_1)a_2 = a_1(ra_2)$, para cada $r \in R$, $a_1, a_2 \in A$. De fato, se A é um R–módulo satisfazendo tal propriedade, então $\phi : R \longrightarrow Z(A)$, dada por $\phi(r) = r1_A$ é um homomorfismo de anéis, como é fácil verificar.

Daremos agora alguns exemplos de R–álgebras:

EXEMPLO 1: Claramente o próprio anel R é uma R–álgebra. Basta considerar o homomorfismo identidade. Mais ainda, $R^{(n)} = \bigoplus_{i=1}^{n} R_i$, com $R_i \simeq R$ $(i = 1, 2, \ldots, n)$ é uma R–álgebra via a aplicação diagonal $r \mapsto (r, r, \ldots, r)$, para cada $r \in R$.

EXEMPLO 2: Consideremos G um grupo multiplicativo e S um anel com unidade. Definimos o ANEL DE GRUPO DE G SOBRE S, como o conjunto $S[G] = \{\sum_{g\in G} s_g g \ : \ s_g \in G, \forall g \in G, \text{ e } s_g = 0, \text{ exceto para um número finito de elementos } s \in S\}$.
As operações de $S[G]$ são definidas da seguinte forma:

$$\sum_{g\in G} r_g g + \sum_{g\in G} s_g g = \sum_{g\in G} (r_g + s_g)g$$

$$\sum_{g\in G} r_g g \sum_{h\in G} s_h h = \sum_{g,h\in G} (r_g s_h)gh$$

para todos $\sum_{g\in G} r_g g$, $\sum_{h\in G} s_h h \in S[G]$. Desta forma, $S[G]$ é um anel com unidade e é comutativo se e somente se S é comutativo e G é abeliano. Definindo-se uma multiplicação por escalares da forma $s(\sum_{g\in G} s_g g) = \sum_{g\in G} (ss_g)g$, para cada $s, s_g \in S$, $g \in G$, $S[G]$ torna-se um S–módulo livre com base formada pelos elementos de G. Se S é um anel comutativo, teremos $s[(\sum_{g\in G} s_g g)(\sum_{h\in G} r_h h)] = s(\sum_{\substack{g\in G \\ h\in G}} (s_g r_h)gh) = \sum_{\substack{g\in G \\ h\in G}} (ss_g r_h)gh = \sum_{\substack{g\in G \\ h\in G}} (s_g s r_h)gh = (\sum_{g\in G} s_g g)(\sum_{h\in G} (sr_h)h) = (\sum_{g\in G} s_g g)[s(\sum_{h\in G} r_h h)]$, para cada $s \in S$, $\sum_{g\in G} s_g g$, $\sum_{h\in G} r_h h \in S[G]$. Assim, $S[G]$ é uma S–álgebra, se S é comutativo. Esta S–álgebra é chamada ÁLGEBRA DE GRUPO de G sobre S.

EXEMPLO 3: Se K é um corpo, então um anel $A \neq 0$ é uma K–álgebra se e somente se A for um anel contendo um subanel isomorfo a K, pois neste caso o homomorfismo $\phi : K \longrightarrow Z(A)$, que define a estrutura de K–álgebra é necessariamente injetivo.

EXEMPLO 4: Seja R um anel. Consideremos $\mathcal{M}_n(R)$ o anel das matrizes quadradas de ordem n sobre R. Então $\mathcal{M}_n(R)$ é uma R– álgebra. De fato, seja $I \in \mathcal{M}_n(R)$ a matriz identidade. Consideremos a aplicação $\phi : R \longrightarrow \mathcal{M}_n(R)$ dada por $\phi(r) = rI$, para todo $r \in R$. Claramente ϕ é um homomorfismo de anéis e $rI \in Z(\mathcal{M}_n(R))$.

Seja A uma R–álgebra. Então um subanel de A, o qual é uma R–álgebra via o mesmo homomorfismo que define a R–álgebra A, será dito uma SUBÁLGEBRA de A.

Dadas duas R–álgebras A e B, dizemos que uma aplicação $f : A \longrightarrow B$ é um homomorfismo de R–álgebras se f é um homomorfismo de anéis e também um homomorfismo de R–módulos. O leitor poderá verificar que $f : A \longrightarrow B$ é um homomorfismo de R–álgebras se e somente se o diagrama abaixo comuta:

$$\begin{array}{ccc} R & \xrightarrow{\phi_B} & B \\ {\scriptstyle \phi_A}\downarrow & \nearrow_{f} & \\ A & & \end{array}$$

onde ϕ_A e ϕ_b São as respectivas aplicações canônicas.

Sejam A e B duas R–álgebras. Podemos considerar o produto tensorial $A \otimes_R B$, o qual também é um R–módulo. Definindo-se em $A \otimes_R B$ um produto da forma $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$, para cada $a_1 \otimes b_1, a_2 \otimes b_2 \in A \otimes_R B$, $A \otimes_R B$ torna-se uma R– álgebra. Observemos que este produto está bem definido. De fato, fixamos $a_2 \in A$ e $b_2 \in B$ e sejam $f : A \longrightarrow A$ e $g : B \longrightarrow B$ definidos por $f(a) = aa_2$ e $g(b) = bb_2$, respectivamente. Consideremos $\varphi : A \times B \longrightarrow A \otimes B$ definido por $\varphi(a, b) = f(a) \otimes g(b)$. Assim, φ é R–bilinear e pela propriedade universal do produto tensorial, segue que existe um único homomorfismo de grupos $f \otimes g : A \otimes B \longrightarrow A \otimes B$ tal que $(f \otimes g)(a \otimes b) = f(a) \otimes g(b) = aa_2 \otimes bb_2$. Segue daí que a multiplicação definida acima está bem definida, como queríamos provar.

Observemos ainda que se A e B são R–álgebras comutativas, então as estruturas de A–módulo e B– módulo de $A \otimes_R B$ fazem deste anel uma álgebra sobre A e B, respectivamente.

§6. ÁLGEBRAS SEPARÁVEIS

Dado um anel A, denotaremos por A^o ao anel definido sobre o próprio conjunto A, com a mesma adição de A e com a multiplicação definida como segue: $x * y = yx$, para

todos $x, y \in A^o$. Com estas operações é fácil ver que A^o é também um anel, chamado ANEL OPOSTO DE A. Ainda, A é um anel comutativo se e somente se $A = A^o$. É fácil ver também que se A é uma R–álgebra então A^o também o é. Neste caso, A^o é chamada de ÁLGEBRA OPOSTA DE A. Podemos considerar o produto tensorial das R–álgebras $A \otimes A^o$, o qual também é uma R–álgebra, denominada ÁLGEBRA ENVOLVENTE DE A e denotada por A^e.

Seja então A uma R–álgebra e consideremos sua álgebra envolvente $A^e = A \otimes A^o$. A R– álgebra A possui uma estrutura de A^e–módulo à esquerda, via a operação externa $(a \otimes c^o)b = abc^o$, para todos $a \otimes c^o \in A^e$, $b \in A$, como é fácil verificar.

Existe também uma aplicação $\mu : A^e \longrightarrow A$, definida por $\mu(a \otimes c^o) = ac^o$, para cada $a \otimes c^o \in A^e$. Assim, μ está bem definida e é um homomorfismo de A^e–módulos. De fato, consideremos a aplicação $f : A \times A^o \longrightarrow A$, dada por $f(a, c^o) = ac^o$, para cada $(a, c^o) \in A \times A^o$. Temos que f é R–bilinear. Logo, pela propriedade universal do produto tensorial, existe um único homomorfismo $\bar{f} : A \otimes A^o \longrightarrow A$, tal que $\bar{f}(a \otimes c^o) = f(a, c^o) = ac^o$, para cada $a \otimes c^o \in A \otimes A^o$. Então $\bar{f} = \mu$. Mais ainda, μ é um epimorfismo de A^e–módulos, como é fácil ver. Este homomorfismo é chamado HOMOMORFISMO CONTRAÇÃO.

A partir de agora não faremos mais distinção entre um elemento $a \in A$ e seu correspondente $a^o \in A^o$, indicando ambos por a, para simplificar notações.

Fazendo $J = ker\mu$, obtemos a seguinte seqüência exata de A^e–módulos

$$0 \longrightarrow J \hookrightarrow A^e \xrightarrow{\mu} A \longrightarrow 0$$

Mostraremos agora que J é exatamente o ideal de A^e gerado por todos os elementos da forma $a \otimes 1 - 1 \otimes a$. De fato, temos $a \otimes 1 - 1 \otimes a \in J$, pois $\mu(a \otimes 1 - 1 \otimes a) = a - a = 0$. Reciprocamente, se $\sum_{i=1}^{n} a_i \otimes b_i \in J$, segue que $\sum_{i=1}^{n} a_i b_i = 0$ e daí, $0 = 0 \otimes 1 = \sum_{i=1}^{n} a_i b_i \otimes 1$. Assim, $\sum_{i=1}^{n} a_i \otimes b_i = \sum_{i=1}^{n} a_i \otimes b_i - (\sum_{i=1}^{n} a_i b_i \otimes 1) = \sum_{i=1}^{n} (a_i \otimes 1)(1 \otimes b_i) - \sum_{i=1}^{n} (a_i \otimes 1)(b_i \otimes 1) = \sum_{i=1}^{n} (a_i \otimes 1)(1 \otimes b_i - b_i \otimes 1)$

No que segue, μ sempre denotará o homomorfismo contração e J seu núcleo. Estamos agora em condições de provar o seguinte

TEOREMA 6.1: Seja A uma R–álgebra. Então as seguintes condições são equivalentes:

(i) A é um A^e–módulo projetivo;

(ii) A seqüência exata de A^e–módulos

$$0 \longrightarrow J \hookrightarrow A^e \xrightarrow{\mu} A \longrightarrow 0$$

cinde;

(iii) Existe um elemento $e \in A^e$ tal que $\mu(e) = 1$ e $Je = 0$;

(iv) Existem elementos $x_i, y_i \in A$, com $0 \leq i \leq n$, tais que

$$\sum_{i=1}^{n} x_i y_i = 1$$

e

$$\sum_{i=1}^{n} xx_i \otimes y_i = \sum_{i=1}^{n} x_i \otimes y_i x$$

para cada $x \in A$.

Prova: Claramente (i) e (ii) são condições equivalentes. Para mostrarmos que (ii) implica (iii) suponhamos que a seqüência

$$0 \longrightarrow J \hookrightarrow A^e \xrightarrow{\mu} A \longrightarrow 0$$

cinde. Então existe um A^e-homomorfismo $\psi : A \longrightarrow A^e$, com $\mu \circ \psi = id_A$. Agora, escolhendo $e = \psi(1)$, temos $\mu(e) = 1$. Mostremos que este é o elemento procurado em (iii). Para tanto, só falta ver que $Je = 0$. De fato, para cada $1 \otimes a - a \otimes 1 \in J$, temos $(1 \otimes a - a \otimes 1)e = (1 \otimes a - a \otimes 1)\psi(1) = \psi[(1 \otimes a - a \otimes 1)1] = \psi[(1 \otimes a)1 - (a \otimes 1)1] = \psi(a - a) = 0$. Assim, como J é gerado por todos os elementos da forma $1 \otimes a - a \otimes 1$ segue que $Je = 0$, como queríamos mostrar.

Reciprocamente, dado $e \in A^e$ tal que $\mu(e) = 1$ e $Je = 0$, e considerando a aplicação $\psi : A \longrightarrow A^e$ dada por $\psi(a) = (a \otimes 1)e$, para cada $a \in A$, temos que ψ é um homomorfismo de A^e–módulos. De fato, como $Je = 0$ temos $(1 \otimes a)e = (a \otimes 1)e$. Daí, $\psi(a) = (a \otimes 1)e = (1 \otimes a)e$ e assim, $\psi(a \otimes a'x) = \psi(axa') = (axa' \otimes 1)e = (ax \otimes 1)(a' \otimes 1)e = (ax \otimes 1)(1 \otimes a')e = (ax \otimes a')e = (a \otimes a')(x \otimes 1)e = (a \otimes a')\psi(x)$ para todos $(a \otimes a') \in A^e$, $x \in A$. Além disso, $\mu \circ \psi(a) = \mu((a \otimes 1)e) = (a \otimes 1)\mu(e) = a\ 1\ 1 = a$ para cada $a \in A$. Assim, a seqüência de A^e– módulos

$$0 \longrightarrow J \hookrightarrow A^e \xrightarrow{\mu} A \longrightarrow 0$$

cinde. Isto mostra que (iii) implica (ii).

$x_i = y_i = e_i$, $1 \leq i \leq n$, obtemos $\sum_{i=1}^{n} x_i \tau(y_i) = \sum_{i=1}^{n} e_i \sigma^j(e_i) = \sum_{i=1}^{n} e_i e_{i+j \pmod n} = \delta_{0,j}$, já que $e_i e_{i+j \pmod n} = \delta_{i,i+j \pmod n}$. Portanto, (S, σ) é uma extensão de Galois de R.

EXEMPLO 2.2: Seja p um número primo e R uma álgebra comutativa sobre $\mathbb{Z}/p\mathbb{Z}$ (ou seja, R é um anel de característica p). Dado $r \in R$, consideremos $R[x] = R[X]/(X^p - X - r)$, onde $x = X + (X^p - X - r)$ é a classe de X módulo o ideal gerado por $X^p - X - r$. Consideremos ainda $\sigma : R[x] \to R[x]$, definido por $\sigma/R = id_R$ e $\sigma(x) = x + 1$. Nestas condições, $(R[x], \sigma)$ é uma extensão de Galois de R com grupo cíclico de ordem p.

Inicialmente mostraremos que σ está bem definida e é um automorfismo de $R[x]$. Consideremos $\varphi : R[X] \to R[X]$, definida por $\varphi/_R = id_R$ e $\varphi(X) = X + 1$ e ainda $\psi : R[X] \to R[X]$ definida por $\psi/R = id_R$ e $\psi(X) = X - 1$. Claramente φ e ψ são homomorfismos de anéis. Além disso, $\varphi \circ \psi(X) = \varphi(X - 1) = X$ e $\psi \circ \varphi(X) = \psi(X + 1) = X$. Portanto, $\varphi \circ \psi = \psi \circ \varphi = id_{R[X]}$ e então φ é um automorfismo de $R[X]$.

Como $\varphi(X^p - X - r) = (X+1)^p - (X+1) - r = X^p + 1 - X - 1 - r = X^p - X - r$, segue que $\varphi(I) = I$, onde I é o ideal gerado por $X^p - X - r$. Então φ induz um automorfismo $\sigma : R[x] \to R[x]$, dado por $\sigma/R = id_R$ e $\sigma(x) = x + 1$, onde $R[x] = R[X]/(X^p - X - r)$ e $x = X + (X^p - X - r)$. Assim, σ está bem definida e é um automorfismo de $R[x]$.

Para ver que σ tem ordem p, observemos que $\sigma^i(x) = x + i1$, $0 \leq i \leq p$. Assim, $\sigma^i(x) \neq x$ para todo $1 \leq i \leq p - 1$ e $\sigma^p(x) = x$. Isto mostra que $\sigma^p = id$ e $\sigma^i \neq id$, se $1 \leq i \leq p - 1$.

Agora, dado $\alpha = \sum_{i=0}^{p-1} a_i x^i \in R[x]$, com $a_i \in R$, $0 \leq i \leq p - 1$, temos $\sigma(\alpha) = \sigma(\sum_{i=0}^{p-1} a_i x^i) = \sum_{i=0}^{p-1} a_i \sigma(x)^i = \sum_{i=0}^{p-1} a_i (x+1)^i$. Então $\sigma(\alpha) = \alpha$ se e somente se $\sum_{i=0}^{p-1} a_i (x+1)^i = \sum_{i=0}^{p-1} a_i x^i$. Esta igualdade nos dá o seguinte sistema:

$$\begin{cases} a_0 &= a_0 + a_1 + \cdots + a_i + \cdots + a_{p-1} \\ a_1 &= a_1 + \cdots + i a_i + \cdots + p - 1 a_{p-1} \\ \vdots & \vdots \quad \vdots \\ a_i &= \binom{i}{i} a_i + \cdots + \binom{p-1}{i} \\ \vdots & \vdots \quad \vdots \\ a_{p-1} &= a_{p-1} \end{cases}$$

o qual admite solução do tipo $a_i = 0$ $(1 \leq i \leq p-1)$ e $a_0 \in R$, como é fácil verificar. Logo $\sigma(\alpha) = \alpha$ se e somente se $\alpha = a_0 \in R$. Portanto $(R[x])^{(\sigma)} = R$.

Finalmente mostraremos que $(R[x], \sigma)$ é uma extensão de Galois de R, Mostrando que vale o ítem (f) do teorema 1.6. Antes, observemos que, para cada $\tau \in (\sigma)$, $\tau \neq id$, existe $j \in \{1, \ldots, p-1\}$ tal que $\tau = \sigma^j$. Assim, $\tau(x) - x = \sigma^j(x) - x = x + j1 - x = j$, onde j é inversível em R, sendo $0 \neq j = j1_R = \bar{j} \in \mathbb{Z}/p\mathbb{Z}$. então $\tau(x) - x \notin \mathcal{M}$, para todo $\tau \in (\sigma)$, $\tau \neq id$ e para todo ideal maximal $\mathcal{M}$ de $R[x]$. Portanto $(R[x], \sigma)$ é uma extensão de galois de R com grupo de Galois cíclico de ordem p.

EXEMPLO 2.3: Seja R um anel comutativo com unidade. Seja n um inteiro maior ou igual a 2, tal que $n \in R^*$, onde R^* representa o conjunto dos elementos de R que são inversíveis em R. Suponhamos que existe uma raiz n–ésima primitiva da unidade $\xi \in R$ tal que $1 - \xi^i \in R^*$ para todo $1 \leq i \leq n$. Seja $a \in R^*$ e consideremos $S = R[x] = R[X]/(X^n - a)$, onde $x = X + (X^n - a)$. Nestas condições, (S, σ) é uma extensão de Galois de R com grupo de Galois cíclico de ordem n, onde σ é tal que $\sigma(x) = \xi x$.

Consideremos inicialmente os homomorfismos $\varphi : R[X] \to R[X]$, dado por $\varphi/R = id_R$ e $\varphi(X) = \xi X$ e $\psi : R[X] \to R[X]$, dado por $\psi/R = id_R$ e $\psi(X) = \xi^{n-1}X$. Assim temos $\psi \circ \varphi(X) = \psi(\xi X) = \xi\psi(X) = \xi\xi^{n-1}X = \xi^n X = X$ e $\varphi \circ \psi(X) = \varphi(\xi^{n-1}X) = \xi^{n-1}\varphi(X) = \xi^{n-1}\xi X = \xi^n X = X$. Logo, $\psi \circ \varphi = \varphi \circ \psi = id_{R[X]}$, o que mostra que φ é um isomorfismo. Agora, como $\varphi(X^n - a) = \varphi(X)^n - \varphi(a) = \xi^n X^n - a = X^n - a$, segue daí que $\varphi(I) = I$, onde I é o ideal gerado por $(X^n - a)$. Então φ induz um R–automorfismo $\sigma : R[X]/(X^n - a) \to R[X]/(X^n - a)$ tal que $\sigma(x) = \xi x$, onde $x = X + (X^n - a)$. Além disso, a ordem de σ é igual a n, pois $\sigma^i(x) = \xi^i x \neq x$ $(1 \leq i \leq n-1)$ e $\sigma^n(x) = \xi^n x = x$. Segue daí que (σ) é um grupo cíclico de ordem n.

Consideremos agora $s \in S = R[x]$. Temos $s = \sum_{i=0}^{n-1} a_i x^i$, com $a_i \in R$ $(0 \leq i \leq n-1)$. Então $\sigma(s) = \sigma(\sum_{i=0}^{n-1} a_i x^i) = \sum_{i=0}^{n-1} a_i \sigma(x)^i = \sum_{i=0}^{n-1} a_i \xi^i x^i$. Logo, $\sigma(s) = s$ se e somente se $\sum_{i=0}^{n-1} a_i \xi^i x^i = \sum_{i=0}^{n-1} a_i x^i$. Não é difícil ver que isto equivale a $a_i = 0$ para todo $1 \leq i \leq n-1$, uma vez que $1 - \xi^i \in R^*$ para tais valores de i. Assim, $\sigma(s) = s$ se e somente se $s = a_0 \in R$, isto é, $S^\sigma = R$.

Para mostrar que (S, σ) é uma extensão de Galois de R, dado $\tau \in (\sigma)$, com $\tau \neq id$, basta encontrarmos $\lambda \in R[x]$ tal que $\tau(\lambda) - \lambda \notin \mathcal{M}$, para todo ideal maximal $\mathcal{M}$ de

$R[x]$. Seja então $\tau = \sigma^j$ $(1 \leq i \leq n-1)$. Tomando-se $\lambda = x = X + (X^n - a)$ tem-se: $\tau(\lambda) - \lambda = \tau(x) - x = \sigma^j(x) - x = \xi^j x - x = (\xi^j - 1)x$. Agora, $(\xi^j - 1)x \in \mathcal{M}$, para todo ideal maximal $\mathcal{M}$ de S, pois $\xi^j - 1$ e x são inversíveis em S (já que $x^n = a \in R^*$). Portanto, (S, σ) é uma extensão de Galois de R com grupo de Galois cíclico de ordem n, como queríamos provar.

Nosso próximo exemplo mostra uma extensão de Galois cujo grupo de Galois não é cíclico.

EXEMPLO 2.4: Seja R um anel comutativo com unidade. Consideremos (S, G) e (T, H) duas extensões de Galois de R com grupos de Galois G e H, respectivamente. Então $S \otimes T$ é uma extensão de Galois de R com grupo de Galois $G \times H = \{(\sigma, \tau) : \sigma \in G, \tau \in H\}$, onde $G \times H$ atua sobre $S \otimes T$ via $(\sigma, \tau)(s \otimes t) = \sigma(s) \otimes \tau(t)$, para todos $s \otimes t \in S \otimes T$, $(\sigma, \tau) \in G \times H$.

Vamos mostrar inicialmente que $(S \otimes T)^{G \times H} = R$. Segue do corolário II.1.9 que $S \otimes T$ é uma extensão de Galois de S com grupo de galois H, onde H é visto como $\{id\} \times H$. Analogamente, $S \simeq S \otimes R$ é uma extensão de Galois de R com grupo $G \simeq G \times \{id\}$. Logo, temos: $(S \otimes T)^{G \times H} = ((S \otimes T)^{\{id\} \times H})^{G \times \{id\}} = (S \otimes R)^{G \times \{id\}} = R \otimes R \simeq R$.

Para mostrar que $S \otimes T$ é uma extensão de Galois de R, basta exibir as coordenadas de Galois de $S \otimes T$ sobre R.

Do fato que (S, G) e (T, H) são extensões de Galois de R, segue que existem elementos $x_1, \ldots, x_n; y_1, \ldots, y_n \in S$ e $u_1, \ldots, u_m; v_1, \ldots, v_n \in T$, tais que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma}$, para cada $\sigma \in G$ e $\sum_{j=0}^{m} u_j \tau(v_j) = \delta_{1,\tau}$, para cada $\tau \in H$. Tomando então $a_{ij} = x_i \otimes u_j$, $b_{ij} = y_i \otimes v_j$, $1 \leq i \leq n$ e $1 \leq j \leq m$, temos $\sum_{i,j} a_{ij}(\sigma, \tau)(b_{ij}) = \sum_{i,j} (x_i \otimes u_j)(\sigma, \tau)(y_i \otimes v_j) = \sum_{i,j} (x_i \otimes u_j)(\sigma(y_i) \otimes \tau(v_j)) = \sum_{i,j} x_i \sigma(y_i) \otimes u_j \tau(v_j) = \sum_{i=1}^{n} x_i \sigma(y_i) \bigotimes \sum_{j=1}^{m} u_j \tau(v_j) = \delta_{1,\sigma} \otimes \delta_{1,\tau} = \delta_{1,(\sigma,\tau)}$, para cada $(\sigma, \tau) \in G \times H$. Segue daí que $S \otimes T$ é uma extensão de Galois de R com grupo de Galois $G \times H$.

O exemplo anterior pode ser generalizado. Mais precisamente, se $(S_1, G_1), \ldots, (S_n, G_n)$ são extensões de Galois de R, então $S_1 \otimes \cdots \otimes S_n$ é uma extensão de Galois de R com grupo de Galois $G_1 \times \cdots \times G_n$.

Além disso, aplicado aos exemplos anteriores, este exemplo permite construir extensões de Galois com grupos de Galois do tipo $G \times G \times \cdots \times G$, onde G é um grupo cíclico de

ordem finita.

Se (S, G) é uma extensão de Galois de R, onde o grupo de G é abeliano, dizemos que S é uma EXTENSÃO ABELIANA DE R.

Como todo grupo abeliano finito G admite uma decomposição do tipo $G = H_1 \times H_2 \times \cdots \times H_r$, onde cada H_i é um grupo de ordem potência de um primo, então o exemplo 2.4 aplicado a teoria do próximo capítulo, nos permite construir extensões abelianas de R.

§3. O TEOREMA FUNDAMENTAL DA TEORIA DE GALOIS DE ANÉIS

Neste parágrafo provaremos o chamado teorema fundamental da teoria de Galois de anéis, o qual generaliza o teorema fundamental da teoria de Galois de corpos. Para que nossos resultados também sejam válidos para anéis com idempotentes próprios, precisamos da seguinte

DEFINIÇÃO 3.1: Seja S uma extensão de Galois de R com grupo de Galois G e seja T um subanel de S. Dizemos que T é G–forte, se a restrição à T de qualquer dois elementos de G forem iguais ou fortemente distintos, como aplicações de T em S.

Claramente, se S não possui idempotentes próprios, então qualquer subanel de S é G–forte. Estamos agora em condições de provar o seguinte

TEOREMA 3.2: Sejam S uma extensão de Galois de R com grupo de Galois G, H um subgrupo de G e $T = S^H$. Então T é uma R–algebra separável G–forte, S é uma extensão de Galois de T com grupo de Galois H e H é o conjunto de todos os elementos de G que, restritos à T, são a identidade. Se, além disso, H é normal em G, então T é uma extensão de Galois de R com grupo de Galois G/H.

Prova: Temos que mostrar as seguintes afirmações:

(i) T é uma R–álgebra separável e G–forte;

(ii) S é uma extensão de Galois de T com grupo de Galois H;

(iii) $H = \{\sigma \in G : \sigma(t) = t, \forall t \in T\}$;

(iv) Se $H \lhd G$ então T é uma extensão de Galois de R com grupo de Galois G/H.

Sejam $x_1, \ldots, x_n; y_1, \ldots, y_n \in S$ tais que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma}$, para qualquer $\sigma \in G$. Em particular, $\sum_{i=1}^{n} x_i \tau(y_i) = \delta_{1,\tau}$, para todo $\tau \in H \subseteq G$. Sendo por hipótese, $T = S^H$, segue do teorema 1.6(b), que S é uma extensão de Galois de T com grupo de Galois H. Isto mostra (ii).

Seja agora $H' = \{\sigma \in G : \sigma(t) = t, \forall t \in T\}$. Queremos mostrar que $H = H'$. Claramente, H' é um subgrupo de G e $H \subseteq H'$. Ainda, $S^H = T = S^{H'}$, como é fácil verificar. Então S é uma extensão de Galois de T com grupo de Galois igual a H e H'. Segue do teorema 1.6(e) que $S \otimes S$ é um S–módulo livre de posto n e também n', onde $n = \mid H \mid$ e $n' = \mid H' \mid$. Como S é um anel comutativo resulta da proposição I.4.7, que $n = n'$, ou seja, $H = H'$, o que mostra (iii).

Agora, por 1.6(c) S é um T–módulo projetivo e finitamente gerado. Logo existem elementos $s_1, \ldots, s_r; \varphi_1, \ldots, \varphi_r \in Hom_T(S, T)$, coordenadas projetivas de S como T–módulo. Então, $s_i \otimes s_j \in S \otimes S$ e $\varphi_i \otimes \varphi_j \in Hom_{T \otimes T}(S \otimes S, T \otimes T)$, $1 \leq i, j \leq r$, são coordenadas projetivas de $S \otimes S$ como $T \otimes T$–módulo, como é fácil verificar.

Como S é uma extensão separável de R, S é projetivo sobre $S \otimes S$. Logo S é projetivo sobre $T \otimes T$, pela transitividade dos módulos projetivos (proposição I.2.5). Agora, do fato de S ser uma extensão de Galois de T e do corolário 1.8, segue que T é um T–somando direto de S, e isto implica que T é um $T \otimes T$–somando direto de S. Portanto, T é um $T \otimes T$–módulo projetivo. Consequentemente, T é uma R–álgebra separável. Obtemos assim a primeira parte de (i).

Para mostrar que T é G–forte faremos as seguintes observações. Como S é uma extensão de Galois de T com grupo de Galois H, segue do corolário 1.8 que existe $c \in S$ tal que $tr_H(c) = \sum_{\rho \in H} \rho(c) = 1$. Sejam $x_1, \ldots, x_n; y_1, \ldots, y_n \in S$, satisfazendo a condição (b) do teorema 1.6, para S e G, e sejam $x_i' = \sum_{\rho \in H} \rho(x_i c)$, $y_i' = \sum_{\rho \in H} \rho(y_i)$, $1 \leq i \leq n$. Temos $x_i', y_i' \in S^H = T$. De fato, para todo $\tau \in H$, $\tau(y_i') = \tau(\sum_{\rho \in H} \rho(y_i)) = \sum_{\rho \in H} \tau\rho(y_i) = \sum_{\tau\rho \in H} \tau\rho(y_i) = y_i'$, $1 \leq i \leq n$. Analogamente, $\tau(x_i') = x_i'$, $1 \leq i \leq n$. Além disso, para $\sigma \in G$, $\sum_{i=1}^{n} x_i' \sigma(y_i') = \sum_{i=1}^{n} \left(\sum_{\rho \in H} \rho(x_i c) \right) \sigma \left(\sum_{\tau \in H} \tau(y_i) \right) = \sum_{i=1}^{n} \left(\sum_{\rho \in H} \rho(x_i c) \sum_{\tau \in H} \sigma\tau(y_i) \right) = \sum_{i=1}^{n} \sum_{\rho, \tau \in H} \rho(x_i c)\sigma\tau(y_i) = \sum_{\rho, \tau \in H} \rho(c) \left(\sum_{i=1}^{n} \rho(x_i)\sigma\tau(y_i) \right) = \sum_{\rho, \tau \in H} \rho(c)\delta_{\rho, \sigma\tau}$. Se $\sigma \notin H$, não podemos ter $\sigma\tau = \rho$ (caso contrário, teríamos $\sigma = \rho\tau^{-1} \in H$, uma contradição). Consequentemente, $\sum_{i=1}^{n} x_i' \sigma(y_i') = 0$. Se $\sigma \in H$, existe exatamente um $\tau \in H$ tal que $\sigma\tau = \rho$. Então temos: $\sum_{i=1}^{n} x_i' \sigma(y_i') = \sum_{\rho, \tau \in H} \rho(c)\delta_{\rho, \sigma\tau} = \sum_{\rho \in H} \rho(c) = 1$. Logo, $\sum_{i=1}^{n} x_i' \sigma(y_i') = 0$ se $\sigma \notin H$ e $\sum_{i=1}^{n} x_i' \sigma(y_i') = 1$ se $\sigma \in H$.

Consideremos agora $\sigma, \tau \in G$ tal que $\sigma/T \neq \tau/T$. Então $\tau\sigma^{-1} \notin H$, pois se $t \in T$ é tal que $\sigma(t) = t_1 \neq t_2 = \tau(t)$, segue que $\tau\sigma^{-1}(t_1) = \tau(t) = t_2$. Seja $e \in S$ um idempotente tal que $\sigma(t)e = \tau(t)e$, para todo $t \in T$. Então $\sigma(y_i')e = \tau(y_i')e$, para cada $i = 1, 2, \ldots, n$. Segue daí que $0 = \sum_{i=1}^{n} x_i'\tau^{-1}\sigma(y_i')\tau^{-1}(e) = \sum_{i=1}^{n} x_i'\tau^{-1}(\sigma(y_i')e) = \sum_{i=1}^{n} x_i'\tau^{-1}(\tau(y_i')e) = \sum_{i=1}^{n} x_i'y_i'\tau^{-1}(e) = \tau^{-1}(e)$, donde segue que $e = 0$. Portanto, T é G-forte, completando a prova de (i).

Suponhamos finalmente que H é normal em G. Então para cada $\sigma \in G$, $\tau \in H$, temos $\sigma\tau\sigma^{-1} \in H$, isto é, $\sigma^{-1}\tau\sigma(t) = t$, para todo $t \in T$. Equivalentemente, $\tau(\sigma(t)) = \sigma(t)$, para todo $t \in T$, ou ainda, $\sigma(t) \in T = S^H$, para todo $t \in T$. Isto é o mesmo que dizer que σ/T é um automorfismo de T, para todo $\sigma \in G$.

Consideremos o grupo quociente G/H. É fácil ver que para $\bar{\sigma} = \sigma H \in G/H$, temos $\bar{\sigma} = \{\tau \in G : \tau/T = \sigma/T\}$. Observemos ainda que a cada $\bar{\sigma} \in G/H$ associa-se um único automorfismo, a saber, σ/T de T. Logo G/H é isomorfo a um grupo de automorfismos de T. Temos que mostrar ainda que $T^{G/H} = R$. Claramente $T^{G/H} \supseteq R$. Reciprocamente, se $t \in T^{G/H}$, então $\sigma(t) = t$, para todo $\sigma \in G$. Isto significa que $t \in S^G = R$. Portanto $T^{G/H} = R$,como queríamos mostrar.

Falta ver que T é uma extensão de Galois de R. Para tanto, basta observar que os elementos x_i', y_i' $(1 \leq i \leq n)$ definidos acima, satisfazem o ítem (b) do teorema 1.6, para T e R, pois se $\bar{\sigma} = id_T$, então $\sigma \in H$ e daí $\sum_{i=1}^{n} x_i'\bar{\sigma}(y_i') = 1$. Agora, se $\bar{\sigma} \neq id_T$, $\sigma \notin H$ e neste caso, $\sum_{i=1}^{n} x_i'\bar{\sigma}(y_i') = 0$. Isto mostra (iv) e completa a prova do teorema.

Para provar o teorema fundamental, precisamos de uma recíproca do teorema anterior. Temos o seguinte

TEOREMA 3.3: Seja S uma extensão de Galois de R com grupo de Galois G e T uma R-subálgebra separável de S [a qual é G-forte]. Seja H o subgrupo de G definido por $H = \{\tau \in G : \tau(t) = t, \forall t \in T\}$. Então $T = S^H$.

Prova: Como $H = \{\tau \in G : \tau(t) = t, \forall t \in T\}$, segue que $T \subseteq S^H$. Então temos que mostrar apenas que $S^H \subseteq T$. Pelo corolário 1.9, $S \otimes S$ é uma extensão de Galois de S com grupo de Galois G, onde G atua sobre $S \otimes S$ via a segunda variável (isto é, $\sigma(s \otimes s') = s \otimes \sigma(s')$, para cada $s \otimes s' \in S \otimes S$, $\sigma \in G$). Consideremos o isomorfismo $h : S \otimes S \to E$ do teorema 1.6(e). Segue daí que E é também uma extensão de Galois de

S com grupo de Galois G, onde a ação de G se transporta para E via o isomorfismo h. Vejamos como é esta ação. Para cada $\sigma \in G$, $v \in E$, temos $h^{-1}(v) = \sum_i s_i \otimes t_i \in S \bigotimes S$. Então, $(\sigma(v))(\tau) = (h \circ \sigma \circ h^{-1}(v))(\tau) = h \circ \sigma[(\sum_i s_i \otimes t_i)](\tau) = \sum_i h(s_i \otimes \sigma(t_i))(\tau) = \sum_i s_i \tau\sigma(t_i)$, para cada $\tau \in G$. Agora, $v(\tau\sigma) = hh^{-1}(v)(\tau\sigma) = \sum_i h(s_i \otimes t_i)(\tau\sigma) = \sum_i s_i \tau\sigma(t_i)$. Logo, a ação de G em E está definida por $(\sigma(v))(\tau) = v(\tau\sigma)$.

T é um subanel de S e como S é R– projetivo a injeção $T \hookrightarrow S$ induz um monomorfismo $S \otimes T \to S \otimes S$. Então podemos identificar $S \otimes T$ com $h(S \otimes T) \subseteq E$. Mostraremos a seguir que $E^H = h(S \otimes T)$.

Seja $G = \bigcup_{i=1}^{r} \sigma_i H$ uma partição de G, onde $\sigma_i H \neq \sigma_j H$, se $i \neq j$, $1 \leq i, j \leq r$ e $E^H = \{v \in E : \tau(v) = v, \forall \tau \in H\}$. Então $v \in E^H$ se e somente se $\tau(v) = v$, para cada $\tau \in H$, isto é, $v(\sigma) = (\tau(v))(\sigma) = v(\sigma\tau)$, para cada $\sigma \in G$, $\tau \in H$. Logo, $v(\sigma_i\tau) = v(\sigma_i)$, para cada $\tau \in H$, $1 \leq i \leq r$. Segue daí que v é constante sobre cada classe lateral $\sigma_i H$ $(1 \leq i \leq r)$. Reciprocamente, se v é constante sobre cada classe lateral $\sigma_i H$ $(1 \leq i \leq r)$, então temos $v(\sigma\tau) = v(\sigma)$, para cada $\sigma \in G$, $\tau \in H$. Assim, $(\tau(v))(\sigma) = v(\sigma\tau) = v(\sigma)$ e segue que $\tau(v) = v$, para todo $\tau \in H$, isto é, $v \in E^H$. Portanto, E^H é o conjunto de todas as funções de G em S, as quais são constantes em cada classe σH, com $\sigma \in G$. Assim, se $s \otimes t \in S \otimes S^H$, para cada $\tau \in H$ e $1 \leq i \leq r$, temos $h(s \otimes t)(\sigma_i\tau) = s\sigma_i\tau(t) = s\sigma_i(t) = h(s \otimes t)(\sigma_i)$. Segue que $h(S \otimes T) \subseteq h(S \otimes S^H) \subseteq E^H$.

É fácil ver que as aplicações $f_i : E \to S$, definidas por $f_i(v) = v(\sigma_i)$, $1 \leq i \leq r$, são homomorfismos de S–álgebras. Mostraremos que $f_1, \ldots, f_r$ são fortemente distintas como homomorfismos de $h(S \otimes T)$ em S, denotando ainda com f_i a restrição de cada f_i à S–subálgebra $h(S \otimes T)$ de E. Se $i \neq j$ então $\sigma^{-1}\sigma_j \notin H$. Logo existe $t \in T$ tal que $\sigma_i(t) \neq \sigma_j(t)$. Assim, $f_i(h(1 \otimes t)) = h(1 \otimes t)(\sigma_i) = \sigma_i(t) \neq \sigma_j(t) = h(1 \otimes t)(\sigma_j) = f_j(h(1 \otimes t))$ e segue que $f_i/h(S \otimes T) \neq f_j/h(S \otimes T)$. Seja $e \in S$ um idempotente não nulo. Como T é G–forte, existe $t \in T$ tal que $\sigma_i(t)e \neq \sigma_j(t)e$. Logo, $f_i(h(1 \otimes t))e = h(1 \otimes t)(\sigma_i)e = \sigma_i(t)e \neq \sigma_j(t)e = h(1 \otimes t)(\sigma_j)e = f_j(h(1 \otimes t))e$. Isto implica que $f_i/h(S \otimes T)$ e $f_j/h(S \otimes T)$ são fortemente distintos, se $i \neq j$, como queríamos mostrar.

Sendo que T é R–separável e S é uma R–álgebra comutativa, segue que $S \otimes T$ é uma S–álgebra saparável, de I.6.5 . Então como $S \otimes T \simeq h(S \otimes T)$, temos que $h(S \otimes T)$ é S–separável. Logo, pelo lema 1.2, existem idempotentes $\omega_1, \ldots, \omega_r \in h(S \otimes T)$, dois a

dois ortogonais, tais que $f_i(x)\omega_i = x\omega_i$, para cada $x \in h(S \otimes T)$ e $\omega_j(\sigma_i) = f_i(\omega_j) = \delta_{i,j}$ $(1 \leq i \leq r)$. Mostraremos agora que $E^H = \sum_{i=1}^{r} S\omega_i$.

Como $h(S \otimes T) \subseteq E^H$, segue que $\omega_1, \ldots, \omega_r \in E^H$. Seja então $v \in E^H$. Temos $[\sum_{i=1}^{r} v(\sigma_i)\omega_i](\sigma_j) = \sum_{i=1}^{r}[v(\sigma_i)]\omega_i(\sigma_j) = \sum_{i=1}^{r} v(\sigma_i)\delta_{i,j} = v(\sigma_j)$, $1 \leq j \leq r$. Então $v = \sum_{i=1}^{r} v(\sigma_i)\omega_i$ e segue que $E^H = \sum_{i=1}^{r} S\omega_i \subseteq h(S \otimes T)$. Portanto, $E^H = h(S \otimes T)$.

Agora, $[h(S \otimes S)]^H \simeq E^H = h(S \otimes T) \subseteq h(S \otimes S^H) \subseteq E^H$. Assim, $h(S \otimes T) = h(S \otimes S^H)$, donde segue que $S \otimes T = S \otimes S^H$. Aplicando-se agora a função $tr \otimes id_S$ e o lema 1.8, que nos garante que $tr(S) = R$, temos $S^H \simeq R \otimes S^H = (tr \otimes id_S)(S \otimes S) = (tr \otimes id_S)(S \otimes T) = R \otimes T \simeq T$. Portanto, $S^H = T$ e isto completa a prova do teorema.

Os dois últimos teoremas nos dão a seguinte generalização do teorema fundamental da teoria de Galois

TEOREMA 3.4: Seja S uma extensão de Galois de R com grupo de Galois G. Então existe uma correspondência biunívoca (invertendo a ordem) entre os subgrupos de G e R–subálgebras separáveis de S [as quais são G–forte].

Se T é uma R–subálgebra separável de S [G–forte], então o subgrupo correspondente é $H_T = \{\sigma \in G : \sigma(t) = t, \forall t \in T\}$. Esta correspondência preserva a ação de G da seguinte maneira: Se $\sigma \in G$ e T é uma R– subálgebra separável [G–forte] de S, então $H_{\sigma(T)} = \sigma H_T \sigma^{-1}$. Além disso, um subgrupo H de G é normal se e somente se S^H é levado sobre si mesmo por todo elemento de G. Neste caso, S^H é uma extensão de Galois de R com grupo de Galois G/H.

Prova: A correspondência biunívoca segue facilmente dos teoremas anteriores.

Sejam $\sigma \in G$ e T uma R–subálgebra separável de S [G–forte]. Devemos mostrar que $H_{\sigma(T)} = \sigma H_T \sigma^{-1}$. Agora, sendo T R–separável, $\sigma(T)$ também o é, pois σ é um automorfismo. Logo, pelos teoremas anteriores, temos $H_{\sigma(T)} = \{\tau \in G : \tau(t) = t, \forall t \in \sigma(T)\} = \{\tau \in G : \tau\sigma(t) = \sigma(t), \forall t \in T\} = \{\tau \in G : \sigma^{-1}\tau\sigma(t) = t, \forall t \in T\} = \{\tau \in G : \sigma^{-1}\tau\sigma \in H_T\} = \sigma H_T \sigma^{-1}$.

Suponhamos que S^H é levado sobre si mesmo por todo elemento de G. Então $\sigma(S^H) = S^H$, para todo $\sigma \in G$, e segue que $H_{S^H} = H_{\sigma(S^H)} = \sigma H_{S^H} \sigma^{-1}$. Por outro lado, pela correspondência biunívoca, $H_{S^H} = H$ e logo $H = \sigma H \sigma^{-1}$, para todo $\sigma \in G$. Consequentemente H é normal em G. A recíproca foi mostrada no teorema 3.2.

§4. HOMOMORFISMOS DE EXTENSÕES DE GALOIS

Neste parágrafo discutiremos alguns resultados sobre homomorfismos de extensões de Galois. Começaremos com o seguinte

TEOREMA 4.1: Sejam S uma extensão de Galois de R com grupo de Galois G, A uma R–álgebra comutativa e $f, g : S \to A$ homomorfismos de R– álgebras. Então existe um único conjunto $\{e_\sigma : \sigma \in G\}$ de idempotentes de A, dois a dois ortogonais (alguns deles possivelmente nulos) tais que $\sum_{\sigma\in G} e_\sigma = 1$ e $g(s) = \sum_{\sigma\in G} f(\sigma(s))e_\sigma$, para cada $s \in S$.

Reciprocamente, qualquer aplicação $g : S \to A$ definida por uma tal fórmula é um homomorfismo de R– álgebras, se f o é.

Prova: Seja θ a composição das aplicações $E \xrightarrow{h^{-1}} S \otimes S \xrightarrow{f\otimes g} A \otimes A \xrightarrow{\mu} A$, onde h é o isomorfismo do teorema 1.6(e) e μ é o homomorfismo contração definido no capítulo anterior. Desta forma θ é um homomorfismo de R–álgebras. Seja agora $v_\sigma \in E$ tal que $v_\sigma(\tau) = \delta_{\sigma,\tau}$, para todo $\tau \in G$. Já vimos que o conjunto $\{v_\sigma : \sigma \in G\}$ é um conjunto de idempotentes de E, dois a dois ortogonais, cuja soma é um. Seja $e_\sigma := \theta(v_\sigma)$. Se $\sigma \neq \tau$, $e_\sigma e_\tau = \theta(v_\sigma)\theta(v_\tau) = \theta(v_\sigma v_\tau) = 0$, pois $v_\sigma v_\tau = 0$. Ainda, $e_\sigma^2 = e_\sigma e_\sigma = \theta(v_\sigma)\theta(v_\sigma) = \theta(v_\sigma^2) = \theta(v_\sigma) = e_\sigma$ e $\sum_{\sigma\in G} e_\sigma = \sum_{\sigma\in G} \theta(v_\sigma) = \theta(\sum_{\sigma\in G} v_\sigma) = \theta(1) = 1$. Portanto, $\{e_\sigma : \sigma \in G\}$ é um conjunto de idempotentes de A, dois a dois ortogonais e cuja soma é um.

Para ver a unicidade, consideremos $\{d_\sigma : \sigma \in G\}$ um conjunto de idempotentes de A, dois a dois ortogonais, cuja soma é um e tal que $g(s) = \sum_{\sigma\in G} f(\sigma(s))d_\sigma$, para todo $s \in S$. Seja $h^{-1}(v_\sigma) = \sum_i s_i \otimes t_i$, onde s_i, t_i dependem de $\sigma \in G$. Então $\sum_i s_i\tau(t_i) = \sum_i h(s_i \otimes t_i)(\tau) = v_\sigma(\tau) = \delta_{\sigma,\tau}$. Logo, $e_\sigma = \theta(v_\sigma) = [\mu \circ f \otimes g \circ h^{-1}](v_\sigma) = \mu(\sum_i f(s_i) \otimes g(t_i)) = \sum_i f(s_i)g(t_i) = \sum_i f(s_i) \sum_{\tau\in G} f(\tau(t_i))d_\tau = \sum_{\tau\in G} f(\sum_i s_i\tau(t_i))d_\tau = \sum_{\tau\in G} f(\delta_{\sigma,\tau})d_\tau = d_\sigma$.

Para obter a expressão de g observemos inicialmente que $h(1 \otimes s)(\tau) = \tau(s) = \sum_{\sigma\in G} \sigma(s)v_\sigma(\tau)$, para todo $\tau \in G$, $s \in S$. Isto é, $h(1 \otimes s) = \sum_{\sigma\in G} \sigma(s)v_\sigma$. Pondo,como antes, $h^{-1}(v_\sigma) = \sum_i s_i \otimes t_i$, e sendo $h(1 \otimes s) \in E$, aplicamos θ em ambos os lados da igualdade $h(1 \otimes s) = \sum_{\sigma\in G} \sigma(s)v_\sigma$. Obtemos então $\theta(h(1 \otimes s)) = [\mu \circ f \otimes g \circ h^{-1}](h(1 \otimes s)) =$

$[\mu \circ f \otimes g](1 \otimes s) = \mu(1 \otimes g(s)) = g(s)$ e $\theta(\sum_{\sigma \in G} \sigma(s)v_\sigma) = [\mu \circ f \otimes g \circ h^{-1}](\sum_{\sigma \in G} \sigma(s)v_\sigma) =$
$[\mu \circ f \otimes g](\sum_{\sigma \in G} \sigma(s)h^{-1}(v_\sigma)) = \sum_{\sigma \in G} \sum_i f(\sigma(s))f(s_i)g(t_i) = \sum_{\sigma \in G} f(\sigma(s))[\sum_i f(s_i)g(t_i)] =$
$\sum_{\sigma \in G} f(\sigma(s))e_\sigma$. Portanto, $g(s) = \sum_{\sigma \in G} f(\sigma(s))e_\sigma$, para cada $s \in S$.

Reciprocamente, seja $g : S \to A$ definido por $g(s) = \sum_{\sigma \in G} f(\sigma(s))e_\sigma$, onde $f : S \to A$ é um homomorfismo de R-álgebras e $\{e_\sigma\}_{\sigma \in G}$ é uma família de idempotentes dois a dois ortogonais cuja soma é um. Vamos mostrar que, nestas condições, g é também um homomorfismos de R-álgebras. De fato, g é claramente aditivo e se $s, t \in S$ então $g(s)g(t) = \left(\sum_{\sigma \in G} f(\sigma(s))e_\sigma\right)\left(\sum_{\tau \in G} f(\tau(t))e_\tau\right) = \sum_{\sigma,\tau} f(\sigma(s)\tau(t))e_\sigma e_\tau = \sum_{\sigma \in G} f(\sigma(s)\sigma(t))e_\sigma =$ $g(st)$ e ainda $g(rs) = \sum_{\sigma \in G} f(\sigma(rs))e_\sigma = r\sum_{\sigma \in G} f(\sigma(s))e_\sigma = rg(s)$, para todo $r \in R$, o que completa a prova.

COROLÁRIO 4.2: Com as mesmas hipóteses e notações do teorema anterior, se A não possui idempotentes próprios, então existe um único elemento $\sigma \in G$ tal que $g = f\sigma$.

Prova: O conjunto $\{e_\sigma : \sigma \in G\}$ de idempotentes de A definido no teorema anterior, possui todos os elementos nulos, com excessão de um deles, a saber, $e_\sigma = 1$, para algum $\sigma \in G$. Logo, para todo $s \in S$, temos $g(s) = f(\sigma(s))$, isto é, $g = f\sigma$.

No seguinte corolário, $j : \Delta \to Hom_R(S, S)$ é o isomorfismo do teorema 1.6(c).

COROLÁRIO 4.3: Seja S uma extensão de Galois de R com grupo de Galois G e W o semi-grupo multiplicativo do anel dos endomorfismos de anéis de S formado pelos endomorfismos que deixam R fixo. Então $W \subseteq Hom_R(S, S)$ e $j^{-1}(W)$ consiste de todos os elementos de Δ da forma $\sum_{\sigma \in G} e_\sigma u_\sigma$, com $\{e_\sigma\}_{\sigma \in G}$ uma família de idempotentes dois a dois ortogonais de S, cuja soma é 1.

Além disso, se todo idempotente de S está em R, então todo elemento de W é um automorfismo. Assim o grupo dos R-automorfismos de S é isomorfo, via j^{-1}, ao subgrupo multiplicativo de anel de grupo $R(G) \subseteq \Delta$, constituido dos elementos $\sum_{\sigma \in G} e_\sigma \sigma$, como acima. Finalmente, S não possui idempotentes próprios se e somente se $W = G$, isto é, se e somente se G é o conjunto de todos os R-endomorfismos de S.

Prova: Seja W o conjunto de todos os endomorfismos de S que deixam R fixo. Claramente $W \subseteq Hom_R(S, S)$ e W é um semi-grupo multiplicativo. Fazendo, no

teorema 4.1, $A = S$ e $f = id_S$ obtemos $g(s) = \sum_{\sigma \in G} \sigma(s)e_\sigma$, para cada $g \in W$, $s \in S$. Considerando agora o isomorfismo $j : \Delta \to Hom_R(S, S)$ definido em 1.6(c), temos $j^{-1}(g) = j^{-1}(\sum_{\sigma \in G} e_\sigma \sigma) = \sum_{\sigma \in G} e_\sigma u_\sigma$, para todo $g \in W$. Reciprocamente, também do teorema 4.1 segue que $j(\sum_{\sigma \in G} e_\sigma u_\sigma) \in W$, o que prova a primeira parte.

Para obtermos a segunda parte, suponhamos que $S \setminus R$ não contenha nenhum idempotente. Claramente, $\left(\sum_{\sigma \in G} e_\sigma u_\sigma\right)\left(\sum_{\tau \in G} e_\tau u_{\tau^{-1}}\right) = \sum_{\sigma,\tau \in G} e_\sigma \sigma(e_\tau) u_{\sigma\tau^{-1}} = \sum_{\sigma \in G} e_\sigma^2 u_{id} = \sum_{\sigma \in G} e_\sigma = 1$ pois $\sigma(e_\tau) = e_\tau$, para todo $\tau \in G$ $(e_\tau \in R)$. Então, $id = j(\sum_{\sigma \in G} e_\sigma u_\sigma \sum_{\tau \in G} e_\tau u_{\tau^{-1}}) = j(\sum_{\sigma \in G} e_\sigma u_\sigma) j(\sum_{\tau \in G} e_\tau u_{\tau^{-1}})$ e isto implica que $j(\sum_{\sigma \in G} e_\sigma u_\sigma) = \left[j(\sum_{\tau \in G} e_\tau u_{\tau^{-1}})\right]^{-1}$. Consequentemente, os elementos de W são automorfismos e W é isomorfo a um subgrupo de $R(G) \subseteq \Delta$, via j^{-1} (aqui temos $R(G) \subseteq \Delta$, via a aplicação $\sigma \mapsto u_\sigma$).

Suponhamos agora que S não possua nenhum idempotente próprio. Então, pelo corolário 4.2, segue que para todo $g \in W$ existe um único $\sigma \in G$ tal que $g = \sigma$, isto é, $W = G$. Reciprocamente, se $W = G$ e $e \in S$ é um idempotente tal que $e \neq 0$ e $e \neq 1$, então tomando $\sigma, \tau \in G$, $\sigma \neq \tau$, temos $j(eu_\sigma + (1-e)u_\tau) \in W$. Agora, sendo que $W = G$, temos que o homomorfismo $g = j(eu_\sigma + (1-e)u_\tau)$, verifica $g = \rho \in G$, para algum $\rho \in G$. Isto é uma contradição, pois se $e\sigma + (1-e)\tau = \rho$, então $e\rho(s) = e(e\sigma + (1-e)\tau)(s) = e\sigma(s)$, de onde segue que $\rho = \sigma$ já que os elementos de G são fortemente distintos. Analogamente, de $(1-e)\rho(s) = (1-e)\tau(s)$ segue que $\rho = \tau$. Isto não pode acontecer, pois $\sigma \neq \tau$. Assim, a prova está completa.

TEOREMA 4.4: Sejam S e S' duas extensões de Galois de R com mesmo grupo de Galois G, e seja $f : S \to S'$ um homomorfismo de R-álgebras e G-módulos. Então f é um isomorfismo.

Prova: Consideremos $x_1, \ldots, x_n; y_1, \ldots, y_n \in S$ satisfazendo o ítem (b) do teorema 1.6 e seja $tr = \sum_{\sigma \in G} \sigma$ a função traço. Mostraremos que f é um isomorfismo, mostrando que f é injetora e sobrejetora.

Seja $s \in S$ tal que $f(s) = 0$. Sendo que f é um G-homomorfismo temos $f(\sigma(sy_i)) = f(\sigma(s)\sigma(y_i)) = f(\sigma(s))f(\sigma(y_i)) = \sigma(f(s))\sigma(f(y_i)) = 0$, para cada $\sigma \in G$ e $1 \leq i \leq n$. Assim, $f(tr(sy_i)) = 0$ e como $tr(sy_i) \in R$, resulta que $tr(sy_i) = 0$, $1 \leq i \leq n$. Então, $0 = \sum_{i=1}^{n} x_i tr(sy_i) = \sum_{i=1}^{n} \sum_{\sigma \in G} x_i \sigma(s)\sigma(y_i) = \sum_{\sigma \in G} \sigma(s) \sum_{i=1}^{n} x_i \sigma(y_i) = \sum_{\sigma \in G} \sigma(s)\delta_{1,\sigma} = s$.

Consequentemente f é injetora.

Seja agora $s' \in S'$. Como f é um G-homomorfismo, temos $f(\sum_{i=1}^{n} x_i tr(f(y_i)s')) = \sum_{i=1}^{n}(f(x_i)\sum_{\sigma\in G}\sigma(f(y_i))\sigma(s')) = \sum_{\sigma\in G}(f(\sum_{i=1}^{n} x_i\sigma(y_i))\sigma(s') = \sum_{\sigma\in G} f(\delta_{1,\sigma})\sigma(s') = id(s') = s'$. Logo, f é sobrejetora e portanto a prova está completa.

TEOREMA 4.5: Seja S um anel comutativo sem idempotentes próprios, G um subgrupo arbitrário do grupo de automorfismos de S e $R = S^G$. Suponhamos que S é uma R-álgebra separável e finitamente gerada como R-módulo. Então G é finito, S é uma extensão de Galois de R com grupo de Galois G e G é o grupo de todos os R-automorfismos de S.

Prova: É claro que $S \otimes S$ é uma S-álgebra via o primeiro fator. Ainda, se $s_1, \ldots, s_r$ são elementos que geram S como R-módulo, então é facil ver que $1 \otimes s_1, \ldots, 1 \otimes s_r$ são geradores de $S \otimes S$ como S-módulo.

Sejam $\sigma_1, \ldots, \sigma_n$ elementos distintos de G. É fácil ver que as aplicações $f_i : S \otimes S \to S$ definidas por $f_i = \mu \circ (1 \otimes \sigma_i)$, $1 \leq i \leq n$, onde μ é o homomorfismo contração, são homomorfismos de S-álgebras.

Como $S \otimes S$ é S-separável e $f_1, \ldots, f_n$ são fortemente distintos segue do lema 1.2 que existem idempotentes $e_1, \ldots, e_n \in S$, dois a dois ortogonais tais que $f_i(e_i) = 1$ e $f_i(x)e_i = xe_i$, para cada $x \in S \otimes S$. Assim, $f_i/(S \otimes S)e_i : (S \otimes S)e_i \to S$ é um isomorfismo de S-módulos, para $1 \leq i \leq n$. De fato, vejamos que $f_i/(S \otimes S)e_i$ é uma bijeção, para qualquer tal i. Dado $x \in S \otimes S$, tal que $f_i(xe_i) = 0$, segue que $0 = f_i(xe_i) = f_i(x)f_i(e_i) = f_i(x)$. Logo, $xe_i = f_i(x)e_i = 0$ o que prova que f_i é injetora. Cosideremos agora $s \in S$. Existe $s' \in S$ tal que $\sigma_i(s') = s$. Assim, $f_i((1 \otimes s')e_i) = f_i(1 \otimes s')f_i(e_i) = f_i(1 \otimes s') = \sigma_i(s') = s$. Logo, $f_i/(S \otimes S)e_i$ é também sobrejetora.

Definindo agora $e = 1 \otimes 1 - e_1 - \cdots - e_n$, temos que e é um idempotente ortogonal a cada e_i, como é fácil ver. Deste modo, $S \otimes S = \bigoplus_{i=1}^{n}(S \otimes S)e_i \oplus (S \otimes S)e$, como S-módulo. Assim, $S \otimes S$ possui um S-somando direto livre de posto n, a saber, $\bigoplus_{i=1}^{n}(S \otimes S)e_i \simeq S^n$ (via $\bigoplus_{i=1}^{n} f_i/(S \otimes S)e_i$).

Seja $\mathcal{M}$ um ideal maximal de S. Então $S/\mathcal{M}$ é um corpo e $\mathcal{M}(S \otimes S)$ é um ideal de $S \otimes S$. Portanto, $S \otimes S/\mathcal{M}(S \otimes S)$ é um espaço vetorial sobre $S/\mathcal{M}$ de maneira natural. Como $S \otimes S$ possui um somando direto de posto n sobre S, segue

que $dim_{S/\mathcal{M}}[S \otimes S/\mathcal{M}(S \otimes S)] \geq n$.

Por outro lado, como $1 \otimes s_i$, $1 \leq i \leq r$ geram $S \otimes S$ como S-módulo, $\overline{1 \otimes s_i}$, $1 \leq i \leq r$, geram $S \otimes S/\mathcal{M}(S \otimes S)$ como $S/\mathcal{M}$- espaço vetorial. Conseqüentemente temos $dim_{S/\mathcal{M}}[S \otimes S/\mathcal{M}(S \otimes S)] \leq r$. Logo, $l(G) = n \leq r$, isto é, G é finito.

Como S é R-separável e $S^G = R$ segue do teorema 1.6 que S é uma extensão de Galois de R com grupo de Galois G. Ainda, do fato que S não possui idempotentes próprios segue, pelo corolário 4.3, que G é o grupo de todos os R-automorfismos de S. Isto completa a prova do teorema.

§.5 - O GRUPO DE HARRISON

Neste parágrafo suporemos sempre que G é um grupo abeliano e R é um anel comutativo.

Duas extensões de Galois S e T de R com mesmo grupo de Galois G são ditas isomorfas, se existir um isomorfismo de R-álgebras $\varphi : S \to T$ que comuta com a ação de G, isto é, o seguinte diagrama é comutativo, para todo $\sigma \in G$:

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & T \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ S & \xrightarrow{\varphi} & T \end{array}$$

Consideremos agora a classe $\mathcal{G}_R$ de todas as extensões de Galois de R com grupo de Galois G. Podemos definir uma relação de equivalência em $\mathcal{G}_R$ de maneira natural, como segue: Dados $S, T \in \mathcal{G}_R$, dizemos que S e T são equivalentes se e somente se S e T são isomorfos como extensões de Galois de R. Notaremos por $[S]$ a classe de equivalência de S e $T(G,R)$ denotará o conjunto de todas estas classes de equivalência. Assim, $T(G,R) = \{[S] : S$ é uma extensão de Galois de R com grupo de Galois $G\}$.

Decorre do exemplo 2.4 do parágrafo 2, que se S e T são duas extensões de Galois de R com mesmo grupo G, então $S \otimes T$ é também uma extensão de Galois de R com grupo $G \times G$. Agora $\Delta(G) = \{ (\sigma^{-1}, \sigma) : \sigma \in G \} \subseteq G \times G$ é um subgrupo de $G \times G$. De fato, $(id, id) \in \Delta(G)$ e para (σ^{-1}, σ), $(\tau^{-1}, \tau) \in \Delta(G)$, temos $(\sigma^{-1}, \sigma) \circ (\tau^{-1}, \tau) = (\sigma^{-1}\tau^{-1}, \sigma\tau) = ((\sigma\tau)^{-1}, \sigma\tau)$, já que G é abeliano. Portanto, $\Delta(G)$ é um subgrupo normal de $G \times G$, e podemos então considerar o grupo quociente $G \times G/\Delta(G)$. Temos então a seguinte

PROPOSIÇÃO 5.1: Com as mesmas notações acima, $G \times G/\Delta(G) \simeq G$.

Prova: Seja $\varphi : G \times G \longrightarrow G$, dado por $\varphi(\sigma, \tau) = \sigma\tau$. É fácil ver que φ é um homomorfismo sobrejetor. Agora, $ker\varphi = \{ (\sigma, \tau) \in G \times G : \sigma\tau = id \} = \{ (\sigma^{-1}, \sigma) : \sigma \in G \times G \} = \Delta(G)$. Portanto, $G \times G/\Delta(G) \simeq G$, como queríamos mostrar.

Segue do teorema fundamental que $(S \otimes T)^{\Delta(G)}$ é uma extensão de Galois de R com grupo de Galois G, onde G atua sobre $S \otimes T$ via $\sigma \otimes id$, para $\sigma \in G$.

Vamos definir agora uma operação em $T(G, R)$ como segue: Dados $[S], [T] \in T(G, R)$ definimos $[S] * [T] = [((S \otimes T)^{\Delta(G)}, \{\sigma \otimes id : \sigma \in G \})]$. É fácil ver que se $[S] = [S']$ e $[T] = [T']$, então $[S] * [T] = [S'] * [T']$. Logo, $*$ está bem definida. Estamos agora em condições de apresentar o seguinte

TEOREMA 5.2: Com as mesmas notações anteriores, $T(G, R)$ é um grupo abeliano.

Provaremos este teorema somente para o caso em que G é um grupo cíclico, pois este é o caso que interessa em nosso trabalho. O leitor interessado poderá encontrar uma prova para o caso geral em [12].

Suporemos então $G = \mathbb{Z}/n\mathbb{Z}$ e mostraremos que $(T(\mathbb{Z}/n\mathbb{Z}, R), *)$ é um grupo abeliano.

Prova do teorema 5.2: É claro que a associatividade e a comutatividade de $*$ decorrem da associatividade e comutatividade do produto tensorial, respectivamente. Então falta mostrar que $*$ possui um elemento neutro e que todo elemento de $T(\mathbb{Z}/n\mathbb{Z}, R)$ possui um simétrico com relação à $*$.

Usaremos a notação (S, σ) para indicar que S é uma extensão de Galois de R com grupo cíclico gerado por σ, e $[S, \sigma]$ para indicar sua respectiva classe em $T_n(\mathbb{Z}/n\mathbb{Z}, R)$.

Consideremos $\mathbb{E} = \bigoplus_{i=1}^{n} Re_i$, onde $\{e_i\}_{1 \leq i \leq n}$ é uma família de idempotentes ortogonais cuja soma é 1. Vimos no exemplo 2.1 do parágrafo 2 que $(\mathbb{E}, \tau)$ é uma extensão de Galois de R com grupo cíclico de ordem n gerado por τ, onde τ é o automorfismo de $\mathbb{E}$ que atua da forma $\tau(e_i) = e_{i+1 \pmod n}$ $(1 \leq i \leq n)$. Mostraremos que $[\mathbb{E}, \tau]$, assim definida, é o elemento neutro de $*$.

Seja $[S, \sigma] \in T(\mathbb{Z}/n\mathbb{Z}, R)$. Temos $[S, \sigma] * [\mathbb{E}, \tau] = [(S \otimes \mathbb{E})^{\sigma^{-1} \otimes \tau}, \sigma \otimes 1]$, sendo que $\Delta(G) = (\sigma^{-1} \otimes \tau)$ neste caso. Devemos mostrar então que $[(S \otimes \mathbb{E})^{\sigma^{-1} \otimes \tau}, \sigma \otimes 1] = [S, \sigma]$. Para tanto observemos que se $\alpha \in S \otimes \mathbb{E} = S \otimes (\oplus_{i=1}^{n} Re_i)$, então existem elementos $s_i \in S$, $i = 1, \ldots, n$, tais que $\alpha = \sum_{i=1}^{n} s_i \otimes e_i$ e esta representação é única,

sendo que $(1 \oslash e_i)_{1 \leq i \leq n}$ é uma base de $S \otimes I\!E$ sobre S. Assim, $(\sigma^{-1} \oslash \tau)(\alpha) = (\sigma^{-1} \otimes \tau)(\sum_{i=1}^{n} s_i \otimes e_i) = \sum_{i=1}^{n} \sigma^{-1}(s_i) \otimes e_{i+1 \pmod n}$. Então temos $\alpha \in (S \otimes I\!E)^{\sigma^{-1} \otimes \tau}$ se e somente se $\sigma^{-1}(s_1) = s_2$, $\sigma^{-1}(s_2) = s_3$, ..., $\sigma^{-1}(s_{n-1}) = s_n$, $\sigma^{-1}(s_n) = s_1$. Logo, $(S \otimes I\!E)^{\sigma^{-1} \otimes \tau} = (S \otimes \bigoplus_{i=1}^{n} Re_i)^{\sigma^{-1} \otimes \tau} = \{\sum_{i=1}^{n} \sigma^{1-i}(s) \oslash e_i \ : \ s \in S\}$.

Definimos então $\varphi : S \longrightarrow (S \otimes I\!E)^{\sigma^{-1} \otimes \tau}$, por $\varphi(s) = \sum_{i=1}^{n} \sigma^{1-i}(s) \oslash e_i$. Assim, φ está bem definida e é sobrejetora. Como $ker\varphi = \{s \in S \ : \ \sum_{i=1}^{n} \sigma^{1-i}(s) \oslash e_i = 0\} = \{0\}$, segue que φ é também injetora. Mostraremos que φ é um isomorfismo de anéis. De fato, é claro que $\varphi(1) = 1$ e para todos $s, t \in S$, temos $\varphi(s+t) = \sum_{i=1}^{n} \sigma^{1-i}(s+t) \oslash e_i = \sum_{i=1}^{n} (\sigma^{1-i}(s) + \sigma^{1-i}(t)) \oslash e_i = (\sum_{i=1}^{n} \sigma^{1-i}(s) \otimes e_i) + (\sum_{i=1}^{n} \sigma^{1-i}(t) \otimes e_i) = \varphi(s) + \varphi(t)$ e $\varphi(st) = \sum_{i=1}^{n} \sigma^{1-i}(st) \otimes e_i = \sum_{i=1}^{n} \sigma^{1-i}(s)\sigma^{1-i}(t) \oslash e_i = (\sum_{i=1}^{n} \sigma^{1-i}(s) \otimes e_i)(\sum_{i=1}^{n} \sigma^{1-i}(t) \oslash e_i) = \varphi(s)\varphi(t)$, pois $\{e_i\}_{1 \leq i \leq n}$ é uma família de idempotentes ortogonais.

O seguinte diagrama

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & (S \otimes I\!E)^{\sigma^{-1} \otimes \tau} \\ \sigma \downarrow & & \downarrow \sigma \oslash 1 \\ S & \xrightarrow{\varphi} & (S \otimes I\!E)^{\sigma^{-1} \otimes \tau} \end{array}$$

é claramente comutativo. Resulta então que φ é um isomorfismo de extensões de Galois. Isto é, $[(S \otimes I\!E)^{\sigma^{-1} \otimes \tau}, \sigma \otimes 1] = [S, \sigma]$, para todo $[S, \sigma] \in T(\mathbb{Z}/n\mathbb{Z}, R)$.

Para mostrarmos que todo elemento de $T(\mathbb{Z}/n\mathbb{Z})$ possui um simétrico com relação à $*$, mostraremos primeitro que, para todo $[S, \sigma] \in T(\mathbb{Z}/n\mathbb{Z}, R)$, temos $[S, \sigma]^k = [S, \sigma^{k^{-1} \pmod n}]$, se $(k, n) = 1$.

Dado $[S, \sigma] \in T(\mathbb{Z}/n\mathbb{Z}, R)$ seja $[T, \sigma] = [S, \sigma]^k$. Por indução em k, segue que $[T, \sigma] = [S, \sigma]^k = [(S^{\otimes k})^{(\sigma^{-1} \otimes 1 \otimes \cdots \otimes 1) \otimes \sigma}, \sigma \otimes 1 \otimes \cdots \otimes 1]$, onde $S^{\otimes k} = S \otimes \cdots \otimes S$ (k vezes), $\sigma^{-1} \otimes 1 \otimes \cdots \otimes 1$ possui $k-1$ fatores e $\sigma \oslash 1 \oslash \cdots \otimes 1$, k fatores. Assim, T é um subanel de $S^{\otimes k}$ e σ atua em T, via $\sigma \otimes 1 \otimes \cdots \otimes 1$. Mostraremos agora que σ^k atua em T da forma $\sigma \otimes \sigma \otimes \cdots \otimes \sigma$ (k fatores).

Como $((\sigma^{-1} \oslash 1 \oslash \cdots \oslash 1) \otimes \sigma)(\alpha) = \alpha$, para todo $\alpha \in T$, segue que $(\sigma \otimes 1 \otimes \cdots \otimes 1) \circ ((\sigma^{-1} \oslash 1 \otimes \cdots \otimes 1) \otimes \sigma)(\alpha) = (\sigma \oslash 1 \otimes \cdots \otimes 1)(\alpha)$, ou seja, $(1 \oslash 1 \otimes \cdots \otimes \sigma)(\alpha) = (\sigma \otimes 1 \otimes \cdots \otimes 1)(\alpha)$, para todo $\alpha \in T$. Da mesma forma, $[S, \sigma]^k = [S, \sigma]^{k-2} * [S, \sigma]^2 = [(S^{\otimes k-2} \otimes S^{\otimes 2})^{(\sigma^{-1} \otimes 1 \otimes \cdots \otimes 1) \otimes (\sigma \otimes 1)}, \sigma \otimes 1 \otimes \cdots \otimes 1]$ (onde $\sigma^{-1} \otimes 1 \otimes \cdots \otimes 1$ possui $k-2$ fatores e $\sigma \oslash 1 \oslash \cdots \oslash 1$, k fatores) e também como $((\sigma^{-1} \otimes 1 \otimes \cdots \otimes 1) \otimes (\sigma \oslash 1))(\alpha) = \alpha$,

para todo $\alpha \in T$, segue que $(\sigma \otimes 1 \otimes \cdots \otimes 1)(\alpha) = (\sigma \otimes 1 \otimes \cdots \otimes 1) \circ ((\sigma^{-1} \otimes 1 \otimes \cdots \otimes 1) \otimes (\sigma \otimes 1))(\alpha) = (1 \otimes 1 \otimes \cdots \otimes \sigma \otimes 1)(\alpha)$. Repetindo este argumento obtemos $(\sigma \otimes 1 \otimes \cdots \otimes 1)(\alpha) = (1 \otimes \sigma \otimes \cdots \otimes 1)(\alpha) = \ldots = (1 \otimes 1 \otimes \cdots \otimes \sigma)(\alpha)$, para todo $\alpha \in T$. Logo, $\sigma^k(\alpha) = (\sigma \otimes 1 \otimes \cdots \otimes 1)^k(\alpha) = [(\sigma \otimes 1 \otimes \cdots \otimes 1) \circ \cdots \circ (1 \otimes 1 \otimes \cdots \otimes \sigma)](\alpha) = (\sigma \otimes \sigma \otimes \cdots \otimes \sigma)(\alpha)$, para todo $\alpha \in T$. Portanto, σ^k age sobre T via $\sigma \otimes \sigma \otimes \cdots \otimes \sigma$, como queríamos mostrar.

Consideremos agora a restrição do homomorfismo contração $\mu : T \longrightarrow S$. Temos assim o seguinte diagrama:

$$\begin{array}{ccc} T & \xrightarrow{\mu} & S \\ {\scriptstyle \sigma^k}\downarrow & & \downarrow{\scriptstyle \sigma} \\ T & \xrightarrow{\mu} & S \end{array}$$

o qual é comutativo. Logo, $\mu : (T, \sigma^k) \longrightarrow (S, \sigma)$ é um isomorfismo de extensões de Galois, pelo teorema 4.4.

Se $(k, n) = 1$, podemos considerar o inteiro $k^{-1} \pmod n$ e o argumento acima (aplicado à $(S, \sigma^{k^{-1} \pmod n})$ mostra que $\mu' : (T, \sigma) \longrightarrow (S, \sigma^{k^{-1} \pmod n})$ é um isomorfismo de extensões de Galois. Portanto, $[S, \sigma]^k = [T, \sigma] = [S, \sigma^{k^{-1} \pmod n}]$.

Assim, $[S, \sigma]^n = [S, \sigma]^{n-1} * [S, \sigma] = [S, \sigma^{-1}] * [S, \sigma] = [(S \otimes S)^{\sigma \otimes \sigma}, \sigma^{-1} \otimes 1]$, pois $n - 1 \equiv -1 \pmod n$. Vamos mostrar agora que $[(S \otimes S^{\sigma \otimes \sigma}, \sigma^{-1} \otimes 1]$ é o elemento neutro de $T(\mathbb{Z}/n\mathbb{Z}, R)$, obtendo que o inverso de $[S, \sigma]$ existe em $T(\mathbb{Z}/n\mathbb{Z}, R)$. Mais ainda, $[S, \sigma]^{-1} = [S, \sigma]^{n-1}$, para todo $[S, \sigma] \in T(\mathbb{Z}/n\mathbb{Z}, R)$.

Consideremos o isomorfismo $h : S \otimes S \longrightarrow E = \bigoplus_{i=0}^{n-1} Se_i$, do teorema 1.6(e), onde e_i denota v_{σ^i} $(0 \leq i \leq n-1)$. Dado $v \in E$, temos $v = \sum_{i=0}^{n-1} s_i e_i$. Como $v(\sigma^j) = \sum_{i=0}^{n-1} s_i e_i(\sigma^j) = \sum_{i=0}^{n-1} s_i \delta_{i,j} = s_j$, para todo $0 \leq i \leq n-1$, segue que $v = \sum_{i=0}^{n-1} v(\sigma^i) e_i$. Assim, dado $s \otimes t \in S \otimes S$, temos $h(s \otimes t) = \sum_{i=0}^{n-1} s_i e_i$, onde $s_j = h(s \otimes t)(\sigma^j) = s\sigma^j(t)$, para todo $0 \leq j \leq n-1$, isto é, $h(s \otimes t) = \sum_{i=0}^{n-1} s\sigma^i(t) e_i$. Tomando agora $\sigma(s) \otimes \sigma(t) \in S \otimes S$, temos $h(\sigma(s) \otimes \sigma(t)) = \sum_{i=0}^{n-1} \sigma(s)\sigma^{i+1}(t) e_i = \sum_{i=0}^{n-1} \sigma(s\sigma^i(t)) e_i$. Portanto, se $s \otimes t \in (S \otimes S)^{\sigma \otimes \sigma}$, então $\sum_{i=0}^{n-1} s_i e_i = h(s \otimes t) = h(\sigma(s) \otimes \sigma(t))$, ou seja, $\sum_{i=0}^{n-1} s\sigma^i(t) e_i = \sum_{i=0}^{n-1} \sigma(s\sigma^i(t)) e_i$, de onde resulta $\sigma(s_i) = \sigma(s\sigma^i(t)) = s\sigma^i(t) = s_i$, para todo $0 \leq i \leq n-1$ e portanto, $s_i \in R$, $0 \leq$

$i \leq n-1$. Assim, $h((S \otimes S)^{\sigma \otimes \sigma}) \subseteq \mathbb{E} = \bigoplus_{i=1}^{n} Re_i$. Claramente, $\mathbb{E} \subseteq h((S \otimes S)^{\sigma \otimes \sigma})$. Consequentemente, $h/(S \otimes S)^{\sigma \otimes \sigma} : (S \otimes S)^{\sigma \otimes \sigma} \longrightarrow \mathbb{E} = \bigoplus_{i=1}^{n} Re_i$ é um isomorfismo de R– álgebras. Notemos por h' tal isomorfismo.

Do exemplo 2.1 e da prova do teorema 3.3 segue que $E \simeq S \otimes S$ é uma extensão de Galois de R com grupo de Galois $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, gerado por $(\sigma, id) = h \circ (\sigma \otimes id) \circ h^{-1}$ e por $(id, \sigma) = h \circ (id \otimes \sigma) \circ h^{-1}$.

Seja $\alpha = \sum_i a_i \otimes b_i \in (S \otimes S)^{\sigma \otimes \sigma}$. Então $h(\alpha) = \sum_{i=0}^{n-1} r_i e_i$, onde $r_i \in R$, $0 \leq i \leq n-1$ e $r_j = \sum_{i=0}^{n-1} r_i e_i(\sigma^j) = h(\alpha)(\sigma^j) = \sum_{i=0}^{n-1} a_i \sigma^j(b_i)$. Agora, $(\sigma^{-1}, id)(\sum_{i=0}^{n-1} r_i e_i) = h \circ (\sigma^{-1} \otimes id) \circ h^{-1}(\sum_{i=0}^{n-1} r_i e_i) = h\left(\sum_{i=0}^{n-1} \sigma^{-1}(a_i) \otimes b_i\right) = \sum_{i=0}^{n-1} u_i e_i$, onde $u_j = \sum_{i=0}^{n-1} \sigma^{-1}(a_i)\sigma^j(b_i) = \sigma^{-1}(\sum_{i=0}^{n-1} a_i \sigma^{j-1}(b_i)) = \sigma^{-1}(r_{j-1 \pmod n})$. Ou seja, $(\sigma^{-1}, id) = \tau$, onde τ é o automorfismo de $\mathbb{E}$ dado por $\tau(e_i) = e_{i+1 \pmod n}$. Portanto o seguinte diagrama

$$\begin{array}{ccc} (S \otimes S)^{\sigma \otimes \sigma} & \xrightarrow{h'} & \mathbb{E} \\ \sigma^{-1} \otimes id \downarrow & & \downarrow (\sigma^{-1}, id) = \tau \\ (S \otimes S)^{\sigma \otimes \sigma} & \xrightarrow{h'} & \mathbb{E} \end{array}$$

é evidentemente comutativo e $[(S \otimes S)^{\sigma \otimes \sigma}, \sigma^{-1} \otimes id] = [\mathbb{E}, \tau]$. Isto completa a prova para o caso cíclico.

NOTA: A prova do teorema acima mostra que todo elemento de $T(\mathbb{Z}/n\mathbb{Z}, R)$ é um elemento de ordem n. De fato, para todo $[S, \sigma] \in T(\mathbb{Z}/n\mathbb{Z}, R)$, $[S, \sigma]^n$ é a identidade do grupo $T(\mathbb{Z}/n\mathbb{Z}, R)$.

CAPÍTULO III : EXTENSÕES DE GALOIS DE ANÉIS DE CARACTERÍSTICA p.

Neste capítulo suporemos sempre R um anel comutativo de característica p, onde p é um número primo, isto é, para todo $r \in R$ temos $pr = 0$. Neste caso, R contém $\mathbb{Z}/p\mathbb{Z}$ como subanel.

Dado uma extensão A de R, dizemos que A é uma extensão p^n–cíclica de R, se A é uma extensão de Galois de R com grupo de Galois cíclico de ordem p^n. As extensões p^n–cíclicas de R serão notadas por (A, σ), onde σ é um gerador do grupo de Galois da extensão A de R. Ainda, notaremos por $[A, \sigma]$ a classe de (A, σ) no grupo de Harrison $T(\mathbb{Z}/p^n\mathbb{Z}, R)$.

Começaremos estudando as extensões p–cíclicas de R, segundo o trabalho de T. Nagahara e A. Nakajima [15]. Após, obteremos uma generalização deste caso, apresentando resultados obtidos por M. Ferrero, A. Paques e A. Solecki. Observemos que alguns resultados foram obtidos previamente por T. Wyller, em [21] e C. Greither, em [9] (corolário 2.4 e teorema 3.2), mas estes autores usaram métodos cohomológicos. Seguiremos aqui os métodos diretos de M. Ferrero, A. Paques e A. Solecki ([7] e [8]).

§1. EXTENSÕES p-CÍCLICAS

Do exemplo I.2.2, temos o seguinte:

TEOREMA 1.1 : Seja $f(X) = X^p - X - r \in R[X]$. Então $(R[X]/(f(X)), \sigma)$ é uma extensão p–cíclica de R, onde $\sigma : \frac{R[X]}{(f(X))} \to \frac{R[X]}{(f(X))}$ é o R–automorfismo dado por $\sigma(X + (f(X)) = X + 1 + (f(X))$.

Mostraremos a recíproca deste teorema. Antes porém, provaremos o seguinte :

LEMA 1.2 : Seja A uma extensão de R e σ um R–automorfismo de A. Se existir $a \in A$ tal que $a^p - a \in R$ e $\sigma(a) = a + 1$, então existe um R–isomorfismo φ tal que o diagrama abaixo comuta:

$$\begin{array}{ccc} \frac{R[X]}{(f(X))} & \xrightarrow{\varphi} & R[a] \\ \psi \downarrow & & \downarrow \sigma/R[a] \\ \frac{R[X]}{(f(X))} & \xrightarrow{\varphi} & R[a] \end{array}$$

onde $f(X) = X^p - X - (a^p - a)$ e ψ é o R– isomorfismo definido acima por $\psi(x) = x+1$, para $x = X + (f(X))$. Em particular, $R[a]$ é uma extensão p– cíclica de R com grupo de Galois $(\sigma/R[a])$.

Prova: Consideremos $\varphi' : R[X] \to R[a]$, definido por $\varphi'(g(X)) = g(a)$, para todo $g(X) \in R[X]$. Assim, φ' é um homomorfismo sobrejetor. Como $f(X) = X^p - X - (a^p - a)$, segue que $f(a) = 0$, e consequentemente, $(f(X)) \subseteq ker\varphi'$.

Consideremos agora $h(X) = \sum_{i=0}^{m} r_i X^i \in R[X]$, tal que $h(a) = 0$. Então, $0 = \sigma(h(a))$ $= \sigma(\sum_{i=0}^{m} r_i a^i) = \sum_{i=0}^{m} r_i \sigma(a)^i = \sum_{i=0}^{m} r_i (a+1)^i = h(a+1)$. Repetindo este argumento, segue que $\sigma^i(a) = a + i$, $0 \leq i \leq p-1$ são raízes de $h(X)$. Agora, como $f(a) = 0$, segue pelo algorítmo da divisão, que $f(X) = (X - a)q(X)$, com $q(X) \in R[X]$, onde o grau de $q(X)$ é $p-1$. Ainda, como $f(a+1) = 0$, temos $q(X) = (X - (a+1))q'(X)$, com $q'(X) \in R[X]$, onde o grau de q' é $p-2$. Continuando este raciocínio, e pelo fato de $f(X)$ ser um polinômio mônico, segue que $f(X) = (X - a)(X - (a+1)) \ldots (X - (a+p-1))$. Logo, dado $g(X) \in ker\varphi'$, temos $g(a) = 0$ e consequentemente, pelos argumentos anteriores, $g(X) = (X - a) \ldots (X - (a+p-1))h(X) = f(X)h(X)$, com $h(X) \in R[X]$, ou seja, $ker\varphi' \subseteq (f(X))$. Portanto, $ker\varphi' = (f(X))$ e então existe um R– isomorfismo $\varphi : R[X]/(f(X)) \to R[a]$, induzido por φ'.

Consideremos agora $g(X)+(f(X)) \in R[X]/(f(X))$. Temos, $(\varphi \circ \psi)(g(X)+(f(X))) = \varphi(g(X+1) + (f(X))) = g(a+1)$ e $(\sigma \circ \varphi)(g(X) + (f(X))) = \sigma(g(a)) = g(a+1)$. Logo, $\varphi \circ \psi = \sigma/R[a] \circ \varphi$ e o diagrama comuta. Isto completa a prova do lema.

O seguinte teorema é uma recíproca do teorema 1.1:

TEOREMA 1.3: Seja A uma extensão p– cíclica de R com grupo de Galois (σ). Então existe $a \in A$ tal que $\sigma(a) = a + 1$. Neste caso, $a^p - a \in R$ e $R[a] = A$. Além disso, existe um isomorfismo de extensões de Galois $(R[X]/(f(X)), \psi) \simeq (A, \sigma)$, onde $f(X) = X^p - X - (a^p - a)$ e ψ é tal que $\psi(X + (f(X))) = X + 1(f(X))$.

Prova: Como A é uma extensão de Galois de R, existe um elemento $c \in A$ tal que $tr_{(\sigma)}(c) = 1$. Temos ainda $(\sigma) = \{id, \sigma, \sigma^2, \ldots, \sigma^{p-1}\} = \{\sigma, \sigma^2, \ldots, \sigma^p\}$. Consideremos então os elementos $x_i = 1 + 1 + \cdots + 1$ (i somandos), $1 \leq i \leq p$. Assim, $x_i \in R \subset A$, para $i = 1, 2, \ldots, p$ e $x_p = 0$, pois R é um anel de característica p. Claramente, temos $\sigma(x_i) = x_i$ e $x_i = x_{i+1} - x_1$, para $1 \leq i \leq p$.

Definimos então $a = -\sum_{i=1}^{p} x_i \sigma^i(c)$. Assim resulta $\sigma(a) = \sigma\left(-\sum_{i=1}^{p} x_i \sigma^i(a)\right) =$

$-\sum_{i=1}^{p} x_i\sigma^{i+1}(c) = -\sum_{i=1}^{p}(x_{i+1}-x_1)\sigma^{i+1}(c) = -\sum_{i=1}^{p} x_{i+1}\sigma^{i+1}(c) + \sum_{i=1}^{p} x_1\sigma^{i+1}(c) = a+1$. Logo, $\sigma(a) = a+1$.

Do fato que $A^{(\sigma)} = R$ segue que $a^p - a \in R$, pois $\sigma(a^p - a) = \sigma(a)^p - \sigma(a) = (a+1)^p - (a+1) = a^p + 1 - a - 1 = a^p - a$. Agora, do lema anterior segue que existe um R–isomorfismo φ tal que o diagrama abaixo comuta:

$$\begin{array}{ccc} \dfrac{R[X]}{(f(X))} & \xrightarrow{\varphi} & R[a] \\ \psi \downarrow & & \downarrow \sigma/R[a] \\ \dfrac{R[X]}{(f(X))} & \xrightarrow{\varphi} & R[a] \end{array}$$

onde $f(X) = X^p - X - (a^p - a)$ e $\psi(x) = x+1$, para $x = X + (f(X))$. Assim, $R[a]$ é uma extensão p– cíclica de R com grupo de Galois $(\sigma/R[a])$.

Resta mostrar que $R[a] = A$. Para tal, é suficiente observarmos que $R[a]$ e A são extensões de Galois de R com grupos de Galois $(\sigma/R[a])$ e (σ), respectivamente, e a inclusão $R[a] \hookrightarrow A$ é um homomorfismo de extensões de Galois. Então segue de II.4.4, que $R[a] = A$.

COROLÁRIO 1.4: Sejam A e A' duas extensões p–cíclicas de R com grupos de Galois (σ) e (σ'), respectivamente. Se $a \in A$ e $a' \in A'$ são tais que $\sigma(a) = a+1$ e $\sigma'(a') = a'+1$, então: (A,σ) é isomorfo à (A',σ') se e somente se $a^p - a = a'^p - a' + (r^p - r)$, para algum $r \in R$.

Prova: Suponhamos que existe um isomorfismo de extensões de Galois $\varphi : (A,\sigma) \to (A',\sigma')$. Neste caso, temos $\sigma'(\varphi(a) - a') = (\sigma' \circ \varphi)(a) - \sigma'(a') = (\varphi \circ \sigma)(a) - \sigma'(a') = \varphi(a+1) - (a'+1) = \varphi(a) - a'$, ou seja, $\varphi(a) - a' \in R$, já que $A^{(\sigma')} = R$. Assim, tomando $r = \varphi(a) - a'$, temos $a'^p - a' + (r^p - r) = a'^p - a' + (\varphi(a) - a')^p - (\varphi(a) - a') = a'^p - a' + \varphi(a)^p - a'^p - \varphi(a) + a' = \varphi(a^p - a) = a^p - a$, pois $a^p - a \in R$.

Reciprocamente, suponhamos que existe $r \in R$ tal que $a^p - a = a'^p - a' + (r^p - r)$. Então temos $a^p - a = (a+r)^p - (a'+r)$. Definindo então $\varphi : R[a] \to R[a']$, por $\varphi/R = id_R$ e $\varphi(a) = a'+r$, segue que φ é um R– homomorfismo de anéis bem definido, como é fácil ver. Agora, como $(\sigma' \circ \varphi)(a) = \sigma'(a'+r) = a'+1+r$ e $\varphi \circ \sigma)(a) = \varphi(a+1) = a'+r+1$, segue de II.4.4 que φ é um isomorfismo de extensões de Galois de R. Do teorema anterior, temos $A = R[a] \simeq R[a'] = A'$, ou seja, $(A,\sigma) \simeq (A',\sigma')$.

Queremos agora classificar as extensões p–cíclicas de R. Mostraremos que esta classificação é feita segundo a estrutura do anel R, visto que existe uma extensão p–cíclica

de R, para cada $r \in R$, a saber $R[X]/(X^p - X - r)$, e toda extensão p– cíclica de R é desta forma. Começaremos por observar que o conjunto $\wp R = \{r^p - r : r \in R\}$ é um subgrupo do grupo aditivo R. De fato, $0 = 1^p - 1 \in \wp R$, e dados $r^p - r, s^p - s \in \wp R$, temos $(r^p - r) + (s^p - s) = (r+s)^p - (r+s) \in \wp R$. Então podemos considerar o grupo quociente $R/\wp R$. Vamos mostrar que $T(\mathbb{Z}/p\mathbb{Z}, R)$, o qual denotaremos simplesmente por $T_1(R)$, é isomorfo ao grupo aditivo $R/\wp R$. Para tanto, consideremos a aplicação $\theta : T_1(R) \to R/\wp R$, definida como segue: Dado $[A, \sigma] \in T_1(R)$, existe $a \in A$ tal que $\sigma(a) = a + 1$, $a^p - a = r_a \in R$ e $A = R[a]$. Definimos então $\theta([A, \sigma]) = [r_a]$, onde $[r_a] = r_a + \wp R \in R\wp/R$. Do corolário 1.4 segue que θ está bem definida e é injetora. É claro que θ é também sobrejetora, pelo teorema 1.1.

Agora estamos em condições de provar o seguinte:

TEOREMA 1.5: Com as mesmas notações acima, $\theta : T_1(R) \to R/\wp R$ é um isomorfismo de grupos.

Prova Falta apenas ver que θ é um homomorfismo de grupos. Consideremos então $[A, \sigma], [B, \tau] \in T_1(R)$. Sejam $a \in A$ e $b \in B$ tais que $\sigma(a) = a + 1$ e $\tau(b) = b + 1$. Consideremos ainda $r_a = a^p - a$ e $r_b = b^p - b$. Temos que mostrar então que $\theta([A, \sigma] * [B, \tau]) = \theta\left([(A \otimes B)^{\sigma^{-1} \otimes \tau}, \sigma \otimes 1]\right) = [r_a + r_b]$. Para tal, definimos $c = a \otimes 1 + 1 \otimes b \in A \otimes B$. Como $(\sigma^{-1} \otimes \tau)(c) = (\sigma^{-1} \otimes \tau)(a \otimes 1 + 1 \otimes b) = (\sigma^{-1} \otimes \tau)(a \otimes 1) + (\sigma^{-1} \otimes \tau)(1 \otimes b) = (a-1) \otimes 1 + 1 \otimes (b+1) = a \otimes 1 - 1 \otimes 1 + 1 \otimes b + 1 \otimes 1 = a \otimes 1 + 1 \otimes b = c$, segue que $c \in (A \otimes B)^{\sigma^{-1} \otimes \tau}$. Além disso, como $(\sigma \otimes 1)(c) = (\sigma \otimes 1)(a \otimes 1 + 1 \otimes b) = (\sigma \otimes 1)(a \otimes 1) + (\sigma \otimes 1)(1 \otimes b) = (a+1) \otimes 1 + 1 \otimes b = a \otimes 1 + 1 \otimes 1 + 1 \otimes b = c + 1$, segue que $c \in (A \otimes B)^{\sigma^{-1} \otimes \tau}$ verifica $(\sigma \otimes 1)(c) = c + 1$. Assim, $\theta\left([(A \otimes B)^{\sigma^{-1} \otimes \tau}, \sigma \otimes 1]\right) = [c^p - c] = [(a \otimes 1 + 1 \otimes b)^p - (a \otimes 1 + 1 \otimes b)] = [(a \otimes 1)^p + (1 \otimes b)^p - (a \otimes 1) - (1 \otimes b)] = [a^p \otimes 1 + 1 \otimes b^p - a \otimes 1 - 1 \otimes b] = [(a^p - a) \otimes 1 + 1 \otimes (b^p - b)] = [r_a \otimes 1 + 1 \otimes r_b] = [(r_a + r_b) \otimes 1] = [r_a + r_b]$. Logo, θ é um isomorfismo de grupos, como queríamos mostrar.

§2. EXTENSÕES p^n–CÍCLICAS

Neste parágrafo descreveremos as extensões p^n– cíclicas de um anel R, via o anel de vetores de Witt sobre R. Usaremos então os resultados obtidos no apêndice, bem como manteremos aquelas notações.

Dado um anel A e $x = (x_0, \ldots, x_{n-1}) \in W_n(A)$, notaremos $x' = (x_0, \ldots, x_{n-2}) \in W_{n-1}(A)$ e $(x', 0) = (x_0, \ldots, x_{n-2}, 0) \in W_n(A)$. Ainda, ao longo deste capítulo, $R[X]$

denotará o anel de polinômios nas indeterminadas $X = (X_0, \ldots, X_{n-1})$ e para todo $r \in W_n(R)$, notaremos por $(X^\pi - X - r)$ o ideal de $R[X]$ gerado por todas as componentes de $X^\pi - X - r \in W_n(R[X])$.

Se $A = R[X]$ e $X'^\pi - X' = (f_0(X'), \ldots, f_{n-2}(X')) \in W_{n-1}(A)$, onde $f_i(X') = f_i(X_0, \ldots, X_{n-2}) \in \mathbb{Z}/p\mathbb{Z}[X_0, \ldots, X_{n-2}]$, $0 \leq i \leq n-2$, então segue do teorema A.2 e corolário A.3 que existe $f_{n-1}(X') \in \mathbb{Z}/p\mathbb{Z}[X_0, \ldots, X_{n-2}]$, tal que $(X', 0)^\pi - (X', 0) = (f_0(X'), \ldots, f_{n-2}(X'), f_{n-1}(X'))$. Além disso, se B é uma álgebra sobre $\mathbb{Z}/p\mathbb{Z}$, então para todo $b = (b_0, \ldots, b_{n-2}) \in W_{n-1}(B)$, temos $(b', 0)^\pi - (b', 0) = (f_0(b), \ldots, f_{n-2}(b), f_{n-1}(b))$.

Lembramos ainda que se $\varphi : A \to A$ é um homomorfismo de anéis, então φ se extende naturalmente a um homomorfismo de anéis de $W_n(A)$, por $(a_0, \ldots, a_{n-1}) \mapsto (\varphi(a_0), \ldots, \varphi(a_{n-1}))$, para todo $(a_0, \ldots, a_{n-1}) \in W_n(A)$. Por simplicidade de notação, escreveremos φ para denotar tal extensão. Ainda, é claro que $\varphi \circ \pi = \pi \circ \varphi$. De fato, $\varphi \circ \pi(a_0, \ldots, a_{n-1}) = \varphi(a_0^p, \ldots, a_{n-1}^p) = (\varphi(a_0^p), \ldots, \varphi(a_{n-1}^p)) = (\varphi(a_0)^p, \ldots, \varphi(a_{n-1})^p) = \pi(\varphi(a_0), \ldots, \varphi(a_{n-1})) = \pi \circ \varphi(a_0, \ldots, a_{n-1})$, para todo $(a_0, \ldots, a_{n-1}) \in W_n(A)$.

Seja (A, σ) uma extensão p^n–cíclica de R. Notaremos por A^σ o anel fixo de A, por (σ).

Podemos provar agora o seguinte teorema, o qual é uma generalização do teorema 1.1

TEOREMA 2.1: Sejam $a = (a_0, \ldots, a_{n-1}) \in W_n(R)$ e $A = R[X]/(X^\pi - X - a)$. Então (A, σ) é uma extensão p^n–cíclica de R com grupo de Galois (σ) gerado pelo automorfismo $\sigma : A \to A$ tal que $\sigma(x) = x + 1$ em $W_n(A)$, onde $x = X + (X^\pi - X - a)$.

Prova: Consideremos as aplicações $\varphi : R[X] \to R[X]$, dada por $\varphi/R = id_R$, $\varphi(X) = X + 1$ em $W_n(R[X])$ e $\psi : R[X] \to R[X]$, dada por $\psi/R = id_R$, $\psi(X) = X - 1$ em $W_n(R[X])$. É fácil ver que φ e ψ são R–homomorfismos de anéis e como $\varphi \circ \psi = \psi \circ \varphi = id_{R[X]}$, segue que φ é um R–isomorfismo de anéis. Considerando então a extensão natural de φ ao anel $W_n(R[X])$, temos $\varphi(X^\pi - X - a) = (X+1)^\pi - (X+1) - a = X^\pi - X - a$. Então, chamando I ao ideal $(X^\pi - X - a)$, é fácil ver que $\varphi(I) = I$ e assim φ induz um R–isomorfismo $\sigma : R[X]/I \to R[X]/I$, dado por $\sigma(x) = x + 1$, onde $x = (x_0, \ldots, x_{n-1}) \in W_n(A)$ é tal que $x_i = X_i + (X^\pi - X - a)$. Assim, $A = R[X]/I = R[x_0, \ldots, x_{n-1}]$.

Vamos agora mostrar que σ é um automorfismo de ordem p^n. De fato, $\sigma^{p^l}(x) = x + p^l 1 = x + V^l(1) = (x_0, \ldots, x_{l-1}, x_l + 1, y_{l+1}, \ldots, y_{n-1})$, com $y_j \in R$, para todo $l + 1 \leq j \leq n - 1$, isto é, $\sigma^{p^l}/R[x_0, \ldots, x_{l-1}] = id_{R[x_0, \ldots, x_{l-1}]}$. Assim, $\sigma^{p^n}(x) = x$ e $\sigma^{p^l}(x) \neq x$, para todo $0 \leq l \leq n - 1$. Logo, σ é um automorfismo de ordem p^n, e ele

gera um grupo cíclico de ordem p^n

Queremos mostrar agora que $A^\sigma = R$. Claramente $R \subseteq A^\sigma$, basta então mostrar que $A^\sigma \subseteq R$. Seja $\alpha \in A^\sigma$. Assim, temos $\sigma^j(\alpha) = \alpha$, para todo $0 \leq j \leq p^n - 1$. Escrevendo α na forma $\alpha = \sum_{i=0}^{p-1} \alpha_i x_{n-1}^i$, com $\alpha_i \in R[x_0, \ldots, x_{n-2}]$, $0 \leq i \leq p-1$, temos $\sigma^{p^{n-1}}(\alpha) = \alpha$, ou equivalentemente, $\sum_{i=0}^{p-1} \alpha_i (x_{n-1}+1)^i = \sum_{i=0}^{p-1} \alpha_i x_{n-1}^i$, já que $\sigma^{p^{n-1}}(x_{n-1}) = x_{n-1} + 1$. Desenvolvendo esta igualdade resulta o seguinte sistema:

$$\begin{cases} \alpha_0 + \alpha_1 + \alpha_2 + \cdots + \alpha_i + \cdots + \alpha_{p-1} = \alpha_0 \\ \alpha_1 + \binom{2}{1}\alpha_2 + \cdots + \binom{i}{1}\alpha_i + \cdots + \binom{p-1}{1}\alpha_{p-1} = \alpha_1 \\ \vdots \quad \vdots = \vdots \\ \alpha_i + \cdots + \binom{p-1}{i}\alpha_{p-1} = \alpha_i \\ \vdots \quad \vdots = \vdots \\ \alpha_{p-2} + (p-1)\alpha_{p-1} = \alpha_{p-2} \\ \alpha_{p-1} = \alpha_{p-1} \end{cases}$$

de onde segue que $\alpha_1 = \alpha_2 = \cdots = \alpha_{p-1} = 0$ como é fácil verificar. Logo, $\alpha = \alpha_0 \in R[x_0, \ldots, x_{n-2}]$. Repetindo-se este argumento tantas vezes quanto necessário, obtemos $\alpha = r_0 \in R$ e portanto $A^\sigma \subseteq R$, de onde segue que $A^\sigma = R$.

Para ver que A é uma extensão de Galois de R com grupo (σ), usamos o ítem (f) do teorema II.1.6. Como para todo $\tau \in (\sigma)$ temos $\tau = \sigma^j$, para algum $0 \leq j \leq p^n - 1$, então $\tau(x) = \sigma^j(x) = x + j1$. Escrevendo $j = l_1 p^{s_1} + \cdots + l_r p^{s_r}$, onde $s_1 < s_2 < \ldots < s_r$ e $0 \leq l_i \leq p-1$, $1 \leq i \leq r$, com $l_1 \geq 1$, obtemos $\tau(x) = x + j1 = x + (l_1 p^{s_1} + \cdots + l_r p^{s_r})1 = x + l_1 p^{s_1} 1 + \cdots + l_r p^{s_r} 1 = x + l_1 V^{s_1}(1) + \cdots + l_r V^{s_r}(1) = (x_0, \ldots, x_{s_1}, \ldots, x_{n-1}) + (0, \ldots, 0, l_1, t_{s_1+1}, \ldots, t_{n-1})$, com $t_i \in R$, para todo $s_1 + 1 \leq i \leq n-1$, onde l_1 oucupa a s_1–ésima posição. Assim, $\tau(x_{s_1}) - x_{s_1} = l_1$ que é um elemento inversível em R. Portanto, para todo $\tau \in (\sigma)$, $\tau \neq id$, existe um elemento $y \in A$ tal que $\sigma(y) - y$ é inversível em R. Segue então de II.1.6(f) que A é uma extensão de Galois de R, o que completa a prova do teorema.

A extensão (A, σ) construida no teorema acima será chamada a extensão p^n–cíclica canônica de R associada com a, a qual será denotada por (A_a, σ). Ainda, o elemnto $x \in W_n(A)$ tal que $\sigma(x) = x + 1$, será dito um elemmento canônico da extensão (A_a, σ).

Da prova do teorema anterior, obtemos o seguinte

COROLÁRIO 2.2: Seja $a \in W_n(R)$ e (A_a, σ) a extensão p^n–cíclica canônica de

R associada com a. Seja $x = (x_0, \ldots, x_{n-1}) \in W_n(A)$ o elemento canônico de $(\mathcal{A}_a, \sigma)$. Então $\mathcal{A}_a = R[x]$ e $\mathcal{A}_a^{\sigma^l} = R[x_0, \ldots, x_{l-1}]$.

Como recíproca do teorema anterior, podemos apresentar o seguinte resultado, o qual corresponde ao teorema 1.3

TEOREMA 2.3: Seja (A, σ) uma extensão p^n–cíclica de R. Então existe $x \in W_n(A)$ tal que $\sigma(x) = x + 1$. Neste caso, temos $x^{p^n} - x \in W_n(R)$ e $\mathcal{A} = R[x]$.

Prova: Como $(\mathcal{A}, \sigma)$ é uma extensão de Galois de R, segue do corolário II.1.8 que existe $z_0 \in \mathcal{A}$ tal que $tr_{(\sigma)}(z_0) = 1$. Tomando $z = (z_0, 0, \ldots, 0) \in W_n(A)$ e $t = \sum_{i=0}^{p^n-1} \sigma^i(z)$, temos $\sigma(t) = \sigma(\sum_{i=0}^{p^n-1} \sigma^i(z)) = \sum_{i=0}^{p^n-1} \sigma^{i+1}(z) = \sum_{i=0}^{p^n-1} \sigma^i(z) = t$, isto é, $t \in (W_n(A))^\sigma = W_n(A^\sigma) = W_n(R)$. Agora, como $tr_{(\sigma)}(z_0) = 1$ segue que $t = (1, t_1, \ldots, t_{n-1})$, com $t_i \in R$, $1 \leq i \leq n-1$. Assim, pela proposição A.13 do apêndice, segue que existe $t^{-1} \in W_n(R)$ tal que $tt^{-1} = \mathbf{1}$. Logo temos $\mathbf{1} = tt^{-1} = t^{-1} \sum_{i=0}^{p^n-1} \sigma^i(z) = \sum_{i=0}^{p^n-1} \sigma^i(t^{-1}z)$. Tomando então $x = -\sum_{i=0}^{p^n-1} i\sigma^i(t^{-1}z)$, obtemos $x \in W_n(A)$ e $\sigma(x) = \sigma(-\sum_{i=0}^{p^n-1} i\sigma^i(t^{-1}z)) = -\sum_{i=0}^{p^n-1} i\sigma^{i+1}(t^{-1}z) = -\sum_{i=0}^{p^n-1} (i+1)\sigma^{i+1}(t^{-1}z) + \sum_{i=0}^{p^n-1} \sigma^{i+1}(t^{-1}z) = -\sum_{i=0}^{p^n-1} i\sigma^i(t^{-1}z) + \sum_{i=0}^{p^n-1} \sigma^i(t^{-1}z) = x+1$. Além disso, temos $\sigma(x^{p^n} - x) = (x+1)^{p^n} - (x+1) = x^{p^n} - x$, em $W_n(A)$. Segue daí que $x^{p^n} - x \in W_n(R)$.

Para mostrar que $A = R[x]$, observemos que $R[x] \subseteq A$. Além disso, $\sigma/R[x]$ é claramente um automorfismo de $R[x]$ e da prova do teorema 2.1, segue que $l(\sigma/R[x]) = p^n$, $(R[x])^{\sigma/R[x]} = R$ e que $R[x]$ é uma extensão de Galois de R. Assim, $(R[x], \sigma/R[x])$ é uma extensão p^n–cíclica de R. Consideremos então o diagrama abaixo:

$$\begin{array}{ccc} R[x] & \hookrightarrow & \mathcal{A} \\ \sigma/R[x] \downarrow & & \downarrow \sigma \\ R[x] & \hookrightarrow & \mathcal{A} \end{array}$$

Este diagrama é claramente comutativo, logo $R[x] \simeq \mathcal{A}$, por II.4.4. Portanto, $A = R[x]$ e isto completa a prova do teorema.

COROLÁRIO 2.4: Sejam $\mathcal{A}$ e R anéis tais que $R \subseteq A$ e seja σ um R–automorfismo de A. Então $(\mathcal{A}, \sigma)$ é uma extensão p^n–cíclica de R se e somente se $(\mathcal{A}, \sigma)$ é isomorfa à extensão p^n–cíclica canônica de R associada com algum elemento

$a \in W_n(R)$. Neste caso podemos tomar $a = x^\pi - x$, para algum $x \in W_n(A)$ tal que $\sigma(x) = x + 1$.

Prova: Mostraremos que se (A, σ) é uma extensão p^n–cíclica de R então $(A, \sigma) \simeq (A_a, \rho)$ para algum elemento $a \in W_n(R)$. A recíproca é imediata.

Seja então (A, σ) uma extensão p^n– cíclica de R. Logo, existe $x = (x_0, \ldots, x_{n-1}) \in W_n(A)$, tal que $\sigma(x) = x + 1$ e seja $a = x^\pi - x$. Consideremos $Y = (Y_0, \ldots, Y_{n-1})$ um conjunto de indeterminadas sobre R e tomemos o anel de polinômios $R[Y]$. A aplicação $f : R[Y] \to A$ definida por $f/R = id$ e $f(Y_i) = x_i$, $0 \leq i \leq n-1$, é um R–homomorfismo de anéis. Olhando agora sua extensão natural à $W_n(R[Y])$ temos $f(Y^\pi - Y - a) = x^\pi - x - a = 0$. Segue daí que $f(I) = 0$, onde $I = (Y^\pi - Y - a)$. Assim, f induz um R–homomorfismo $g : R[Y]/I \to A$, dado por $g(y) = x$, onde $y = Y + I$. Seja τ o R–automorfismo canônico da extensão $R \subseteq R[X]/I$. Então $g \circ \tau(y) = g(y+1) = x + 1 = \sigma(x) = \sigma(g(y)) = \sigma \circ g(y)$. Portanto, $g \circ \tau = \sigma \circ g$ e segue então de II.4.4 que g é um isomorfismo de extensões de Galois. Isto completa a prova.

Finalizamos este parágrafo observando que toda extensão p^n–cíclica de R pode ser mergulhada em uma extensão p^m–cíclica de R, para todo $m > n$. Mais precisamente,

PROPOSIÇÃO 2.5: Seja (A, σ) uma extensão p^n–cíclica de R. Então para todo $m > n$ existe uma extensão p^m–cíclica (B, τ) de R, tal que $(A, \sigma) \simeq (B^{\tau^{p^n}}, \tau/B^{\tau^{p^n}})$.

Prova: Pelo corolário anterior, existe $a = (a_0, \ldots, a_{n-1}) \in W_n(R)$ tal que $(A, \sigma) \simeq (R[X]/(X^\pi - X - a), \rho)$, com $\rho(x) = x + 1$, onde $x = X + (X^\pi - X - a)$. Escolhendo arbitrariamente $a_n, \ldots, a_{m-1} \in R$ e fazendo $b = (a_0, \ldots, a_{n-1}, a_n, \ldots, a_{m-1}) \in W_m(R)$, consideremos (B, τ) a extensão p^m–cíclica canônica associada com b. Então, $B = R[Y]/(Y^\pi - Y - b)$, onde $Y = (Y_0, \ldots, Y_{m-1})$ é um conjunto de indeterminadas sobre R e τ é tal que $\tau(y) = y + 1$, com $y = Y + (Y^\pi - Y - b)$.

Segue da prova do teorema 2.1 que $B^{\tau^{p^n}} = R[y_0, \ldots, y_{n-1}]$. Consideremos então o seguinte diagrama:

$$\begin{array}{ccc} B^{\sigma^{p^n}} = R[y_0, \ldots, y_{n-1}] & \xrightarrow{\varphi} & R[x_0, \ldots, x_{n-1}] = A \\ \tau/B^{\sigma^{p^n}} \downarrow & & \downarrow \sigma \\ B^{\sigma^{p^n}} = R[y_0, \ldots, y_{n-1}] & \xrightarrow{\varphi} & R[x_0, \ldots, x_{n-1}] = A \end{array}$$

onde $y_i = Y_i + (Y^\pi - Y - b)$, $x_i = X_i + (X^\pi - X - a)$, $0 \leq i \leq n-1$ e φ é o R–homomorfismo definido por $\varphi/R = id_R$ e $\varphi(y_i) = x_i$, $0 \leq i \leq n-1$.

Como este diagrama é comutativo, segue de II.4.4 que φ é um isomorfismo de extensões de Galois de R, o que completa a prova da proposição.

§3. CLASSIFICAÇÃO DAS EXTENSÕES p^n–CÍCLICAS

A partir deste parágrafo, $T_n(R)$ denotará o grupo de Harrison $T(\mathbb{Z}/p^n\mathbb{Z}, R)$ de extensões p^n– cíclicas de R. Nosso objetivo aqui é determinar a estrutura deste grupo como um quociente do grupo aditivo $W_n(R)$.

Definiremos $\wp W_n(R) = \{a^\pi - a : a \in W_n(R)\}$. Do fato que π é um homomorfismo de anéis, segue que $\wp W_n(R)$ é um subgrupo do grupo aditivo $W_n(R)$.

Dada uma extensão p^n–cíclica (A, σ) de R, existe $x \in W_n(A)$ tal que $\sigma(x) = x + 1$ e $a = x^\pi - x \in W_n(R)$, pelo teorema 2.3. Um tal a será dito vetor de Witt correspondente à extensão (A, σ). Com esta convenção podemos provar nosso próximo resultado, o qual é uma generalização de 1.4.

LEMA 3.1: Sejam (A, σ) e (B, τ) duas extensões p^n–cíclicas de R, e sejam a e b vetores de Witt correspondentes às extensões (A, σ) e (B, τ), respectivamente. Então (A, σ) é isomorfo à (B, τ) se e somente se $a \equiv b \pmod{\wp W_n(R)}$.

Prova: Sejam $X = (X_0, \ldots, X_{n-1})$, $Y = (Y_0, \ldots, Y_{n-1})$ indeterminadas sobre R, x e y elementos de $W_n(A)$ e $W_n(B)$, respectivamente, tais que $\sigma(x) = x + 1$ e $\tau(y) = y+1$. Sejam ainda, $a = x^\pi - x$ e $b = y^\pi - y$. Sabemos que $A \simeq R[X]/(X^\pi - X - a)$ e $B \simeq R[Y]/(Y^\pi - Y - b)$, pelo corolário 2.4. Suponhamos $a \equiv b \pmod{\wp W_n(R)}$. Então existe $r \in W_n(R)$ tal que $b = a + r^\pi - r$.

A aplicação $\varphi : R[X] \to R[Y]$, dada por $\varphi/R = id_R$ e $\varphi(X_i) = \alpha_i$, onde α_i é a i–ésima componente de $Y + r$ em $W_n(R[Y])$, para $0 \leq i \leq n-1$, é um R–homomorfismo de anéis. Olhando sua extensão natural $\varphi : W_n(R[X]) \to W_n(R[Y])$, temos $\varphi(X) = Y + r$ e portanto $\varphi(X^\pi - X - a) = (Y + r)^\pi - (Y + r) - a = Y^\pi - Y - a + r^\pi - r = Y^\pi - Y - b$. Segue então que φ induz um R–homomorfismo de anéis $g : A \to B$, dado por $g(x) = y + r$.

Como $\tau \circ g(x) = \tau(y + r) = y + 1 + r = g(x + 1) = g(\sigma(x)) = g \circ \sigma(x)$, segue que $\tau \circ g = g \circ \sigma$ e então g é um isomorfismo de extensões de Galois, por II.4.4.

Reciprocamente, suponhamos que $f : (A, \sigma) \to (B, \tau)$ é um isomorfismo de extensões de Galois. Do fato que $\tau(f(x) - y) = \tau \circ f(x) - \tau(y) = f \circ \sigma(x) - (y+1) = f(x) - y$, segue que $f(x) - y \in W_n(R)$. Tomando então $r = f(x) - y$, temos $r^\pi - r = (f(x) - y)^\pi - (f(x) - y) = f(x^\pi) - y^\pi - f(x) + y = f(x^\pi - x) - (y^\pi - y) = f(a) - b = a - b$, isto é, $a = b + r^\pi - r$.

Portanto, $a \equiv b \pmod{\wp W_n(R)}$, como queríamos mostrar.

Notaremos por $\omega_n(R)$ o grupo quociente $\omega_n(R) = W_n(R)/\wp W_n(R)$. Vamos definir uma aplicação $\theta_n : T_n(R) \to \omega_n(R)$, como segue: Dada uma extensão p^n–cíclica (A, σ) de R, seja $a \in W_n(R)$ um vetor de Witt correspondente ã extensão (A, σ). Definimos então $\theta_n([A, \sigma]) = [a]$, onde $[a] = a + \wp W_n(R)$. Segue do lema anterior que θ_n está bem definida e é injetora. Segue também do teorema 2.1 que θ_n é sobrejetora. Vamos mostrar em nosso próximo teorema que θ_n é um isomorfismo de grupos. Antes porém, observamos que no caso $n = 1$, esta aplicação coincide com a aplicação θ definida no parágrafo 1.

Introduziremos ainda as seguintes notações: Se $a = (a_0, \ldots, a_{n-1}) \in W_n(A)$, escreveremos $a \otimes 1 = (a_0 \otimes 1, \ldots, a_{n-1} \otimes 1) \in W_n(A \otimes B)$. Assim, $(a \otimes 1)^\pi = ((a \otimes 1)^p, \ldots, (a_{n-1} \otimes 1)^p) = (a_0^p \otimes 1, \ldots, a_{n-1}^p \otimes 1) = a^\pi \otimes 1$. Mostraremos ainda que $(a + b) \otimes 1 = a \otimes 1 + b \otimes 1$, para todos $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in W_n(A)$. De fato, consideremos $f : A \to A \otimes B$, dado por $f(a) = a \otimes 1$, para todo $a \in A$. Assim, f é um R–homomorfismo de anéis. Então f possui uma extensão natural $f : W_n(A) \to W_n(A \otimes B)$, dada por $f(a) = f(a_0, \ldots, a_{n-1}) = (f(a_0), \ldots, f(a_{n-1})) = (a_0 \otimes 1, \ldots, a_{n-1} \otimes 1) = a \otimes 1$ em $W_n(A \otimes B)$. Como f é um homomorfismo aditivo, segue que $(a + b) \otimes 1 = f(a + b) = f(a) + f(b) = a \otimes 1 + b \otimes 1$.

Ainda, se $\rho : A \to A$ é um homomorfismo de R–álgebras, então $\rho \otimes 1 : A \otimes B \to A \otimes B$ é também um homomorfismo de R–álgebras. Considerando então sua extensão natural $\rho \otimes 1 : W_n(A \otimes B) \to W_n(A \otimes B)$, temos para cada $a \in W_n(A)$, $(\rho \otimes 1)(a \otimes 1) = (\rho \otimes 1)(a_0 \otimes 1, \ldots, a_{n-1} \otimes 1) = (\rho(a_0) \otimes 1, \ldots, \rho(a_{n-1}) \otimes 1) = \rho(a) \otimes 1$. De maneira análoga, todas as considerações acima podem ser feitas à segunda variável em $W_n(A \otimes B)$.

Estamos agora em condições de mostrar o seguinte

TEOREMA 3.2: Com as mesmas notações acima, $\theta_n : T_n(R) \to \omega_n(R)$ é um isomorfismo de grupos abelianos, para todo $n \geq 1$.

Prova: Já sabemos que θ_n é uma bijeção. Falta então mostrar que θ_n é um homomorfismo de grupos. Sejam (A, σ) e (B, τ) duas extensões p^n–cíclicas de R e sejam $x \in W_n(A)$ e $y \in W_n(B)$ tais que $\sigma(x) = x + 1$ e $\tau(y) = y + 1$. Logo, $\theta_n([A, \sigma]) = [a]$ e $\theta_n([B, \tau]) = [b]$, onde $a = x^\pi - x \in W_n(R)$ e $b = y^\pi - y \in W_n(R)$.

Temos que mostrar que $\theta_n([A, \sigma] * [B, \tau]) = [a + b]$. Para tal, consideremos $z = x \otimes 1 + 1 \otimes y \in W_n(A \otimes B)$. Como $(\sigma^{-1} \otimes \tau)(z) = (\sigma^{-1} \otimes \tau)(x \otimes 1 + 1 \otimes y) = \sigma^{-1}(x) \otimes \tau(1) + \sigma^{-1}(1) \otimes \tau(y) = (x - 1) \otimes 1 + 1 \otimes (y + 1) = x \otimes 1 - 1 \otimes 1 + 1 \otimes y + 1 \otimes 1 = x \otimes 1 + 1 \otimes y = z$,

segue que $z \in W_n((A \otimes B)^{\sigma^{-1}\otimes\tau})$. Além disso, $(\sigma \otimes 1)(z) = (\sigma \otimes 1)(x \otimes 1 + 1 \otimes y) = \sigma(x) \otimes 1 + \sigma(1) \otimes y = (x+1) \otimes 1 + 1 \otimes y = x \otimes 1 + 1 \otimes 1 + 1 \otimes y = z + 1$. Assim, $z \in W_n((A \otimes B)^{\sigma^{-1}\otimes\tau})$ é tal que $(\sigma \otimes 1)(z) = z + 1$.

Agora, do fato que $[(A \otimes B)^{\sigma^{-1}\otimes\tau}, \sigma \otimes 1] = [A, \sigma] * [B, \tau]$, segue que $\theta_n([A, \sigma] * [B, \tau]) = [z^\pi - z] = [(x \otimes 1 + 1 \otimes y)^\pi - (x \otimes 1 + 1 \otimes y)] = [(x \otimes 1)^\pi + (1 \otimes y)^\pi - (x \otimes 1) - (1 \otimes y)] = [x^\pi \otimes 1 + 1 \otimes y^\pi - x \otimes 1 - 1 \otimes y] = [x^\pi - x \otimes 1 + 1 \otimes y^\pi - y] = [a + b]$, como queríamos provar.

Vamos mostrar agora que todo elemento de $T_n(R)$ possui ordem aditiva divisor de p^n.

Inicialmente, seja $a = (a_0, \ldots, a_{n-1}) \in W_n(R)$. Então $V(a^\pi - a) = V(a^\pi) - V(a) = (V(a))^\pi - (V(a)) \in \wp W_n(R)$ e $\pi(a^\pi - a) = (a^\pi)^\pi - (a^\pi) \in \wp W_n(R)$. Assim, $V(\wp W_n(R)) \subseteq \wp W_n(R)$ e $\pi(\wp W_n(R)) \subseteq \wp W_n(R)$. Logo as aplicações V e π induzem naturalmente homomorfismos aditivos de $w_n(R)$ em $w_n(R)$, os quais notaremos por v e π, respectivamente. Se $[a] \in w_n(R)$, então $a^\pi \equiv a \pmod{\wp W_n(R)}$ e assim $[a] = [a^\pi] = [a]^\pi$. Segue que a aplicação $\pi : w_n(R) \to w_n(R)$ induzida por $\pi : W_n(R) \to W_n(R)$ é a aplicação identidade em $w_n(R)$.

Agora, do fato que $pa = V(a^\pi)$ em $W_n(A)$, temos que $p[a] = v([a]^\pi) = v([a])$ em $w_n(R)$. Assim $p^n[a] = v^n([a]) = 0$, para todo $[a] \in w_n(R)$. Logo todo elemento de $w_n(R)$ tem ordem aditiva um divisor de p^n e segue que $w_n(R)$ é um $\mathbb{Z}/p^n\mathbb{Z}$-módulo. Portanto $T_n(R) \simeq w_n(R)$ possui uma estrutura de $\mathbb{Z}/p\mathbb{Z}$-módulo.

Assim, $T_1(R) \simeq R/\wp R$ é um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$ e portanto $T_1(R)$ possui uma base distinta do conjunto vazio, sempre que $T_1(R) \neq 0$. Mostraremos que $T_n(R)$ é $\mathbb{Z}/p^n\mathbb{Z}$-módulo livre com posto $dim_{\mathbb{Z}/p\mathbb{Z}} T_1(R)$. (Para o caso $T_1(R) = 0$ ver o corolário 4.8, adiante).

Suponhamos $T_1(R) \neq 0$ e fixemos uma base $(u_i)_{i\in I}$ de $R/\wp R$ sobre $\mathbb{Z}/p\mathbb{Z}$, isto é, $R/\wp R = \bigoplus_{i\in I} \mathbb{Z}/p\mathbb{Z}u_i$. Como $u_i \in R/\wp R$, para todo $i \in I$, existe $a_i \in R$ tal que $u_i = a_i + \wp R$. Consideremos $u_i' = [a_i, 0, \ldots, 0] \in w_n(R)$ $(i \in I)$. Para termos uma descrição mais precisa do grupo de Harrison $T_n(R)$, provaremos primeiro o seguinte

TEOREMA 3.3: Com as mesmas notações acima, $w_n(R)$ é livre sobre $\mathbb{Z}/p^n\mathbb{Z}$ com base $(u_i')_{i\in I}$.

Prova: Suponhamos que para uma subfamília finita $a_1, \ldots, a_s \in (a_i)_{i\in I}$, e inteiros $n_1, \ldots, n_s$, $1 \leq n_i \leq p^n - 1$, $1 \leq i \leq s$, temos $\sum_{i=1}^{s} n_i[a_i, 0, \ldots, 0] = 0$ em $w_n(R)$. Escrevendo $n_i = \lambda_{1i}p^{n-1} + \cdots + \lambda_{l_i i}p^{n-l_i}$, onde $0 \leq \lambda_{ji} \leq p-1$, $l \leq n$, seja t tal que

$\lambda_{lt} \neq 0$ e $\lambda_{l+r,k} = 0$, para todo $1 \leq r \leq n-l$ e todo $1 \leq k \leq s$. (eventualmente podemos ter $l = n$). Temos então $0 = \sum_{i=1}^{s} n_i[a_i, 0, \ldots, 0] = \sum_{i=1}^{s} \sum_{j} \lambda_{ji} p^{n-j}[a_i, 0, \ldots, 0] = \sum_{i=1}^{s} \lambda_{li} p^{n-l}[a_i, 0, \ldots, 0] + \sum_{i=1}^{s} \sum_{j>l} \lambda_{ji} p^{n-j}[a_i, 0, \ldots, 0] = [0, \ldots, 0, c_{n-l}, \ldots, c_{n-1}]$, onde $c_{n-l} = \sum_{i=1}^{s} \lambda_{li} a_i$ e $c_{n-l-1}, \ldots, c_{n+1} \in R$. Logo existe $b = (b_0, \ldots, b_{n-1})$ com $(0, \ldots, 0, c_{n-l}, \ldots, c_{n-1}) = (b_0, \ldots, b_{n-1})^\pi - (b_0, \ldots, b_{n-1}) = (b_0, \ldots, b_{n-l-1}, 0, \ldots, 0)^\pi + (0, \ldots, 0, b_{n-l}, \ldots, b_{n-1})^\pi - (b_0, \ldots, b_{n-l-1}, 0, \ldots, 0) - (0, \ldots, 0, b_{n-l}, \ldots, b_{n-1})$.

Consideremos o homomorfismo $\varphi : W_n(R) \to W_{n-l-1}(R)$ dado por $\varphi(a_0, \ldots, a_{n-1}) = (a_0, \ldots, a_{n-l-1})$. Aplicando este homomorfismo ao primeiro e ao último membro da igualdade acima segue que $(b_0, \ldots, b_{n-l-1})^\pi - (b_0, \ldots, b_{n-l-1}) = 0$ em $W_{n-l-1}(R)$, e assim, $b_i^p = b_i$, $0 \leq i \leq n-l-1$. Portanto, em $W_n(R)$, temos $(b_0, \ldots, b_{n-l-1}, 0, \ldots, 0)^\pi - (b_0, \ldots, b_{n-l-1}, 0, \ldots, 0) = 0$. Logo, $(0, \ldots, 0, c_{n-l}, \ldots, c_{n-1}) = (0, \ldots, 0, b_{n-l}, \ldots, b_{n-1})^\pi - (0, \ldots, 0, b_{n-l}, \ldots, b_{n-1})$ e então $c_{n-l} = b_{n-l}^p - b_{n-l} \in \wp R$. Segue daí que $\sum_{i=1}^{s} \lambda_{li}(a_i + \wp R) = [0]$ em $R/\wp R$, o que contradiz a escolha de $(a_i)_{i \in I}$, pois $\lambda_{lt} \neq 0$. Assim, $(u_i')_{i \in I}$ é um sistema linearmente independente sobre $\mathbb{Z}/p^n\mathbb{Z}$.

Falta mostrar então que $(u_i)_{i \in I}$ é um sistema de geradores de $w_n(R)$ como $\mathbb{Z}/p^n\mathbb{Z}$-módulo. Para tal, seja L o $\mathbb{Z}/p^n\mathbb{Z}$- submódulo de $w_n(R)$ gerado por $(u_i)_{i \in I}$. Como $[y_0, y_1, \ldots, y_{n-1}] = [y_0, 0, \ldots, 0] + [0, y_1, 0, \ldots, 0] + \cdots + [0, \ldots, 0, y_{n-1}]$, para todo $[y_0, \ldots, y_{n-1}] \in w_n(R)$, é suficiente mostrarmos que $[0, \ldots, 0, y_i, 0, \ldots, 0] \in L$, onde y_i aparece na i-ésima componente, para todo $y_i \in R$, $0 \leq i \leq n-1$. Faremos isto por indução.

Seja $y_{n-1} \in R$ um elemento qualquer de R. Por hipótese, existem elementos $a_1, \ldots, a_m \in (a_i)_{i \in I}$ e inteiros $\lambda_1, \ldots, \lambda_m$ $(0 \leq \lambda_j \leq p-1)$ tais que $y_{n-1} + \wp R = \sum_{j=1}^{m} \lambda_j a_j + \wp R$. Logo existe $r \in R$ tal que $y_{n-1} = \sum_{j=1}^{m} \lambda_j a_j + r^p - r$. Portanto temos $(0, \ldots, 0, y_{n-1}) = (0, \ldots, 0, \sum_{j=1}^{m} \lambda_j a_j + r^p - r) = (0, \ldots, 0, \sum_{i=1}^{m} \lambda_j a_j) + (0, \ldots, 0, r)^\pi - (0, \ldots, 0, r)$ e assim, $[0, \ldots, 0, y_{n-1}] = [0, \ldots, 0, \sum_{j=1}^{m} \lambda_j a_j] = \sum_{j=1}^{m} \lambda_j v^{n-1}([a_j, 0, \ldots, 0]) = \sum_{j=1}^{m} \lambda_j p^{n-1}[a_j, 0, \ldots, 0] \in L$.

Suporemos por indução que, para todos $y_{i+1}, \ldots, y_{n-1} \in R$, $[0, \ldots, 0, y_{i+1}, \ldots, y_{n-1}] \in L$. Consideremos então $y_i \in R$. Assim, existem $a_1, \ldots, a_l \in (a_i)_{i \in I}$ e inteiros $\mu_1, \ldots, \mu_l$

com $0 \leq \mu_k \leq p-1$, $1 \leq k \leq l$ e $s \in R$ tais que $y_i = \sum_{j=1}^{l} \mu_j a_j + s^p - s$. Agora, $(0,\ldots,0,y_i,0,\ldots,0) = (0,\ldots,0,\sum_{j=1}^{l} \mu_j a_j + s^p - s, 0,\ldots,0) = (0,\ldots,0,\sum_{j=1}^{l} \mu_j a_j, 0,\ldots,0) + (0,\ldots,0,s,0,\ldots,0)^\pi - (0,\ldots,0,s,0,\ldots,0) + (0,\ldots,0,d_{i+1},\ldots,d_{n-1})$, onde $d_{i+1},\ldots,d_{n-1}$ são elementos de R e $s \in R$ está na i–ésima componente. Então temos:

$$\begin{aligned}[0,\ldots,0,y_i,0,\ldots,0] &= [0,\ldots,0,\sum_{j=1}^{l} \mu_j a_j, 0,\ldots,0] + [0,\ldots,0,d_{i+1},\ldots,d_{n-1}] \\ &= \sum_{j=1}^{l} \mu_j p^i [a_j,0,\ldots,0] + [0,\ldots,0,d_{i+1},\ldots,d_{n-1}]\end{aligned}$$

Como $[0,\ldots,0,d_{i+1},\ldots,d_{n-1}]$ e $\sum_{j=1}^{l} \mu_j p^i [a_j,0,\ldots,0]$ são elementos de L, segue que $[0,\ldots,0,y_i,0,\ldots,0] \in L$. Completando assim o processo de indução e a prova do teorema.

Do teorema anterior obtemos os seguintes corolários:

COROLÁRIO 3.4: Com as mesmas notações anteriores, temos:

$$T_n(R) \simeq \bigoplus_{i \in I} (\mathbb{Z}/p^n\mathbb{Z})\theta_n^{-1}(v_i')$$

para todo $n \geq 1$, onde $\theta_n^{-1}(v_i')$ são geradores livres de $T_n(R)$.

COROLÁRIO 3.5: Seja F um corpo finito de característica p. Então $T_n(F) \simeq \mathbb{Z}/p^n\mathbb{Z}$, para todo $n \geq 1$.

Prova: Pelo teorema anterior, é suficiente provar este corolário para o caso $n = 1$. Suponhamos então que F possui p^m elementos. Consideremos o homomorfismo aditivo $\varphi : F \to F$, definido por $\varphi(a) = a^p - a$, para cada $a \in F$. Como $Im\varphi = \wp F$, segue que $F/ker\varphi \simeq \wp F$. Agora, $ker\varphi$ é justamente o conjunto de todas as raízes, em F, do polinômio $Y^p - Y \in F[Y]$. Assim, $|ker\varphi| = p$ e portanto, $|F/ker\varphi| = p^{m-1}$. Logo, $|F/\wp F| = p$ e então $dim_{\mathbb{Z}/p\mathbb{Z}}(F/\wp F) = 1$. Portanto, $F/\wp F \simeq \mathbb{Z}/p\mathbb{Z}$.

§4. EXEMPLOS E CONSEQÜÊNCIAS

Apresentamos a seguir alguns exemplos, onde daremos uma descrição de $T_n(R)$, para $n \geq 1$. De acordo com o teorema 3.3 e o corolário 3.4, é suficiente apresentarmos uma base de $R/\wp R$ como $\mathbb{Z}/p\mathbb{Z}$–espaço vetorial.

Observemos ainda que o resultado do corolário 3.5 continua válido para qualquer anel R de característica p tal que $dim_{\mathbb{Z}/p\mathbb{Z}}(R/\wp R) = 1$.

EXEMPLO 4.1: Seja $S = R[[X]]$ o anel das séries formais sobre R. Então temos $S/\wp S \simeq R/\wp R$. De fato, dado um elemento $g = \sum_{i\geq 1} c_i X^i \in S$, é claro que $\sum_{j=0}^{\infty} g^{p^j} \in S$ e então $g = (\sum_{j=0}^{\infty} g^{p^j}) - (\sum_{j=0}^{\infty} g^{p^j})^p$. Assim, tomando $f = -\sum_{j=0}^{\infty} g^{p^j} \in S$ temos $g = f^p - f$ de onde segue que $g \in \wp S$. Seja então o homomorfismo $\psi : S \to R/\wp R$, dado por $\psi(\sum_{j=0}^{\infty} a_i X^i) = a_0 + \wp R$ e seja $h \in ker\psi$. Então $h = \sum_{j=0}^{\infty} a_i X^i$ é tal que $a_0 \equiv 0 \pmod{\wp R}$. Logo existe $b_0 \in R$ tal que $b_0^p - b_0 = a_0$ e neste caso, $h = b_0^p - b_0 + \sum_{i\geq 1} a_i X^i \in \wp S$. Portanto, $ker\psi \subseteq \wp S$. A recíproca é clara e segue então que $ker\psi = \wp S$. Assim existe um isomorfismo $\varphi : S/\wp S \to R/\wp R$.

Desta forma, se $(a_i)_{i\in I}$ é uma família de elementos de R tais que $(a_i + \wp R)_{i\in I}$ é uma base de $R/\wp R$ como $\mathbb{Z}/p\mathbb{Z}$–espaço vetorial, então $(a_i + \wp S)_{i\in I}$ é uma base de $S/\wp S$ como $\mathbb{Z}/p\mathbb{Z}$–espaço vetorial.

Em particular, se R é um corpo finito de característica p, segue do corolário 3.5 que $R[[X]]/\wp R[[X]] \simeq \mathbb{Z}/p\mathbb{Z}$.

Antes de apresentarmos o próximo exemplo, veremos um lema que nos será útil.

LEMA 4.2: Seja R um anel de característica p. Então $R/\wp R \simeq \bar{R}/\wp\bar{R}$, onde $\bar{R} = R/N(R)$ e $N(R) = \{r \in R : \exists n \in \mathbb{N} \text{ tal que } r^n = 0\}$.

Prova: Começaremos por observar que para todo $t \in N(R)$ existe um $a \in R$ tal que $a^p - a = t$. De fato, seja $t \in N(R)$. Então existe $n \in \mathbb{N}$ tal que $t^n = 0$. Seja i o menor inteiro tal que $t^{p^i} = 0$. Temos $t = t + t^p - t^p + t^{p^2} - t^{p^2} + \cdots + t^{p^{i-1}} - t^{p^{i-1}} - t^{p^i} = (t + t^p + \cdots + t^{p^{i-1}}) - (t + t^p + \cdots + t^{p^{i-1}})^p = a^p - a$, onde $a = -(t + t^p + \cdots + t^{p^{i-1}})$. Portanto $t \in \wp R$, para todo $t \in N(R)$ e segue daí que $N(R) \subseteq \wp R$.

Consideremos agora os homomorfismos de anéis $\varphi : R \to \bar{R}$, definido por $\varphi(r) = \bar{r} = r + N(R)$, para todo $r \in R$ e $\psi : \bar{R} \to \bar{R}/\wp\bar{R}$, dado por $\psi(\bar{r}) = [\bar{r}]$, para todo $\bar{r} = r + N(R) \in \bar{R}$, onde $[\bar{r}] = \bar{r} + \wp\bar{R}$. Consideremos também a composição destes homomorfismos $\varphi* = \psi \circ \varphi : R \to \bar{R}/\wp\bar{R}$. Assim $\varphi*$ é um homomorfismo sobrejetor.

Seja $r \in ker\varphi*$. Então $\varphi*(r) = [\bar{r}] = [\bar{0}]$. Logo existe $\bar{s} = \in \bar{R}$ tal que $\bar{r} = \bar{s}^p - \bar{s}$ e assim existe um $t \in N(R)$, tal que $r = s^p - s + t$. Como $N(R) \subseteq \wp R$ temos $t = a^p - a$,

para algum $a \in R$. Logo $r = s^p - s + t = s^p - s + a^p - a = (s+a)^p - (s+a) \in \wp R$ e segue daí que $ker\varphi* \subseteq \wp R$.

Agora dado $r \in \wp R$ temos $\varphi*(r) = \psi \circ \varphi(r) = \psi(r + N(R)) = [\bar{0}]$, pois $N(R) \subseteq \wp R$. Logo $ker\varphi* = \wp R$ e portanto $\varphi*$ induz um isomorfismo $\bar{\varphi} : R/\wp R \to \bar{R}/\wp\bar{R}$. Isto completa a prova do lema.

OBSERVAÇÃO 4.3: Segue deste lema que $T_n(R) \simeq T_n(\bar{R})$, se R é um anel de característica p. Este resultado vale em geral. De fato, C. Greither e R. Haggenmüller em [10] mostraram que $T(G,R) \simeq T(G,\bar{R})$, para todo grupo abeliano G, onde $\bar{R} = R/N(R)$.

Gostaríamos de lembrar ainda que $R/N(R)$ é um anel sem elementos nilpotentes próprios e que $R[X]$ possui elementos nilpotentes próprios se e somente se R possui elementos nilpotentes próprios. Podemos agora apresentar nosso próximo exemplo.

EXEMPLO 4.4: Seja $S = R[X]$ o anel de polinômios na indeterminada X. Queremos encontrar uma base de $S/\wp S$ como $\mathbb{Z}/p\mathbb{Z}$–espaço vetorial. Do lema anterior segue que podemos supor R um anel sem elementos nilpotentes.

Tomando $R^p = \{r^p : r \in R\}$ é fácil ver que R^p é um $\mathbb{Z}/p\mathbb{Z}$–subespaço vetorial de R. Seja $(b_j)_{j\in J'}$ uma base de R^p sobre $\mathbb{Z}/p\mathbb{Z}$ e sejam $c_j \in R$ elementos tais que $b_j = c_j^p$, para todo $j \in J'$. Extendendo esta base a uma base $(b_j)_{j\in J'} \cup (b_j)_{j\in J''}$ de R como $\mathbb{Z}/p\mathbb{Z}$–espaço vetorial e tomando $J = J' \cup J''$, definimos:

$(*)$ $B_0 = \{a_i + \wp S : i \in I\}$, onde $(a_i + \wp R)_{i\in I}$ é uma base de $R/\wp R$ como $\mathbb{Z}/p\mathbb{Z}$–espaço vetorial;

$(**)$ $B_k = \{b_j X^k + \wp S : j \in J\}$, se $(k,p) = 1$ e $k \geq 1$;

$(***)$ $B_k = \{b_j X^k + \wp S : j \in J''\}$, se $(k,p) = p$ e $k \geq 1$.

Afirmamos que $B = \bigcup_{k=0}^{\infty} B_k$ é uma base de $S/\wp S$ como $\mathbb{Z}/p\mathbb{Z}$– espaço vetorial. Mostraremos isto a seguir.

Precisamos ver que B é um sistema de geradores de $S/\wp S$ e que é linearmente independente sobre $\mathbb{Z}/p\mathbb{Z}$.

Para a primeira parte, é suficiente mostrar que $cX^i + \wp S$ é uma combinação linear finita de elementos de $B = \bigcup_{k=0}^{\infty} B_k$, para todo $c \in R$, $i \in \mathbb{N}$. Faremos isto por indução em i.

Se $i = 0$ o resultado segue trivialmente. Suponhamos que para todo $i < l$, cX^i é combinação linear de elementos de B e mostremos que cX^l também o é.

Como $c \in R$, temos que $c = \sum_{j \in J} \lambda_j b_j$, onde $\lambda_j \in \mathbb{Z}/p\mathbb{Z}$, para todo $j \in J$ e $\lambda_j \neq 0$ somente para um número finito de valores de $j \in J$. Temos então, $cX^l + \wp S = \sum_{j \in J} \lambda_j b_j X^l + \wp S = \sum_{j \in J'} \lambda_j b_j X^l + \wp S + \sum_{j \in J''} \lambda_j b_j X^l + \wp S$.

Suponhamos $(l,p) = 1$, então $cX^l + \wp S = \sum_{j \in J} \lambda_j b_j X^l + \wp S = \sum_{j \in J} \lambda_j b_j X^l + \wp S)$ que é uma combinação linear de elementos B, do tipo $(**)$. Agora, se $(l,p) = p$ então $l = kp$, para algum $k \in \mathbb{Z}$. Neste caso, $cX^l + \wp S = \sum_{j \in J'} \lambda_j b_j X^l + \wp S + \sum_{j \in J''} \lambda_j b_j X^l + \wp S = (\sum_{j \in J'} \lambda_j b_j X^{kp} + \sum_{j \in J''} \lambda_j b_j X^{kp}) + \wp S = [\sum_{j \in J'} (\lambda_j c_j X^k)^p + \sum_{j \in J''} \lambda_j b_j X^{kp}] + \wp S = \sum_{j \in J'} \lambda_j (c_j X^k + \wp S) + \sum_{j \in J''} \lambda_j (b_j X^{kp} + \wp S)$. Assim, o segundo somatório é uma combinação linear de elementos de B, do tipo $(***)$ e o primeiro, é também uma combinação linear de elementos de B, por hipótese de indução. Portanto, $cX^l + \wp S$ é uma combinação linear de elementos de B, e assim $B = \bigcup_{k=0}^{\infty} B_k$ é um sistema de geradores de $S/\wp S$ como $\mathbb{Z}/p\mathbb{Z}$– espaço vetorial.

Para ver que B é linearmente independente tomamos uma combinação linear finita do tipo $\sum_{j,k} (\lambda_{jk} b_j X^k + \wp S) = 0$ em $S/\wp S$. Então $\sum_{j,k} \lambda_{jk} b_j X^k = \sum_{i \in I} \lambda_{i0} a_i + \sum_{\substack{k=1 \\ (k,p)=1}}^{m} \sum_{j \in J'} \lambda_{jk} b_j X^k + \sum_{\substack{k=1 \\ (\lambda,p)=p}}^{m} \sum_{j \in J''} \lambda_{jk} b_j X^k = f^p - f$, para algum $f \in R[X]$. Suponhamos $f = \sum_{l=0}^{n} d_l X^l$, com $d_n \neq 0$.

Se $n = 0$, então $\sum_{i \in I} \lambda_{i0} a_i = d_0^p - d_0 \in \wp R$. Isto implica que $\sum_{i \in I} \lambda_{i0} (a_i + \wp S) = 0$, de onde resulta $\lambda_{i0} = 0$, para todo $i \in I$, pela escolha dos elementos a_i $(i \in I)$. A prova está completa neste caso.

Se $n > 0$, comparando os termos de maior grau na igualdade $\sum_{i \in I} \lambda_{i0} a_i + \sum_{k=1}^{m} (\sum_{j \in J'} \lambda_{jk} b_j X^k + \sum_{j \in J''} \lambda_{jk} b_j X^k) = (\sum_{l=0}^{n} d_l X^l)^p - (\sum_{l=0}^{n} d_l X^l)$, obtemos $\sum_{j \in J''} \lambda_{jm} b_j X^m = d_n^p X^{np}$, uma vez que $m = np$ e portanto a soma $\sum_{j \in J'} \lambda_{jk} b_j X^k$ não aparece neste caso. Segue daí que $\sum_{j \in J''} \lambda_{jm} b_j = d_n^p \in R^p \cap \sum_{j \in J''} R b_j = 0$, de onde resulta $d_n^p = 0$ o que é uma contradição com o fato de R não possuir elementos nilpotentes próprios. Portanto, $B = \bigcup_{k=0}^{\infty} B_k$ é um sistema de geradores linearmente independente de $S/\wp S$, isto é, é uma base de $S/\wp S$

como $\mathbb{Z}/p\mathbb{Z}$– espaço vetorial, como queríamos mostrar.

EXEMPLO 4.5: Seja F um corpo de característica p e $S = F((X))$ o corpo das séries formais sobre F, isto é, S é o corpo de fraçoes do domínio de integridade $F[[X]]$. É fácil ver que $S = \{\sum_{i \geq n} a_i X^i : a_i \in F,\ n \in \mathbb{Z}\}$.

Consideremos o $\mathbb{Z}/p\mathbb{Z}$–subespaço vetorial $I = \{\sum_{i \geq 1} a_i X^i : a_i \in F\}$ de S. Por um cálculo semelhante ao do exemplo 4.1, obtemos $I = \wp I$. É fácil ver ainda que $S/I \simeq F[X^{-1}] \simeq F[t]$, onde t é uma indeterminada sobre F. Mostraremos que $S/\wp S \simeq (S/I)/\wp(S/I) \simeq F[t]/\wp F[t]$ e então podemos construir uma base de $S/\wp S$ como $\mathbb{Z}/p\mathbb{Z}$–espaço vetorial analogamente ao exemplo anterior.

Seja $f = \sum_{i \geq 1} a_i X^i \in \wp S$. Temos $f^p - f = (\sum_{i \leq 0} a_i X^i + \sum_{i \geq 1} a_i X^i)^p - (\sum_{i \leq 0} a_i X^i + \sum_{i \geq 1} a_i X^i) \equiv (\sum_{i \leq 0} a_i X^i)^p - (\sum_{i \leq 0} a_i X^i) \pmod{\wp I}$. Logo, $\wp S/I \simeq \wp F[X^{-1}]$. Segue daí que $S/\wp S \simeq \frac{S/I}{\wp S/I} \simeq \frac{F[X^{-1}]}{\wp F[X^{-1}]} \simeq \frac{F[t]}{\wp F[t]}$, como queríamos mostrar.

Vamos dar agora algumas conseqüências dos resultados obtidos neste capítulo.

Dado $[A, \sigma] \in T_n(R)$, uma extensão p^n– cíclica de R, segue do corolário 2.2 e teorema 2.1 que $B = A^{\sigma^{p^{n-1}}}$ é uma extensão p^{n-1}– cíclica de R, com grupo de Galois (σ/B). É fácil ver que se $(A, \sigma) \simeq (A', \sigma')$ então $(B, \sigma/B) \simeq (B', \sigma'/B')$, onde $B = A^{\sigma^{p^{n-1}}}$ e $B' = A'^{\sigma'^{p^{n-1}}}$. Podemos então definir uma aplicação $\psi : T_n(R) \to T_{n-1}(R)$, pondo $\psi([A, \sigma]) = [B, \sigma/B] \in T_{n-1}(R)$, para cada $[A, \sigma] \in T_n(R)$. Denotando $K_n(R) = ker\psi$ e $\varphi : K_n(R) \hookrightarrow T_n(R)$ a inclusão canônica, obtemos a seguinte seqüência exata:

$$0 \to K_n(R) \xrightarrow{\varphi} T_n(R) \xrightarrow{\psi} T_{n-1}(R) \to 0 \tag{4.6}$$

Queremos mostrar que $K_n(R) \simeq T_1(R)$. Antes porém, faremos algumas observações. Denotaremos por $(E_n(R), \rho_n)$ o elemento neutro de $T_n(R)$. Conforme parágrafo 5 do capítulo II, $E_n(R) = \bigoplus_{i=0}^{p^n-1} Re_i$, onde $\{e_i\}_{0 \leq i \leq p^n-1}$ é uma família de idempotentes ortogonais cuja soma é um, e a ação de ρ_n é dada por $\rho_n(e_i) = e_{i+1 \pmod{p^n}}$. Pelo que vimos neste capítulo, sendo que o elemento neutro de $w_n(R)$ é $[0, \ldots, 0]$, segue que $(E_n(R), \rho_n) \simeq (R[X]/(X^\pi - X), \tau_n)$, onde $X = (X_0, \ldots, X_{n-1})$ é um conjunto de indeterminadas sobre R e $\tau_n(x) = x + 1$, com $x = (x_0, \ldots, x_{n-1})$ e $x_i = X_i + (X^\pi - X)$, $0 \leq i \leq n-1$.

Observemos que o ideal $(X^\pi - X)$ de $R[X]$ é igual ao ideal gerado por $(X_0^p - X_0, \ldots, X_{n-1}^p - X_{n-1})$. De fato, seja $I = (X^\pi - X)$ e $J = (X_0^p - X_0, \ldots, X_{n-1}^p - X_{n-1})$. Então, $X^\pi - X = (X_0^p, \ldots, X_{n-1}^p) - (X_0, \ldots, X_{n-1}) = (X_0^p, 0, \ldots, 0) - (X_0, 0, \ldots, 0) + (0, X_1^p, \ldots, X_{n-1}^p) - (0, X_1, \ldots, X_{n-1}) \equiv (0, X_1^p, \ldots, X_{n-1}^p) - (0, X_1, \ldots, X_{n-1}) \pmod{J}$. Proceguindo este raciocínio, obtemos $X^\pi - X \equiv 0 \pmod{J}$, isto é, $I \subseteq J$.

Reciprocamente, $X^\pi - X \equiv 0 \pmod{I}$, implica que $X^\pi \equiv X \pmod{I}$ e conseqüêntemente $X_i^p \equiv X_i \pmod{I}$, $0 \leq i \leq n-1$. Portanto, $(X_0^p - X_0, \ldots, X_{n-1}^p - X_{n-1}) \equiv 0 \pmod{I}$ e assim, $J \subseteq I$.

Assim, escrevemos $(E_n(R), \rho_n) \simeq (R[X_0, \ldots, X_{n-1}]/(X_0^p - X_0, \ldots, X_{n-1}^p - X_{n-1}), \tau_n)$ onde $\tau_n(x_0, \ldots, x_{n-1}) = (x_0, \ldots, x_{n-1}) + 1$ e $x_i = X_i + (X_0^p - X_0, \ldots, X_{n-1}^p - X_{n-1})$, $0 \leq i \leq n-1$.

Observemos também que $K_n(R)$ é o conjunto de todos os elementos $[A, \sigma] \in T_n(R)$ tais que $[B, \sigma/B] = [E_{n-1}(R), \rho_{n-1}]$, onde $B = A^{\sigma^{p^{n-1}}}$.

Dado $[C, \eta] \in T_1(R)$, existe $a \in R$ tal que $\theta_1([C, \eta]) = [a]$, isto é, $C \simeq R[X]/(X^p - X - a)$ e $\eta(X + (X^p - X - a)) = X + 1 + (X^p - X - a)$. Assim, associamos com $[C, \eta] \in T_1(R)$ a classe $[A, \sigma] \in K_n(R)$ tal que

$$\begin{aligned}(A, \sigma) &\simeq (R[X]/(X^\pi - X - (0, \ldots, 0, a)), \tau) \\ &\simeq \left(\frac{R[X_0, \ldots, X_{n-1}]}{(X_0^p - X_0, \ldots, X_{n-2}^p - X_{n-2}, X_{n-1}^p - X_{n-1} - a)}, \tau\right)\end{aligned}$$

onde τ atua da forma $\tau(x_0, \ldots, x_{n-1}) = (x_0, \ldots, x_{n-1}) + 1$, com $x_i = X_i + (X_0^p - X_0, \ldots, X_{n-2}^p - X_{n-2}, X_{n-1}^p - X_{n-1} - a)$. Pode-se ver que a aplicação $T_1(R) \to K_n(R)$, assim definida, é um isomorfismo.

No que segue identificaremos $K_n(R)$ com $T_1(R)$ via este isomorfismo. Com esta identificação, a seqüência (4.6) se torna equivalente a seguinte seqüência:

$$0 \longrightarrow T_1(R) \xrightarrow{\varphi} T_n(R) \xrightarrow{\psi} T_{n-1}(R) \longrightarrow 0 \qquad (4.7)$$

O seguinte resultado é claro.

PROPOSIÇÃO 4.8: O seguinte diagrama é comutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_1(R) & \xrightarrow{\varphi} & T_n(R) & \xrightarrow{\psi} & T_{n-1}(R) & \longrightarrow & 0 \\ & & \downarrow \theta_1 & & \downarrow \theta_n & & \downarrow \theta_{n-1} & & \\ 0 & \longrightarrow & w_1(R) & \xrightarrow{\varphi'} & w_n(R) & \xrightarrow{\psi'} & w_{n-1}(R) & \longrightarrow & 0 \end{array}$$

onde $\varphi' : w_1(R) \longrightarrow w_n(R)$ é dado por $\varphi'([a]) = [0, \ldots, 0, a]$, para todo $[a] \in w_1(R)$ e $\psi' : w_n(R) \longrightarrow w_{n-1}(R)$ é dado por $\psi'([a_0, \ldots, a_{n-1}]) = [a_0, \ldots, a_{n-2}]$, para todo $[a_0, \ldots, a_{n-1}] \in w_n(R)$.

COROLÁRIO 4.9: Com as mesmas notações anteriores temos:

(i) Se $T_1(R) = 0$, então $T_n(R) = 0$ para todo $n \geq 1$.

(ii) Se $T_1(R) \neq 0$, então $T_n(R)$ contém um elemento de ordem p^n. Neste caso a seqüência (4.7) não cinde.

Prova: *(i)* Se $T_1(R) = 0$ então, por (4.7), temos $T_n(R) \simeq T_{n-1}(R)$, para todo $n \geq 1$. Assim $T_n(R) = 0$, para todo $n \geq 1$, segue por indução.

(ii) Só temos que mostrar que se $T_1(R) \neq 0$ então a seqüência (4.7) não cinde. Isto é claro pois se $T_n(R) \simeq T_1(R) \oplus T_{n-1}(R)$, todo elemento de $T_n(R)$ teria ordem aditiva divisor de p^{n-1}, o que é um absurdo.

Pelo teorema 3.2 existe um elemento de ordem p^n em $T_n(R)$, para $n \geq 1$. Nosso próximo resultado nos auxilia a encontrar tais elementos.

PROPOSIÇÃO 4.10: Suponhamos que $T_1(R)$ é um $\mathbb{Z}/p\mathbb{Z}$-espaço vetorial não trivial e seja $a \in R$. Então $[a]$ tem ordem aditiva p em $w_1(R)$ se e somente se $[a, a_1, \ldots, a_{n-1}]$ tem ordem aditiva p^n em $w_n(R)$, para todos $a_1, \ldots, a_{n-1} \in R$.

Prova: Se $0 = p^{n-1}[a, a_1, \ldots, a_{n-1}] = v^{n-1}([a, a_1, \ldots, a_{n-1}]) = [0, \ldots, 0, a]$. segue que $(0, \ldots, 0, a) = b^\pi - b$, para algum $b = (b_0, \ldots, b_{n-1}) \in W_n(R)$. Assim $(0, \ldots, 0, a) = (b_0, \ldots, b_{n-1})^\pi - (b_0, \ldots, b_{n-1}) = (b', 0)^\pi - (b', 0) + (0, \ldots, 0, b_{n-1}^p) - (0, \ldots, 0, b_{n-1})$. Aplicando o homomorfismo projeção canônica $\varphi : W_n(R) \longrightarrow W_{n-1}(R)$, ao primeiro e ao último membros da igualdade acima, obtemos $b'^\pi - b' = 0$ em $W_{n-1}(R)$, isto é, $b_i^p = b_i$ para todo $0 \leq i \leq n-2$. Assim, $(0, \ldots, 0, a) = (0, \ldots, 0, b_{n-1}^p) - (0, \ldots, 0, b_{n-1}) = (0, \ldots, 0, b_{n-1}^p - b_{n-1})$ e então $a = b_{n-1}^p - b_{n-1} \in \wp R$.

Logo, se $[a]$ tem ordem aditiva p em $w_1(R)$, $a \notin \wp R$ e então $p^{n-1}[a, a_1, \ldots, a_{n-1}] \neq 0$. Isto implica que $[a, a_1, \ldots, a_{n-1}]$ tem ordem p^n em $w_n(R)$.

Reciprocamente, se $[a, a_1 \ldots, a_{n-1}]$ tem ordem aditiva p^n em $w_n(R)$, segue que $p^{n-1}[a, a_1, \ldots, a_{n-1}] \neq 0$. Facilmente se verifica que $[a]$ tem ordem p em $w_1(R)$.

Apresentaremos a seguir dois lemas. As respectivas provas serão omitidas para não nos extendermos demasiadamante. O leitor interessado poderá obtê-las em ([15], lema 1.2 e teorema 1.8(2), respectivamente).

LEMA 4.11: Seja R um anel sem idempotentes próprios e $f(X) = X^p - X - r_0 \in R[X]$. Então $f(X)$ é irredutível se e somente se $f(r) \neq 0$, para todo $r \in R$.

LEMA 4.12: Seja (A, σ) uma p^n– extensão cíclica de R e R_1 o anel fixo de A por (σ^p). Então A é um corpo se e somente se R_1 é um corpo.

Com o auxílio destes lemas, podemos provar o seguinte resultado, o qual caracteriza os elementos de ordem p^n em $T_n(F)$, quando F é um corpo de característica p.

PROPOSIÇÃO 4.13: Sejam F um corpo de característica p e $a = (a_0, \ldots, a_{n-1}) \in W_n(F)$. Seja (A_a, τ) a extensão p^n– cíclica canônica de F associada com a. Então as seguintes condições são equivalentes:

(i) $X_0^p - X_0 - a_0 \in F[X_0]$ é irredutivel;

(ii) A_a é um corpo;

(iii) $[A_a, \tau]$ é um elemento de ordem p^n em $T_n(F)$.

Prova: Segue do corolário 2.2 que $A_a^{\sigma^p} = F[x_0] \simeq F[X_0]/(X_0^p - X_0 - a_0)$. Então a equivalência (i) $\Leftrightarrow$ (ii) segue do lema 4.12.

A equivalência (i) $\Leftrightarrow$ (iii) é conseqüência do lema 4.11 e da proposição 4.10. Basta observar que $a_0 \notin \wp F$ se e somente se $X_0^p - X_0 - a_0$ não possui raízes em F.

Como aplicação dos resultados anteriores obtemos a seguir o grupo de Harrison do anel R/pR onde R é um anel qualquer e pR é o ideal de R definido por $pR = \{pr : r \in R\}$. Este foi obtido por M. Ferrero e A. Paques mas não está publicado.

Se R é um anel e p um número primo, denotamos por $W_n(pR)$ o conjunto de vetores de Witt de $W_n(R)$ cujas componentes estão em pR. Seja $W = \wp W_n(R) + W_n(pR) \subseteq W_n(R)$ o conjunto de todas as somas $x + y$, com $x \in \wp W_n(R)$ e $y \in W_n(pR)$, onde, como antes, $\wp W_n(R) = \{a^\tau - a : a \in W_n(R)\}$.

Consideremos agora o anel $\bar{R} = R/pR$. Assim, $\bar{R}$ é um anel de característica p. Seja ainda, $T_n(\bar{R}) = T(\mathbb{Z}/p^n\mathbb{Z}, \bar{R})$. Temos então o seguinte

COROLÁRIO 4.14: Com as mesmas notações acima, W é um subgrupo de $W_n(R)$ e $T_n(\bar{R}) \simeq W_n(R)/W$.

Prova: Consideremos a projeção canônica $g : R \longrightarrow \bar{R}$ e sua extensão natural $g : W_n(R) \longrightarrow W_n(\bar{R})$. É claro que g comuta com π. Vejamos agora que $ker g = W_n(pR)$. É evidente que $W_n(pR) \subseteq ker g$. Consideremos então $a = (a_0, \ldots, a_{n-1}) \in ker g$. Assim, $0 = g(a) = (g(a_0), \ldots, g(a_{n-1}))$. Segue daí que $g(a_i) = 0$ em $\bar{R}$, para todo $0 \leq i \leq n-1$,

ou seja, $a = (a_0, \ldots, a_{n-1}) \in W_n(pR)$.

Consideremos ainda a projeção canônica $g' : W_n(R) \longrightarrow w_n(R)$ e seja $\varphi = g' \circ g$. Então $\varphi : W_n(R) \longrightarrow w_n(R)$ é um homomorfismo sobrejetor e temos $w_n(R) \simeq W_n(R)/ker\varphi$. Vamos mostrar então que $ker\varphi = W$, o que completa a prova do corolário.

A inclusão $W \subseteq ker\varphi$ é clara. Seja $a = (a_0, \ldots, a_{n-1}) \in ker\varphi$. Então $\varphi(a) = [\bar{0}]$ em $w_n(R)$, isto é, $g' \circ g(a) = g'(g(a)) = [\bar{0}]$. Isto implica que $g(a) \in kerg' = \wp W_n(R)$. Assim, existe $\bar{b} \in \wp W_n(R)$ tal que $g(a) = \bar{b}^\pi - \bar{b}$. Agora, como g é sobrejetora, existe $b \in W_n(R)$ tal que $\bar{b} = g(b)$. Desta forma, $g(a) = g(b)^\pi - g(b) = g(b^\pi - b)$, pois g comuta com π. Portanto $g(a - (b^\pi - b)) = 0$ em $W_n(R)$. Isto implica que $a - (b^\pi - b) \in kerg = W_n(pR)$. Logo, $a \in \wp W_n(R) + W_n(pR)$, o que mostra que $kerg \subseteq W$.

OBSERVAÇÃO: O fato de W ser um subgrupo de $W_n(R)$, para um anel qualquer R, é um pouco surpreendente, mas pode ser obtido também diretamente, independente do corolário anterior, como aplicação dos resultados do apêndice (Lema A.1 e corolário A.5).

APÊNDICE - ANÉIS DE VETORES DE WITT

Introduziremos aqui os anéis de vetores de Witt sobre um anel comutativo A. O caso que mais nos interessa é quando A é um anel de característica p, onde p é um primo. Contudo, começaremos por definir os vetores de Witt sobre um anel contendo o corpo dos racionais. Nesta exposição seguiremos D.J. Winter [20,apêndice W] e P. Ribemboim [18].

Consideremos então um anel A tal que $\mathbb{Q} \subseteq A$, onde $\mathbb{Q}$ denota o corpo dos números racionais. Sejam p um número primo e n um número inteiro positivo. Consideremos o anel comutativo $(A^n, +, \cdot)$, onde $A^n = A \times A \times \cdots \times A$ (n fatores), $+$ e $\cdot$ são as operações usuais de soma e produto, definidas componente à componente.

Consideremos agora a aplicação $\gamma : A^n \to A^n$, definida por $\gamma(a_0, \ldots, a_{n-1}) = (a_0, a_0^p + pa_1, a_0^{p^2} + pa_1^p + p^2a_2, \ldots, a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-1}a_{n-1})$, para todo $(a_0, \ldots, a_{n-1})$ de A^n. Do fato de p ser inversível em A segue que, para cada $(b_0, \ldots, b_{n-1}) \in A^n$, existem únicos $a_0, \ldots, a_{n-1} \in A$ tais que:

$$\begin{cases} a_0 & = b_0 \\ a_0^p + pa_1 & = b_1 \\ \quad \vdots & \vdots \quad \vdots \\ a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \ldots + p^{n-1}a_{n-1} & = b_{n-1} \end{cases}$$

como é fácil verificar. Segue então que γ é uma bijeção. Logo, podemos definir duas novas operações em A^n como segue: Dados $a = (a_0, \ldots, a_{n-1})$, $b = (b_0, \ldots, b_{n-1}) \in A^n$, existe um único $c = (c_0, \ldots, c_{n-1}) \in A^n$, tal que $\gamma(c) = \gamma(a) + \gamma(b)$. Definimos então $a \oplus b = c$. De maneira análoga, definimos $a \odot b$. Desta forma, as propriedades das operações $+$ e $\cdot$ se transportam para as operações $\oplus$ e $\odot$, via a aplicação γ, como é fácil ver. Assim, $(A^n, \oplus, \odot)$ é um anel comutativo, o qual será chamado ANEL DE VETORES DE WITT SOBRE A, com respeito à p, e será denotado por $W_n(A)$. Observemos que a estrutura do anel $W_n(A)$ foi definida de tal forma que a aplicação $\gamma : W_n(A) \to A^n$ é um isomorfismo de anéis.

Da definição de $\oplus$ e $\odot$ segue facilmente que $\mathbf{1} = (1, 0 \ldots, 0) \in W_n(A)$ e $\mathbf{0} = (0, \ldots, 0) \in W_n(A)$, são a unidade e o elemento zero do anel $W_n(A)$, respectivamente.

Observamos ainda que se $\varphi : A \to A$ é um endomorfismo de anéis, então também o é $\varphi^* : A^n \to A^n$ dado por $\varphi^*(a_0, \ldots, a_{n-1}) = (\varphi(a_0), \ldots, \varphi(a_{n-1}))$. Este último se extende

naturalmente a um endomorfismo φ^{**} de $W_n(A)$, pois o diagrama abaixo comuta

$$\begin{array}{ccc} A^n & \xrightarrow{\varphi^*} & A^n \\ \gamma^{-1} \downarrow & & \downarrow \gamma^{-1} \\ W_n(A) & \xrightarrow{\varphi^{**}} & W_n(A) \end{array}$$

onde $\varphi^{**} = \gamma^{-1} \circ \varphi^* \circ \gamma$. Desta forma, $\varphi^{**}(a_0, \ldots, a_{n-1}) = (\varphi(a_0), \ldots, \varphi(a_{n-1}))$, para todo $(a_0, \ldots, a_{n-1}) \in W_n(A)$. Por simplicidade de notação, escreveremos φ em lugar de φ^{**}

Dado $a = (a_0, \ldots, a_{n-1}) \in W_n(A)$, notaremos por $[a^{(0)}, \ldots, a^{(n-1)}]$ o elemento $\gamma(a) = (a_0, a_0^p + pa_1, \ldots, a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-1}a_{n-1}) \in A^n$. Assim, dados $a = (a_0, \ldots, a_{n-1})$, $b = (b_0, \ldots, b_{n-1}) \in W_n(A)$, temos $\gamma(a) = [a^{(0)}, \ldots, a^{(n-1)}]$, $\gamma(b) = [b^{(0)}, \ldots, b^{(n-1)}]$ e então $[(a \oplus b)^{(0)}, \ldots, (a \oplus b)^{(n-1)}] = \gamma(a \oplus b) = \gamma(a) + \gamma(b) = [a^{(0)}, \ldots, a^{(n-1)}] + [b^{(0)}, \ldots, b^{(n-1)}]$, ou seja, $(a+b)^{(i)} = a^{(i)} + b^{(i)}$, para todo $0 \leq i \leq n-1$. Analogamente, $(ab)^{(i)} = a^{(i)}b^{(i)}$, para todo $0 \leq i \leq n-1$.

A partir de agora notaremos $\oplus$ e $\odot$ por $+$ e $\cdot$, respectivamente, pois estaremos sempre operando em $W_n(A)$.

Dado $a = (a_0, \ldots, a_{n-1}) \in W_n(A)$, existem elementos $a'^{(0)}, \ldots, a'^{(n-1)} \in A$ tais que $(a_0, \ldots, a_{n-1}) = [a'^{(0)}, \ldots, a'^{(n-1)}]$, pois γ é bijeção. Neste caso temos

$$a'^{(0)} = a_0 \quad \text{e também} \quad a'^{(i)} = a_0^{p^i} + pa_1^{p^{i-1}} + \cdots + p^i a_i, \ 1 \leq i \leq n-1$$

ou, equivalentemente

$a_0 = a'^{(0)}$, e

$a_i = 1/p^i[a'^{(i)} - (a_0^{p^{i-1}} + pa_1^{i-2} + \cdots + p^{i-1}a_{i-1}^p)]$, $1 \leq i \leq n-1$.

Vamos determinar agora, com auxílio das fórmulas acima, algumas componentes de $a+b$ e ab. Sejam $a = (a_0, \ldots, a_{n-1})$, $b = (b_0, \ldots, b_{n-1}) \in W_n(A)$, temos $a+b = ((a+b)_0, \ldots, (a+b)_{n-1})$ e $ab = ((ab)_0, \ldots, (ab)_{n-1})$, onde:

$(a+b)_0 = (a+b)^{(0)} = a^{(0)} + b^{(0)} = a_0 + b_0$

$(a+b)_1 = 1/p[(a+b)^{(1)} - (a+b)_0^p] = 1/p(a^{(1)} + b^{(1)} - (a_0+b_0)^p) = 1/p(a_0^p + pa_1 + b_0^p +$

$pb_1^p - (a_0+b_0)^p) = a_1 + b_1 + 1/p(a_0^p + b_0^p - (a_0+b_0)^p) = a_1 + b_1 - \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} a_0^{p-i} b_0^i$

onde $\binom{p}{i}$ indica os números combinatórios correspondentes e $\frac{\binom{p}{i}}{p} \in \mathbb{Z}$, pois $i \neq 0$.

Da mesma maneira:

$(ab)_0 = a_0 b_0$

$(ab)_1 = a_0^p b_1 + a_1 b_0^p + p a_1 b_1$

Poderíamos naturalmente tentar calcular todas as componentes de $a+b$ e ab, para $a, b \in W_n(A)$, mas estes cálculos são muito difíceis.

Observamos que as duas primeiras componentes de $a+b$ e ab em $W_n(A)$ são polinômios com coeficientes inteiros nas componentes de a e b. Mostraremos mais adiante que todas as componentes de $a+b$ e ab em $W_n(A)$ são dadas por polinômios com coeficientes inteiros. Estes polinômios serão utilizados para definir o anel de vetores de Witt sobre um anel de característica p, pois neste caso, $(A^n, +, \cdot)$ não será isomorfo à $(A^n, \oplus, \odot)$. Antes porém, definiremos dois operadores que nos serão úteis no decorrer deste apêndice.

Sejam $\pi : W_n(A) \to W_n(A)$, definido por $\pi(a) = a^\pi = (a_0^p, \ldots, a_{n-1}^p)$ e $V : W_n(A) \to W_n(A)$, dado por $V(a_0, \ldots, a_{n-1}) = (0, a_0, \ldots, a_{n-2})$, para todo $(a_0, \ldots, a_{n-1}) \in W_n(A)$. Estes operadores são chamados operador p-ésima potência e operador translação, respectivamente. Convém observar que $V \circ \pi = \pi \circ V$, como é fácil verificar.

Da definição do operador π segue que, se $(a_0, \ldots, a_{n-1}), [a^{(0)}, \ldots, a^{(n-1)}] \in W_n(A)$, então temos $a_0 = a^{(0)}$ e $a^{(i+1)} = (a^\pi)^{(i)} + p^{i+1} a_{i+1}$, $0 \leq i \leq n-2$, como é fácil verificar.

Observemos ainda que, para $a, b \in A$, onde A é um anel qualquer, temos $a \equiv b \pmod{p^r A}$ implica $a^p \equiv b^p \pmod{p^{r+1} A}$, onde r é um número inteiro positivo e p um primo qualquer. De fato, se $a \equiv b \pmod{p^r A}$, então existe $a' \in A$ tal que $a = b + p^r a'$. Assim, $a^p = (b + p^r a')^p = b^p + \sum_{i=1}^{p} \binom{p}{i} b^{p-i} p^{ir} a'^i = b^p + p^{r+1} a''$, onde $a'' = b^{p-1} a' + \sum_{i=2}^{p} \binom{p}{i} b^{p-i} p^{ir-(r+1)} a'^i \in A$. Assim, $a \equiv b \pmod{p^{r+1} A}$.

Estamos em condições de provar o seguinte

LEMA A.1: Sejam $a = (a_0, \ldots, a_{n-1})$, $b = (b_0, \ldots, b_{n-1})$ elementos de $W_n(A)$, e seja $j > 0$ e $0 \leq k \leq n-1$. Então as seguintes condições são equivalentes:

(a) $a_i \equiv b_i \pmod{p^j A}$, $0 \leq i \leq k$

(b) $a^{(i)} \equiv b^{(i)} \pmod{p^{j+i} A}$, $0 \leq i \leq k$

Prova: Faremos a prova deste lema por indução com respeito a k. Para $k = 0$ a equivalência é trivial.

Para mostrar que (a) implica (b), faremos a seguinte hipótese de indução: Suponhamos que $a_i \equiv b_i \pmod{p^j A}$ $(0 \leq i \leq k)$ implica $a^{(i)} \equiv b^{(i)} \pmod{p^{j+i} A}$ $(0 \leq i \leq k)$. Temos que mostrar então que se $a_i \equiv b_i \pmod{p^j A}$, $0 \leq i \leq k+1$ então $a^{(k+1)} \equiv b^{(k+1)}$

$(\text{mod } p^{j+k+1}A)$.

Suponhamos então que $a_i \equiv b_i \pmod{p^jA}$, $0 \leq i \leq k+1$. Segue daí que $a_i^p \equiv b_i^p \pmod{p^{j+1}A}$, $0 \leq i \leq k+1$. Como $a_i^p = (a^\pi)_i$, para todo $0 \leq i \leq n-1$, decorre da hipótese de indução que $(a^\pi)^{(i)} \equiv (b^\pi)^{(i)} \pmod{p^{j+i+1}A}$, $0 \leq i \leq k$. Assim, $a^{(k+1)} - b^{(k+1)} = (a^\pi)^{(k)} - (b^\pi)^{(k)} + p^{k+1}(a_{k+1} - b_{k+1}) \equiv p^{k+1}(a_{k+1} - b_{k+1}) \equiv 0 \pmod{p^{j+k+1}A}$, como queríamos provar.

Para provar a recíproca, faremos a seguinte hipótese de indução: Suponhamos que $a^{(i)} \equiv b^{(i)} \pmod{p^{j+i}A}$, $0 \leq i \leq k$, implica $a_i \equiv b_i \pmod{p^jA}$, $0 \leq i \leq k$. Para mostrar que (b) implica (a), analogamente ao anterior, basta mostrarmos que $a^{(i)} \equiv b^{(i)} \pmod{p^{j+i}A}$, $0 \leq i \leq k$, implica $a_{k+1} \equiv b_{k+1} \pmod{p^jA}$.

Suponhamos então que $a^{(i)} \equiv b^{(i)} \pmod{p^{j+i}A}$, $0 \leq i \leq k+1$. De $a^{(i)} \equiv b^{(i)} \pmod{p^{j+i}A}$, $0 \leq i \leq k$, segue por indução que $a_i \equiv b_i \pmod{p^jA}$, $0 \leq i \leq k$. Isto por sua vez implica que $a_i^p \equiv b_i^p \pmod{p^{j+1}A}$, ou seja, temos $(a^\pi)_i \equiv (b^\pi)_i \pmod{p^{j+1}A}$, $0 \leq i \leq k$. Da primeira parte vem que $(a^\pi)^{(i)} \equiv (b^\pi)^{(i)} \pmod{p^{j+i+1}A}$, $0 \leq i \leq k$. Agora, como $a^{(k+1)} - b^{(k+1)} = (a^\pi)^{(k)} - (b^\pi)^{(k)} + p^{k+1}(a_{k+1} - b_{k+1})$, segue que $p^{k+1}(a_{k+1} - b_{k+1}) \in p^{j+k+1}A$, ou seja, $a_{k+1} - b_{k+1} \in p^jA$. Isto é, $a_{k+1} \equiv b_{k+1} \pmod{p^jA}$, o que completa a prova do lema.

No que segue, $\mathbb{Z}$ denotará o anel dos inteiros, $\mathbb{Z}[X_0, \ldots, X_j; Y_0, \ldots, Y_j]$ denotará o anel de polinômios nas indeterminadas $X = (X_0, \ldots, X_j)$ e $Y = (Y_0, \ldots, Y_j)$, $0 \leq j \leq n-1$, com coeficientes inteiros e $(X_0, \ldots, X_j; Y_0, \ldots, Y_j)\mathbb{Z}[X_0, \ldots, X_j; Y_0, \ldots, Y_j]$, o ideal gerado por $\{X_0, \ldots, X_j; Y_0, \ldots, Y_j\}$ no anel $\mathbb{Z}[X_0, \ldots, X_j; Y_0, \ldots, Y_j]$. Com estas notações, temos o seguinte:

TEOREMA A.2: Sejam X_r, Y_s, $0 \leq r, s \leq n-1$, indeterminadas sobre $\mathbb{Z}$. Então existe polinômios $s_j, m_j \in (X_0, \ldots, X_j; Y_0, \ldots, Y_j)\mathbb{Z}[X_0, \ldots, X_j; Y_0, \ldots, Y_j]$, $0 \leq j \leq n-1$, unicamente determinados, tais que:

$$(a) \quad \sum_{j=0}^{i} p^j (s_j)^{p^{i-j}} = \left(\sum_{j=0}^{i} p^j X_j^{p^{i-j}} \right) + \left(\sum_{j=0}^{i} p^j Y_j^{p^{i-j}} \right), \quad 0 \leq i \leq n-1.$$

$$(b) \quad \sum_{j=0}^{i} (m_j)^{p^{i-j}} = \left(\sum_{j=0}^{i} p^j X_j^{p^{i-j}} \right) \left(\sum j = 0^i p^j Y_j^{p^{i-j}} \right), \quad 0 \leq i \leq n-1.$$

Nota: Observemos que estes polinômios s_j, m_j, $0 \leq j \leq n-1$, se existirem são exatamente as componentes de $X + Y$ e XY, para $X = (X_0, \ldots, X_{n-1}), Y = (Y_0, \ldots, Y_{n-1}) \in W_n(\mathbb{Z}[X_0, \ldots, X_{n-1}; Y_0, \ldots, Y_{n-1}])$. Logo, estão unicamente determinados, pois $\gamma : W_n(\mathbb{Z}[X_0, \ldots, X_{n-1}; Y_0, \ldots, Y_{n-1}]) \to (\mathbb{Z}[X_0, \ldots, X_{n-1}; Y_0, \ldots, Y_{n-1}])^n$ é

uma bijeção.

Decorre ainda destas fórmulas que a i–ésima componente de $X+Y$ e XY em $W_n(\mathbb{Z}[X_0,\ldots,X_{n-1};Y_0,\ldots,Y_{n-1}])$, $0 \leq i \leq n-1$, se escreve em função da i–ésima componente e das componentes anteriores de $X=(X_0,\ldots,X_{n-1})$ e de $Y=(Y_0,\ldots,Y_{n-1})$.

Prova do Teorema A.2: Vamos fazer apenas a prova de (a), a qual será feita por indução. A prova de (b) é inteiramente análoga. Temos que mostrar apenas a existência destes polinômios, uma vez que a unicidade já está clara, pela nota acima. Para tal, consideremos $X=(X_0,\ldots,X_{n-1}), Y=(Y_0,\ldots,Y_{n-1}) \in W_n(\mathbb{Z}[X_0,\ldots,X_{n-1};Y_0\ldots,Y_{n-1}])$ e seja $I_k=(X_0,\ldots,X_k;Y_0,\ldots,Y_k)\mathbb{Z}[X_0,\ldots,X_k;Y_0,\ldots,Y_k]$, $0 \leq k \leq n-1$.

Para $k=0$, (a) se torna $s_0=X_0+Y_0$, o qual é evidentemente um polinômio em I_0. Suponhamos que $s_i=(X+Y)_i \in I_i$, $0 \leq i \leq k$, para algum $k \leq n-2$. Mostraremos que $s_{k+1}=(X+Y)_{k+1} \in I_{k+1}$.

Temos:

$((X+Y)^\pi)_i=(X+Y)_i^p=(s_i(X_0,\ldots,X_i;Y_0,\ldots,Y_i))^p \equiv s_i(X_0^p,\ldots,X_i^p;Y_0^p,\ldots,Y_i^p) \equiv (X^\pi+Y^\pi)_i \pmod{pI_i}$, $0 \leq i \leq k$. Segue do lema anterior que $((X+Y)^\pi)^{(i)} \equiv (X^\pi+Y^\pi)^{(i)} \pmod{p^{i+1}I_i}$, $0 \leq i \leq k$. Em particular temos $((X+Y)^\pi)^{(k)} \equiv (X^\pi+Y^\pi)^{(k)} \pmod{p^{k+1}I_k}$.

Por outro lado, $(X^\pi+Y^\pi)^{(k)}=(X^\pi)^{(k)}+(Y^\pi)^{(k)}=X^{(k+1)}+Y^{(k+1)}-p^{k+1}(X_{k+1}+Y_{k+1})$. Logo, $(X^\pi+Y^\pi)^{(k)} \equiv X^{(k+1)}+Y^{(k+1)} \equiv (X+Y)^{(k+1)} \pmod{p^{k+1}I_{k+1}}$. Então, temos $p^{k+1}(X+Y)_{k+1}=(X+Y)^{(k+1)}-((X+Y)^\pi)^{(k)} \equiv 0 \pmod{p^{k+1}I_{k+1}}$, ou seja, $(X+Y)_{k+1}=s_{k+1} \in I_{k+1}$, como queríamos mostrar.

COROLÁRIO A.3: Seja A um anel comutativo contendo o corpo dos racionais. Sejam $a=(a_0,\ldots,a_{n-1}), b=(b_0,\ldots,b_{n-1}) \in W_n(A)$. Então:

$a+b=(s_0(a_0,b_0),s_1(a_0,a_1;b_0,b_1),\ldots,s_{n-1}(a_0,\ldots,a_{n-1};b_0,\ldots,b_{n-1}))$

$ab=(m_0(a_0,b_0),m_1(a_0,a_1;b_0,b_1),\ldots,m_{n-1}(a_0,\ldots,a_{n-1};b_0,\ldots,b_{n-1}))$

Prova: As equações do teorema anterior continuam válidas, se substituirmos $X=(X_0,\ldots,X_{n-1})$ e $Y=(Y_0,\ldots,Y_{n-1})$ por $a=(a_0,\ldots,a_{n-1})$ e $b=(b_0,\ldots,b_{n-1})$, respectivamente. Basta considerar o homomorfismo de anéis $\varphi : \mathbb{Z}[X_0,\ldots,X_{n-1};Y_0,\ldots,Y_{n-1}] \to A$, dado por $\varphi(X_i)=a_i$, $\varphi(Y_i)=b_i$, $0 \leq i \leq n-1$, e aplicar sua extensão natural $\varphi : W_n(\mathbb{Z}[X_0,\ldots,X_{n-1};Y_0,\ldots,Y_{n-1}] \to W_n(A)$.

Seja agora A um anel comutativo qualquer cuja característica é zero. Consideremos $B=A_{\mathbb{Z}-\{0\}}$ o anel de frações de A, com respeito à $\mathbb{Z}-\{0\}$. Nestas condições, temos

o seguinte diagrama:

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

onde as setas verticais significam as inclusões $\mathbb{Z} \hookrightarrow A$ e $\mathbb{Q} \hookrightarrow B$, respectivamente. Logo podemos supor sempre que A está contido em algum anel que contém o corpo dos racionais.

Consideremos o homomorfismo inclusão canônica $A \hookrightarrow B$ e extendemos à $W_n(A) \hookrightarrow W_n(B)$. Dados $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in W_n(A)$, facilmente se vê que $s_i(a_0, \ldots, a_i; b_0, \ldots, b_i), m_i(a_0, \ldots, a_i; b_0, \ldots, b_i) \in W_n(A)$, para todo $o \leq i \leq n-1$. Nosso próximo resultado é claro e mostra que $W_n(A)$ é também um anel comutativo.

COROLÁRIO A.4: Seja A um anel comutativo de característica zero. Sejam $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in W_n(A)$. Então:

$a + b = (s_0(a_0, b_0), s_1(a_0, a_1; b_0, b_1), \ldots, s_{n-1}(a_0, \ldots, a_{n-1}; b_0, \ldots, b_{n-1}))$

$ab = (m_0(a_0, b_0), m_1(a_0, a_1; b_0, b_1), \ldots, m_{n-1}(a_0, \ldots, a_{n-1}; b_0, \ldots, b_{n-1})$

Em particular, $W_n(A)$ é um subanel de $W_n(B)$.

Ainda, da prova do teorema anterior e do lema A.1 temos o seguinte

COROLÁRIO A.5: Sejam $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in W_n(A)$. Então temos $((a+b)^\pi)_i \equiv (a^\pi + b^\pi)_i \pmod{pA}$ e $((ab)^\pi)_i \equiv (a^\pi b^\pi)_i \pmod{pA}$, para $0 \leq i \leq n-1$.

Resumindo os resultados anteriores, temos o seguinte

TEOREMA A.6: Seja A um anel comutativo de característica zero. Então $W_n(A)$ é um anel comutativo. Dados $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in W_n(A)$ então as componentes de $a + b$ e ab em $W_n(A)$, são dadas por polinômios com coeficientes inteiros calculados em $a_0, \ldots, a_{n-1}; b_0, \ldots, b_{n-1}$.

Antes de definirmos os anéis de vetores de Witt sobre um anel de característica p, veremos algumas propriedades dos operadores π e V definidos anteriormente.

PROPOSIÇÃO A.7: Seja $a = (a_0, \ldots, a_{n-1}) \in W_n(A)$, Então $\gamma(V^i(a)) = [0, \ldots, 0, p^i a^{(0)}, \ldots, p^i a^{(n-1-i)}]$, $0 \leq i \leq n-1$.

Prova: Temos $V^i(a) = (0, a_0, \ldots, a_{n-2}) = [a'^{(0)}, \ldots, a'^{(n-1)}]$, onde:

$a'^{(0)} = 0$

$a^{(1)} = 0^p + pa_0 = pa_0 = pa^{(0)}$

$\vdots$

$a^{(n-1)} = 0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-1}a_{n-2} = p(a_0^{p^{n-2}} + pa_1^{p^{n-3}} + \cdots + p^{n-2}a_{n-2}) = pa^{n-2}$.

Ou seja, $\gamma(V(a)) = [0, pa^{(0)}, \ldots, pa^{(n-2)}]$. Agora, iterando i vezes obtemos o resultado desejado.

COROLÁRIO A.8: Sejam $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in W_n(A)$. Então $V(a+b) = V(a) + V(b)$.

Prova: Temos $a+b = ((a+b)_0, \ldots, (a+b)_{n-1}) = \gamma^{-1}([(a+b)^{(0)}, \ldots, (a+b)^{(n-1)}])$. Resulta da proposição anterior que $\gamma(V(a+b)) = [0, p(a+b)^{(0)}, \ldots, p(a+b)^{(n-2)}] = [0, p(a^{(0)} + b^{(0)}), \ldots, p(a^{(n-2)}+b^{(n-2)}] = [0, pa^{(0)}, \ldots, pa^{(n-2)}]+[0, pb^{(0)}, \ldots, pb^{(n-2)}] = \gamma(V(a))+\gamma(V(b))$. Agora, como γ é um isomorfismo de anéis, segue que $\gamma(V(a))+\gamma(V(b)) = \gamma(V(a)+V(b))$, de onde segue que $V(a+b) = V(a) + V(b)$. Assim, o corolário está provado.

Dado $a \in A$, notaremos $\{a\} = (a, 0, \ldots, 0) \in W_n(A)$. Assim, temos $\gamma(\{a\}) = [a, a^p, \ldots, a^{p^{n-1}}]$. Segue da proposição A.7 que $\gamma(V^i(\{a\})) = [0, \ldots, 0, p^i a, \ldots, p^i a^{p^{n-1-i}}]$, para $0 \leq i \leq n-1$. Desta forma, para cada $a = (a_0, \ldots, a_{n-1}) \in W_n(A)$ e $b \in A$, temos $a = \sum_{i=0}^{n-1} V^i(\{a_i\})$ e $\{b\}a = (ba_0, b^p a_1, \ldots, b^{p^{n-1}} a_{n-1}) = \sum_{i=0}^{n-1} v^i(\{b^{p^i} a_i\})$. De fato, $\sum_{i=0}^{n-1} \gamma(V^i(\{a_i\})) = \sum_{i=0}^{n-1}[0, \ldots, 0, p^i a_i, \ldots, p^i a_i^{p^{n-i-1}}] = [a^{(0)}, \ldots, a^{(n-1)}]$, como é fácil verificar. Assim, $\sum_{i=0}^{n-1} V^i(\{a_i\}) = a$. Ainda, $\gamma(\{b\}a) = [b, b^p, \ldots, b^{p^{n-1}}][a^{(0)}, \ldots, a^{(n-1)}] = [ba^{(0)}, b^p a^{(1)}, \ldots, b^{p^{n-1}} a^{(n-1)}]$. Logo, $\{b\} = (ba_0, b^p a_1, \ldots, b^{p^{n-1}} a_{n-1})$, como é fácil ver. Logo, $\{b\}a = \sum_{i=0}^{n-1} V^i(\{b^{p^i} a_i\})$.

Dados $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in W_n(A)$, dizemos que a e b são elementos disjuntos sempre que, para cada $0 \leq i \leq n-1$, temos: ou $a_i = 0$ ou $b_i = 0$. Resulta daí a seguinte

PROPOSIÇÃO A.9: Sejam $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1}) \in W_n(A)$, elementos disjuntos. Então $a + b = (a_0 + b_0, \ldots, a_{n-1} + b_{n-1})$.

Prova: Temos $a+b = \sum_{i=0}^{n-1} V^i(\{a_i\}) + \sum_{i=0}^{n-1} V^i(\{b_i\}) = \sum_{i=0}^{n-1} V^i(\{a_i\}+\{b_i\}) = \sum_{i=0}^{n-1} V^i(\{a_i + b_i\}) = (a_0 + b_0, \ldots, a_{n-1} + b_{n-1})$, como queríamos mostrar.

Finalmente, dado $X = (X_0, \ldots, X_{n-1})$ indeterminadas sobre $\mathbb{Z}$, consideremos o anel de polinômios a n indeterminadas $\mathbb{Z}[X] = \mathbb{Z}[X_0, \ldots, X_{n-1}]$. Observemos que os polinômios $(pX)_i$ e $(V(X^\pi))_i$ $(0 \leq i \leq n-1)$ possuem coeficientes em $\mathbb{Z}$. Assim temos o seguinte

PROPOSIÇÃO A.10: Com as mesmas notações acima, $(pX)_i \equiv (V(X^\pi))_i \pmod{p\mathbb{Z}[X]}$, para todo $0 \leq i \leq n-1$.

Prova: Sabemos que $(pX)^{(i)} = pX^{(i)} = p(X^{\pi^{(i-1)}} + p^i X_i) \equiv pX^{\pi^{(i-1)}} \equiv V(X^\pi)^{(i)} \pmod{p^{i+1}\mathbb{Z}[X]}$, para todo $0 \leq i \leq n-1$, pois $V(X^\pi)^{(i)} = pX^{\pi^{(i-1)}}$, pela proposição A.7. Então segue do lema A.1 que $(pX)_i \equiv (V(X^\pi))_i \pmod{p\mathbb{Z}[X]}$, $0 \leq i \leq n-1$, como queríamos provar.

Consideremos agora um anel A de característica p. Seja $W_n(A) = \{(a_0, \ldots, a_{n-1}) : a_i \in A, 0 \leq i \leq n-1\}$ e tomemos $a = (a_0, \ldots, a_{n-1})$ e $b = (b_0, \ldots, b_{n-1})$ em $W_n(A)$. Seja $\mathbb{Z}[X, Y] := \mathbb{Z}[X_0, \ldots, X_{n-1}; Y_0, \ldots, Y_{n-1}]$ o anel de polinômios nas indeterminadas $X = (X_0, \ldots, X_{n-1})$ e $Y = (Y_0, \ldots, Y_{n-1})$. Seja ainda $\varphi : W_n(\mathbb{Z}[X, Y]) \to W_n(A)$ o homomorfismo induzido por $X_i \mapsto a_i$, $Y_i \mapsto b_i$, $o \leq i \leq n-1$. Sabemos que:

$$X + Y = (s_0(X_0, Y_0), \ldots, s_{n-1}(X_0, \ldots, X_{n-1}; Y_0, \ldots, Y_{n-1}))$$

$$XY = (m_0(X_0, Y_0), \ldots, m_{n-1}(X_0, \ldots, X_{n-1}; Y_0, \ldots, Y_{n-1}))$$

em $W_n(\mathbb{Z}[X, Y])$. Definimos então $a + b$ e ab via φ, como segue:

$a + b = (\bar{s}_0(a_0, b_0), \ldots, \bar{s}_{n-1}(a_0, \ldots, a_{n-1}; b_0, \ldots, b_{n-1}))$

$ab = (\bar{m}_0(a_0, b_0), \ldots, \bar{m}_{n-1}(a_0, \ldots, a_{n-1}; b_0, \ldots, b_{n-1}))$

em $W_n(A)$, onde $\bar{s}_i(a_0, \ldots, a_i; b_0, \ldots, b_i)$, $\bar{m}_i(a_0, \ldots, a_{n-i}; b_0, \ldots, b_{n-i})$ são as expressões obtidas dos polinômios s_i, m_i do teorema A.2, respectivamente $(o \leq i \leq n-1)$, substituindo-se cada coeficiente inteiro por seu correspondente em $\mathbb{Z}/p\mathbb{Z}$. Desta forma, $(W_n(A), +, \cdot)$ é um anel comutativo, chamado ANEL DE VETORES DE WITT SOBRE A. De fato, sejam $X = (X_0, \ldots, X_{n-1})$, $Y = (Y_0, \ldots, Y_{n-1})$ e $Z = (Z_0, \ldots, Z_{n-1})$ indeterminadas sobre $\mathbb{Z}$. Seja o anel $\mathbb{Z}[X, Y, Z] = \mathbb{Z}[X_0, \ldots, X_{n-1}; Y_0, \ldots, Y_{n-1}; Z_0, \ldots, Z_{n-1}]$. Definindo-se então o homomorfismo $\psi : W_n(\mathbb{Z}[X, Y, Z]) \to W_n(A)$, por $\psi(X) = \psi(X_0, \ldots, X_{n-1}) = (a_0, \ldots, a_{n-1}) = a$, $\psi(Y) = (Y_0, \ldots, Y_{n-1}) = (b_0, \ldots, b_{n-1}) = b$ e $\psi(Z) = \psi(Z_0, \ldots, Z_{n-1}) = (c_0, \ldots, c_{n-1}) = c$, onde $a, b, c \in W_n(A)$, podemos observar que as propriedades de anel comutativo de $W_n(\mathbb{Z}[X, Y, Z]$ induzem propriedades análogas em $W_n(A)$, via o homomorfismo ψ.

Ainda, no caso de A ser um anel de característica p todas as congruências acima se tornam igualdades. Assim, temos a seguinte

PROPOSIÇÃO A.11: Seja A um anel de característica p. Então, $(a+b)^{\pi} = a^{\pi}+b^{\pi}$, $(ab)^{\pi} = a^{\pi}b^{\pi}$ e $pa = V(a^{\pi})$, para todos $a, b \in W_n(A)$. Além disso, $p^i a = V^i(a^{\pi^i})$.

Queremos mostrar agora que o anel primo de $W_n(A)$ é $W_n(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Para tal, consideremos o homomorfismo $\varphi : \mathbb{Z} \to W_n(A)$, dado por $\varphi(m) = m1 = 1 + \cdots + 1 \in W_n(A)$, para todo $m \in \mathbb{Z}$. Então $Im\ \varphi$ é o subanel primo de $W_n(A)$. Como $p^n 1 = V^n(1) = 0$ e $p^i 1 = V^i(1) \neq 0$, para todo $0 \leq i \leq n-1$, segue que $\varphi(1)$ tem ordem aditiva p^n, de modo que $Im\ \varphi$ possui p^n elementos. Agora, como $Im\ \varphi \subseteq W_n(\mathbb{Z}/p\mathbb{Z})$ e $W_n(\mathbb{Z}/p\mathbb{Z})$ possui p^n elementos, segue que $Im\ \varphi = W_n(\mathbb{Z}/p\mathbb{Z})$ e portanto $W_n(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$. Assim, temos o seguinte

TEOREMA A.12: Seja A um anel comutativo de característica p. Então $W_n(A)$ é um anel comutativo tal que para todos $a, b \in W_n(A)$, as componentes de $a+b$ e ab em $W_n(A)$ são polinômios com coeficientes em $\mathbb{Z}/p\mathbb{Z}$. Além disso, $\pi : W_n(A) \to W_n(A)$ é um homomorfismo de anéis e o anel primo de $W_n(A)$ é $W_n(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Para finalizar este apêndice, mostraremos a seguinte

PROPOSIÇÃO A.13: Seja A um anel de característica p e $a = (a_0, \ldots, a_{n-1})$ um elemento de $W_n(A)$. Então a é inversível em $W_n(A)$ se e somente se a_0 é inversível em A.

Prova: Suponhamos que $a = (a_0, \ldots, a_{n-1}) \in W_n(A)$ é inversível em $W_n(A)$. Então existe $b = (b_0, \ldots, b_{n-1}) \in W_n(A)$ tal que $ab = 1$. Logo, $a_0 b_0 = 1$ em A, isto é, a_0 é inversível em A.

Para provar a recíproca, observamos que dado um elemento $c = (c_0, \ldots, c_{n-1}) \in W_n(A)$, existe uma extensão B de A e um elemento $b \in W_n(B)$ tal que $b^{\pi} = c$. De fato, basta tomar $B = A[X]/(X^{\pi} - c) = A[x]$, onde $x = X + (X^{\pi} - c)$ e $X = (X_0, \ldots, X_{n-1})$ é um conjunto de indeterminadas sobre A. Tomando $b = x$, temos $b^{\pi} = x^{\pi} = c$ em $W_n(B)$. Além disso, se $b = (b_0, \ldots, b_{n-1}) \in W_n(A)$ é tal que $b_0 = 0$ então $b = V(c)$ para algum $c \in W_n(A)$.

Suponhamos então $a = (a_0, \ldots, a_{n-1}) \in W_n(A)$, com a_0 inversível em A. Seja $b = (a_0^{-1}, 0, \ldots, 0) \in W_n(A)$. Temos $1 - ab = d = (0, d_1, \ldots, d_{n-1}) \in W_n(A)$. Então existe algum $c \in W_n(A)$ tal que $d = V(c)$. Seja B a extensão definida acima e

$c' \in W_n(B)$ um elemento tal que $c'^{\pi} = c$. Então, $d^n = (V(c))^n = V(c)\dots V(c) = V(c'^{\pi})\dots V(c'^{\pi}) = V^n((c'^{n})^{\pi^n}) = 0$ em $W_n(B)$. Como $W_n(A) \hookrightarrow W_n(B)$, segue que $d^n = 0$ em $W_n(A)$. Logo, $d = \mathbf{1} - ab$ é um elemento nilpotente de $W_n(A)$ e portanto $\mathbf{1} - d$ é inversível em $W_n(A)$. Mas $\mathbf{1} - d = \mathbf{1} - (\mathbf{1} - ab) = ab$. Isto completa a prova da proposição.

REFERÊNCIAS

[1] F.W. ANDERSON, K.R. FULLER: "Rings and Categories of Modules", Springer, New York, 1974.

[2] M.F. ATIYAH, I.G. MACDONALD: "Introduction to Commutative Algebra", Addison-Wesley, Reading, 1969.

[3] M. AUSLANDER, O. GOLDMAN: The Brauer group of a commutative ring, Trans. Amer. Math. Soc.,97 (1960), 367-409.

[4] N. BOURBAKI: "Algèbre". In:_. Éléments de Mathématique. vol. 1, Herman, Paris, 1970.

[5] S.U. CHASE, D.K. HARRISON, A. ROSENBERG: Galois theory and cohomology of commutative rings, Mem. Amer. math. Soc., 52 (1968), 1-19.

[6] F. DEMEYER, E. INGRAHAM: "Separable Algebras Over commutative Rings", Lectures Notes in Mathematics, 181. Springer, Berlin, 1971.

[7] M. FERRERO, A. PAQUES, A. SOLECKI: Cyclic p^n– extensions and $\mathbb{Z}_p$–extensions of commutative rings of characteristic p, Relatório técnico 43/89, IMECC-UNICAMP, 1989.

[8] ——: On $\mathbb{Z}_p$–extensions of commutative rings, J. Pure Appl. Algebra, 72 (1991), 5-22.

[9] C. GREITHER: Unramified Kummer extensions of prime power degree, Manuscripta Math., 64 (1987), 261-290.

[10] C. GREITHER, R. HAGGENMÜLLER: Abelche Galoiserweiterungen von R[X], Manuscripta Math., 38 (1982), 239- 256.

[11] C. GREITHER, R. MIRANDA: Galois extensions of prime degree, J. of Algebra,124 (1989), 354-366.

[12] D.K. HARRISON: Abelian extensions of commutative rings, Mem. Amer. Math. Soc., 52 (1968), 66-79.

[13] A. MICALLI, A. PAQUES: Sur le groupe des extensions cycliques, J. of Algebra, 63 (1980), 268-278.

[14] F.C.P. MILLIES: "Anéis e Módulos", IME-USP, São Paulo, 1972.

[15] T. NAGAHARA, A. NAKAJIMA: On cyclic extensions of commutative rings, Math. J. Okayama Univ., 15 (1971), 81-90.

[16] A. NAKAJIMA: On group of cyclic extensions over commutative rings, Math. J. Okayama Univ., 16 (1972), 83-98.

[17] D.G. NORTHCOTT: "A First Course of Homological Algebra", Cambridge University Press., London, 1973.

[18] P. RIBEMBOIN: "Tópicos de Teoria dos Números", Notas de Matemática - IMPA, 35 (1966),142-148.

[19] ——: "Rings and Modules", Interscience, New York, 1969.

[20] D.J. WINTER: "The Structure of Fields", Springer, New York, 1974.

[21] T. WYLLER: Torsor under abelian p-groups, J. Pure Appl. Algebra, 45 (1987) 273-286.

[22] O ZARISKI, P. SAMUEL: "Commutative Algebra", Vol. I, van Noostrand, Princeton, 1958.