

3129

RT - BIMECC
2935

ON R -AUTOMORPHISMS OF $R[X]$

Miguel Ferrero
and
Antonio Paques

Outubro

RP 53/93

Relatório de Pesquisa

**Instituto de Matemática
Estatística e Ciência da Computação**



UNIVERSIDADE ESTADUAL DE CÂMPINAS
Campinas - São Paulo - Brasil

R.P.
IM/53/93

ABSTRACT – We study R -automorphisms of the polynomial ring $R[X]$, where R is a not necessarily commutative ring. We give a description of the R -automorphisms of finite order of $R[X]$ in the case that the characteristic of R is finite, a characterization of the Galois automorphisms of $R[X]$ and necessary conditions for the existence of these last ones. We also study the subrings of $R[X]$ that are invariant under the action of Galois automorphisms of $R[X]$.

IMECC – UNICAMP
Universidade Estadual de Campinas
CP 6065
13081-970 Campinas SP
Brasil

O conteúdo do presente Relatório de Pesquisa é de única responsabilidade dos autores.

Outubro – 1993

I. M. E. C. C.
B I B L I O T E C A

On R -automorphisms of $R[X]$

Miguel Ferrero and Antonio Paques

Let R be a ring with an identity element and let $R[X]$ be the polynomial ring over R in an indeterminate X . The R -automorphisms of $R[X]$ have been characterized by R. W. Gilmer when R is a commutative ring ([6], Theorem 3). It follows that if φ is an R -automorphism of $R[X]$, φ is completely determined by $\varphi(X) = \sum_{i=0}^n a_i X^i$. This is also true if R is a non-commutative ring and since $\varphi(X)$ is a central element of $R[X]$, the description given by Gilmer shows that φ is an R -automorphism of $R[X]$ if and only if $a_i \in Z(R)$, for $0 \leq i \leq n$, a_1 is a unit and a_i is nilpotent for $i \geq 2$.

On the other hand, if G is a group of R -automorphisms of $R[X]$, the computation of the invariant subring $R[X]^G$ is a question of interest. In particular, if G is a finite group and R is an integral domain, J. B. Castillon [1] showed that $R[X]^G = R[f]$, where $f = \prod_{\varphi \in G} \varphi(X)$. The original motivation of our study was to obtain an extension of this result and to determine conditions under which $R[X]$ is a Galois extension of $R[X]^G$. Since every automorphism of such a group is of finite order, we found that it is interesting to characterize such kind of automorphisms. Also, in section 3 we show that when there exists a finite group G of R -automorphisms of $R[X]$ such that $R[X]$ is a Galois extension of $R[X]^G$, then the characteristic of R is finite. So, this case is of particular interest.

In § 1 we study automorphisms of finite order. The main theorem of this section

⁰This paper was partially supported by Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) and Coordenação de Aperfeiçoamento de Pessoal Superior (CAPES), Brazil.

states that when the characteristic of R is finite, then an automorphism such as φ given above is of finite order if and only if there exists an integer $t \geq 1$ with $a_1^t = 1$. In § 2 we extend the result of [1]. We prove that if G is finite and $\varphi(X) - X$ is not a zero divisor in $R[X]$, for any $1 \neq \varphi \in G$, then $R[X]^G = R[f]$ where $f = \prod_{\varphi \in G} \varphi(X)$. The converse is also true if R has no non-zero nilpotent elements.

In § 3 we consider the question of whether $R[X]$ is a Galois extension of $R[X]^G$ under some additional assumptions. The main result of this section gives a characterization of a Galois automorphism of $R[X]$, i.e., an R -automorphism φ such that $R[X]$ is a Galois extension of $R[X]^{(\varphi)}$, where (φ) is the cyclic group generated by φ . It follows that the order of φ must be a prime integer p and the characteristic of R must be p^e , $e \geq 1$. Also we show that a group G as above is necessarily a p -elementary abelian group.

Throughout this paper R is a (not necessarily commutative) ring with an identity element. The center of R is denoted by Z and the group of units of Z by $U(Z)$. The set of all the nilpotent elements of R will be denoted by $N(R)$ and we put $N(Z) = N$. Finally, the order of φ is denoted by $|\varphi|$. We recall that a commutative ring is said to be reduced if it has no non-zero nilpotent elements.

1. Automorphisms of finite order

Throughout this section we assume that φ is an R -automorphism of $R[X]$ defined by $\varphi(X) = a_0 + a_1X + \cdots + a_nX^n$, where $a_i \in Z$, $i = 0, 1, \dots, n$, $a_1 \in U(Z)$ and $a_j \in N$ for $j \geq 2$.

Recall that an element $a \in R$ is said to be a ($\mathbb{Z}$ -) torsion element if there exists an integer $t \geq 1$ such that $ta = 0$. The ring R is said to be torsion free (or having characteristic zero) if R has no non-zero torsion elements. In the case that there exists an integer $m \geq 2$ such that $mR = 0$, R is said to be of finite characteristic

and the characteristic of R is the smallest such integer m .

The main result of this section gives a complete description of the R -automorphisms of $R[X]$ which are of finite order, under the assumption that R is a ring of finite characteristic. In fact, we will prove the following more general result

Theorem 1.1. Assume that a_j is a torsion element, for $j = 0, 2, 3, \dots, n$. Then $|\varphi| < \infty$ if and only if a_1 is a root of the unit element of R .

To prove the theorem we need some lemmas. We begin with the following

Lemma 1.2. Assume that $b_i \in N$ are torsion elements of R , for $i = 1, 2, \dots, n$, and σ is the R -automorphism of $R[X]$ defined by $\sigma(X) = X + \sum_{i=1}^n b_i X^i$. Then $|\sigma| < \infty$.

Proof. Denote by I the ideal of R generated by $\{b_1, b_2, \dots, b_n\}$. Note that $\sigma^2(X) = X + \sum_{i=1}^n b_i X^i + \sum_{i=1}^n b_i \left(X + \sum_{j=1}^n b_j X^j \right)^i = X + 2 \sum_{i=1}^n b_i X^i + \sum_{k \geq 1} c_k X^k$, for some elements $c_k \in I^2$. An easy induction argument gives $\sigma^s(X) = X + s \sum_{i=1}^n b_i X^i + \sum_{j \geq 1} d_j X^j$, for any integer $s \geq 2$, where $d_j \in I^2$. Since $b_1, b_2, \dots, b_n$ are torsion elements there exists an integer $v \geq 2$ with $\sigma^v(X) = X + \sum_{\ell \geq 1} e_\ell X^\ell$, where $e_\ell \in I^2$. Repeating the argument starting with σ^v we obtain $\sigma^{v^2}(X) = X + \sum_{k \geq 1} f_k X^k$, for some elements $f_k \in I^4$. Now it is easy to complete the proof since I is a nilpotent ideal.

Lemma 1.3. Assume that $b_i \in N$, for $i = 0, \dots, n$, and let σ be the R -automorphism of $R[X]$ defined by $\sigma(X) = b_0 + X + \sum_{i=1}^n b_i X^i$. Then for every $s \geq 2$ there exist elements $c_0 \in I^2$ and $c_1, \dots, c_m \in I$ such that $\sigma^s(X) = sb_0 + c_0 + X + \sum_{j=1}^m c_j X^j$, where I is the ideal of R generated by $\{b_0, b_1, \dots, b_n\}$.

Proof. We have $\sigma^2(X) = b_0 + \left(b_0 + X + \sum_{i=1}^n b_i X^i\right) + \sum_{j=1}^n b_j \left(b_0 + X + \sum_{i=1}^n b_i X^i\right)^j = 2b_0 + X + \sum_{i=1}^n b_i X^i + \sum_{j=1}^n b_j b_0^j + \sum_{\ell \geq 1} c_\ell X^\ell$, for some $c_\ell \in I$. Note that $\sum_{i=1}^n b_j b_0^j \in I^2$ and so the result is true for $s = 2$. Now it is easy to complete the proof using an induction argument.

Corollary 1.4. Assume that $b_i \in N$ are torsion elements of R , for $i = 0, 1, \dots, n$, and let σ be the R -automorphism of $R[X]$ defined by $\sigma(X) = b_0 + X + \sum_{i=1}^n b_i X^i$. Then $|\sigma| < \infty$.

Proof. By the assumption there exists an integer $s \geq 2$ such that $sb_i = 0$, for $i = 0, \dots, n$. Then there exist $c_0 \in I^2$ and $c_1, \dots, c_m \in I$ such that $\sigma^s(X) = c_0 + X + \sum_{i=1}^m c_i X^i$, by Lemma 1.3. Applying the same argument to the automorphism σ^s we obtain $\sigma^{s^2}(X) = d_0 + X + \sum_{i=1}^t d_i X^i$, where $d_0 \in I^3$, $d_1, \dots, d_t \in I$. Since the ideal I is nilpotent, repeating this way we arrive to $\sigma^v(X) = X + \sum_{j=1}^u e_j X^j$, for some integer $v \geq 2$ and $e_1, \dots, e_u \in I$. Hence σ^v is of finite order by Lemma 1.2 and we have $|\sigma| < \infty$.

Proof of Theorem 1.1. Assume that there exists an integer $s \geq 1$ such that $a_1^s = 1$. By an induction argument we can easily see that $\varphi^s(X) = a_0 \sum_{i=0}^{s-1} a_1^i + b_0 + X + \sum_{j=1}^m b_j X^j$, where $b_0, b_1, \dots, b_m$ are in the ideal I generated by $\{a_2, \dots, a_n\}$. Then $\varphi^{2s}(X) = 2a_0 \sum_{i=0}^{s-1} a_1^i + c_0 + X + \sum_{j=1}^t c_j X^j$, where $c_0, \dots, c_t$ are in I . Repeating the argument and using the fact that a_0 is a torsion element we obtain an integer $v \geq 1$ and elements $d_0, d_1, \dots, d_u$ in I such that $\varphi^v(X) = d_0 + X + \sum_{i=1}^u d_i X^i$. Then φ is of finite order by Corollary 1.4.

Conversely, assume that $|\varphi| = m < \infty$. From the formula obtained for $\varphi^s(X)$

above it follows that $a_1^m + b = 1$, for some $b \in I = (a_2, \dots, a_n)$. Since b is a torsion element there exists an integer $u \geq 1$ with $ub = 0$. Then $a_1^{mu} = (1 - b)^u = 1 + b^2r$, for some $r \in R$. Thus $a_1^{mu} = 1 + c$, where $c \in I^2$. Repeating the argument and using the fact that I is a nilpotent ideal we find an integer $t \geq 1$ such that $a_1^t = 1$.

Now we include some additional remarks concerning the easy particular case in which $\varphi(X) = a_0 + a_1X$, $a_1 \in U(Z)$. This is the case for any R -automorphism of $R[X]$ if the center Z of R is reduced.

An easy computation shows the following

Proposition 1.5. Let φ be the R -automorphism of $R[X]$ defined by $\varphi(X) = a_0 + a_1X$. Then $\varphi^n = 1$ if and only if $a_1^n = 1$ and $a_0(1 + a_1 + \dots + a_1^{n-1}) = 0$.

We say that the ring R satisfies the condition (C) if the following holds:

(C) For every $1 \neq \varepsilon \in Z$ such that $\varepsilon^n = 1$, for $n \geq 2$, we have $1 - \varepsilon \in U(Z)$.

Condition (C) holds, for example, if the center Z of R is a field.

Corollary 1.5. Let φ be the R -automorphism of $R[X]$ defined by $\varphi(X) = a_0 + a_1X$ and assume that R satisfies the condition (C). Then $\varphi^n = 1$ if and only if one of the following conditions holds

i) $a_1 = 1$ and $na_0 = 0$

ii) $a_1 \neq 1$ and $a_1^n = 1$.

Proof. It is clear that if i) holds, then $\varphi^n = 1$. Assume that ii) holds. Since $(1 - a_1)(1 + a_1 + \dots + a_1^{n-1}) = 1 - a_1^n = 0$ we have $1 + a_1 + \dots + a_1^{n-1} = 0$ by the condition (C). Hence Proposition 1.5 gives $\varphi^n = 1$.

Conversely, assume that $\varphi^n = 1$. Hence $a_1^n = 1$ and we have either $a_1 \neq 1$ or

$a_1 = 1$ and so $na_0 = a_0(1 + a_1 + \cdots + a_1^{n-1}) = 0$.

Remark 1.7. The above Corollary shows that if $\varphi(X) = a_0 + X$, then $|\varphi| < \infty$ if and only if a_0 is a torsion element. Now, if σ is defined by $\sigma(X) = b_0 + b_1X$, where $b_1^m = 1$ and $1 + b_1 + \cdots + b_1^{m-1} = 0$ we have $\sigma^m = 1$ for any $b_0 \in Z$. This is the case, for example, if a_1 is a root of the unity of order m and Z is a field. This remark shows that probably is very difficult to obtain a general theorem corresponding to Theorem 1.1 without any additional assumption.

Proposition 1.5 has also the following

Corollary 1.8. Assume that R is a ring of characteristic a prime integer p and Z is reduced. If φ is an R -automorphism of $R[X]$, then the following conditions are equivalent

- i) $|\varphi| = p^e$, for some integer $e \geq 1$.
- ii) $|\varphi| = p$.
- iii) $\varphi(X) = a_0 + X$, for some $a_0 \in Z$.

Proof. Assume that $\varphi(X) = a_0 + a_1X$ and $|\varphi| = p^e$. If $a_1 \neq 1$ we have $a_1^{p^e} = 1$. Thus $(a_1 - 1)^{p^e} = 0$ and so $a_1 - 1 = 0$, a contradiction. Hence i) $\rightarrow$ iii) and the rest is clear.

From Corollary 1.8 the following is clear.

Remark 1.9. If R is as in Corollary 1.8 we have

- i) The set of all the R -automorphisms of $R[X]$ of order p^e , for some $e \geq 1$, is a subgroup of $\text{Aut}_R(R[X])$ which is isomorphic to the group $(R, +)$
- ii) Assume that G is a p -group which is a subgroup of $\text{Aut}_R(R[X])$. Then G is

abelian and any element of G has order p .

Example 1.10. Assume that R is a field of characteristic p and let ε be a primitive root of the unity of order a prime $q \neq p$. Then the automorphism σ defined by $\sigma(X) = a_0 + \varepsilon X, a_0 \in R$, has order q . This example shows that the subgroup of all the R -automorphisms of $R[X]$ of order p^e considered in the Remark 1.9 may be a proper subgroup of $\text{Aut}_R(R[X])$.

2. The fixed subring

Let G be a group of R -automorphisms of $R[X]$. The computation of the invariant subring $R[X]^G$ is a subject of interest ([1], [4]). In particular, in [4] the author studied $R[X]^G$ when G is the group of all the R -automorphisms of $R[X]$, for a commutative ring R . On the other hand, J. B. Castillon [1] proved that if R is a commutative domain and G is a finite group, then $R[X]^G = R[f]$, where $f = \prod_{\varphi \in G} \varphi(X)$.

The purpose of this section is to extend the above result. Throughout R is a (not necessarily commutative) ring and G is a finite group of R -automorphisms of $R[X]$ whose order is n . We put $f = \prod_{\varphi \in G} \varphi(X) \in Z[X]$. We will prove the following

Theorem 2.1. Assume that for every $\varphi \in G$, $\varphi \neq 1$, $\varphi(X) - X$ is not a zero divisor in $R[X]$. Then $R[X]^G = R[f]$ and $R[X]$ is a free left (right) $R[X]^G$ -module with the basis $\{1, X, \dots, X^{n-1}\}$.

Note that $\varphi(X) - X \in Z[X]$. Then the following is clear.

Corollary 2.2. If R is a prime ring, then $R[X]^G = R[f]$.

By the definition of f it is clear that $R[f] \subseteq R[X]^G$. We begin with the following

Lemma 2.3. Assume that $\varphi(X) - X$ is not a zero divisor in $R[X]$ for every $\varphi \in G$, $\varphi \neq 1$. Then $R[X] = \sum_{j=0}^{n-1} R[f]X^j$.

Proof. An easy computation shows that there exist $g \in Z[X]$ with $\partial g = n$ and the leading coefficient of g is invertible and $h \in N[X]$ such that $f = g + h$, where N is the set of all the nilpotent elements of Z . Then there exists an integer $m \geq 1$ with $h^m = 0$. Hence $g^m = \sum_{i=1}^m b_i f^i g^{m-i}$, for some $b_i \in Z$, and we easily obtain

$X^{nm} \in \sum_{j=0}^{nm-1} Z[f]X^j$. It follows that $Z[X]$ is finitely generated over $Z[f]$.

If Z is a reduced ring, then $h = 0$ and we obtain that $Z[X]$ is generated over $Z[f]$ by $\{1, X, \dots, X^{n-1}\}$. Consequently $R[X] = R \otimes_Z Z[X] = \sum_{j=0}^{n-1} R[f]X^j$. The result follows in this case.

Assume now that R is arbitrary. Put $\bar{Z} = Z/N$ and note that every $\varphi \in G$ induces a $\bar{Z}$ -automorphism of $\bar{Z}[X]$. Also, by the assumption $\bar{\varphi}(X) \neq X$ if $\varphi \neq 1$. Thus the group $\bar{G} = \{\bar{\varphi} : \varphi \in G\} \simeq G$ and we have $\bar{Z}[X] = \sum_{j=0}^{n-1} \bar{Z}[\bar{f}]X^j$, where

$\bar{f} = \prod_{\bar{\varphi} \in \bar{G}} \bar{\varphi}(X) = f + N[X] \in \bar{Z}[X]$. Consequently $Z[X] = \sum_{j=0}^{n-1} Z[f]X^j + N[X]$

and the Nakayama's Lemma gives $Z[X] = \sum_{j=0}^{n-1} Z[f]X^j$. Finally, as above we obtain

$$R[X] = \sum_{j=0}^{n-1} R[f]X^j.$$

Remark 2.4. We point out that when Z is a reduced ring the result $R[X] = \sum_{j=0}^{n-1} R[f]X^j$ is independent of the assumption. Also, since $\partial f = n$ and the lead-

ing coefficient of f is invertible we easily obtain that $\sum_{j=0}^{n-1} R[f]X^j = \sum_{j=0}^{n-1} \oplus R[f]X^j$.

Consequently in this case $R[X] = \sum_{j=0}^{n-1} \oplus R[f]X^j$ holds for any finite group G .

Now we are able to prove the theorem.

Proof of Theorem 2.1. Note that $R[X] = \sum_{j=0}^{n-1} R[f]X^j \subseteq \sum_{j=0}^{n-1} R[X]^G X^j \subseteq R[X]$.

Thus it is enough to show that $\sum_{j=0}^{n-1} R[X]^G X^j = \sum_{j=0}^{n-1} \oplus R[X]^G X^j$.

Assume that $h_i \in R[X]^G, i = 0, \dots, n-1$, and $\sum_{i=0}^{n-1} h_i X^i = 0$. Then

$\sum_{i=0}^{n-1} h_i \varphi_j(X)^i = 0$, for every $\varphi_j \in G$. Denote by A the matrix whose entries are $\varphi_j(X)^i \in Z[X]$. We easily obtain $\det(A)h_\ell = 0$, for $\ell = 0, \dots, n-1$. However $\det(A)$ is a Vandermonde determinant and by the assumption is not a zero divisor in $R[X]$. Consequently $h_\ell = 0$ for $\ell = 0, \dots, n-1$, and the proof is complete.

It is an open problem whether the converse of Theorem 2.1 holds. We can prove this under an additional assumption.

Proposition 2.5. Assume that the ring R has no non-zero nilpotent elements. Then the following conditions are equivalent

- i) $R[X]^G = R[f]$
- ii) $\sum_{i=0}^{n-1} R[X]^G X^i$ is a direct sum
- iii) $\varphi(X) - X$ is not a zero divisor in $R[X]$, for every $1 \neq \varphi \in G$.

Proof. The equivalence between i) and ii) follows from the Remark 2.4. We prove i) $\rightarrow$ iii).

Assume, by contradiction, that there exists $\varphi \in G, \varphi \neq 1$, such that $\varphi(X) - X$ is a zero divisor in $R[X]$. Since $\varphi(X) - X \in Z[X]$ it follows easily that there exists a non-zero $c \in R$ such that $c(\varphi(X) - X) = 0$. Then $H = \{\sigma \in G : \sigma(cX) = cX\}$

is a subgroup of G with $|H| \geq 2$. Take a set $\tau_1, \dots, \tau_t$ of representatives of the distinct left cosets of H in G and put $g = \prod_{i=1}^t \tau_i(cX)$. Then g is a non-zero element of $R[X]^G$ whose degree is $t < n$ and the leading coefficient is of the type $c^t d$, for some $d \in U(Z)$. By the assumption $g = b_n f^n + \dots + b_0$, for some $b_i \in R$, which is a contradiction since the leading coefficient of f^n is invertible.

We finish this section with the following

Remark 2.6. The subring $R[f]$ of $R[X]$ is a polynomial ring over R , i.e., there exists an R -isomorphism $\psi : R[t] \rightarrow R[f]$ such that $\psi(t) = f$. In fact, note that the coefficient of X^n in f is always invertible. Since $f \in Z[X]$ this implies that f is not a zero divisor in $R[X]$. Assume that $a_0 + a_1 f + \dots + a_n f^n = 0$, $a_i \in R$. Then $a_0 = 0$ because the constant term of f is zero. Thus $(a_1 + a_2 f + \dots + a_n f^{n-1})f = 0$ and so $a_1 + a_2 f + \dots + a_n f^{n-1} = 0$. Repeating the argument we obtain $a_i = 0$ for $i = 0, \dots, n$.

3. Galois automorphisms and Galois groups

Let S be a ring and G a finite group of automorphisms of S . Recall that S is said to be a Galois extension of S^G with group G if there exist x_i, y_i in S , $i = 1, \dots, m$, such that $\sum_{i=1}^m x_i \sigma(y_i) = \delta_{1,\sigma}$ for every $\sigma \in G$ ([2], [7]). The set $\{x_i, y_i\}_{1 \leq i \leq m}$ is called a Galois coordinate system for S over S^G .

Throughout this section G is again a finite group of R -automorphisms of $R[X]$. We study here under which conditions $R[X]$ is a Galois extension of $R[X]^G$ with group G . When this is the case we say that G is a *Galois group* of $R[X]$. An R -automorphism of $R[X]$ is said to be a *Galois automorphism* if the cyclic group $\langle \varphi \rangle$ generated by φ is a Galois group of $R[X]$. Clearly, every element of a Galois group of $R[X]$ is a Galois automorphism.

Every group G of R -automorphisms of $R[X]$ induces a group of Z -automorphisms of $Z[X]$ which is isomorphic to G . Assume that $1 \neq \varphi \in G$. Then $\varphi(X) - X \in Z[X]$ and so $\varphi(X) - X$ is invertible in $Z[X]$ if and only if $\varphi(X) - X$ is invertible in $R[X]$. Hereafter we will say simply " $\varphi(X) - X$ is invertible" when this is the case.

We begin this section with the following

Lemma 3.1. The following conditions are equivalent:

- i) G is a Galois group of $R[X]$
- ii) G is a Galois group of $Z[X]$
- iii) $\varphi(X) - X$ is invertible, for every $\varphi \in G$, $\varphi \neq 1$.

Proof. i) $\rightarrow$ iii) By the assumption there exist $x_i, y_i \in R[X]$, $1 \leq i \leq m$, such that $\sum_{i=1}^m x_i \varphi(y_i) = \delta_{1,\varphi}$, for every $\varphi \in G$. Suppose that $\varphi(X) - X$ is not invertible. Then there exists a maximal ideal $\mathcal{M}$ of $R[X]$ such that $\varphi(X) - X \in \mathcal{M}$. We easily obtain that $\varphi(h) - h \in \mathcal{M}$, for every $h \in R[X]$, and so $\sum_{i=1}^m x_i (y_i - \varphi(y_i)) \in \mathcal{M}$. Thus $\varphi = 1$.

iii) $\rightarrow$ ii) This follows directly from ([2], Theorem 1.3).

ii) $\rightarrow$ i) This is clear since the Galois coordinate system for $Z[X]$ is in $R[X]$.

Combining Lemma 3.1 with Theorem 2.1 we immediately have

Corollary 3.2. If G is a Galois group of $R[X]$, then $R[X]^G = R[f]$ and $R[X]$ is a free left (right) $R[X]^G$ -module with the basis $\{1, X, \dots, X^{n-1}\}$, where $f = \prod_{\varphi \in G} \varphi(X)$ and $n = \text{order}(G)$.

Now we give a characterization of a Galois automorphism. Assume that $\varphi(X) = a_0 + a_1 X + \dots + a_n X^n$, $a_0 \in Z$, $a_1 \in U(Z)$ and $a_i \in N$ for $i \geq 2$. We have

Theorem 3.3. The following conditions are equivalent:

- i) φ is a non-trivial Galois automorphism of $R[X]$

ii) $a_0 \in U(Z)$ and there exists a prime integer p such that the characteristic of R is p^e , $e \geq 1$, and $|\varphi| = p$.

Moreover, under the above conditions $a_1 \equiv 1 \pmod{N}$.

Proof. i) $\rightarrow$ ii) Suppose that φ is a Galois automorphism of $R[X]$ with $|\varphi| = p$. We may write $\varphi(X) = a_0 + a_1X + g$, where $g = a_2X^2 + \dots + a_nX^n \in N[X]$. By Lemma 3.1 $\varphi(X) - X = a_0 + (a_1 - 1)X + g$ is invertible in $Z[X]$, so we have $a_0 \in U(Z)$ and $a_1 - 1 \in N$. Then we can easily show that for every $i \geq 1$ there exists $h_i \in N[X]$ such that $\varphi^i(X) = ia_0 + X + h_i$. Therefore $ia_0 = (\varphi^i(X) - X) - h_i$ is invertible in Z if $i < p$ and is nilpotent if $i = p$. It follows that the integer i is invertible in Z if $i < p$ and is nilpotent if $i = p$. Consequently p is prime and $p^t = 0$ for some integer $t \geq 1$. Thus the characteristic of R is a power of p .

ii) $\rightarrow$ i) We write again $\varphi(X) = a_0 + a_1X + g$, $g \in N[X]$. Then $X = \varphi^p(X) = b_0 + a_1^pX + h$, for some $b_0 \in Z$ and $h \in N[X]$. It follows that $a_1^p \equiv 1 \pmod{N}$ and so $(a_1 - 1)^{p^e} \equiv 0 \pmod{N}$. Thus $a_1 \equiv 1 \pmod{N}$ and we have $\varphi^i(X) - X = ia_0 + h_i$, for some $h_i \in N[X]$. Since i and a_0 are invertible, for $1 \leq i < p$, Lemma 3.1 completes the proof.

For a ring with reduced center we have the following particular case.

Corollary 3.4. Assume that Z is a reduced ring and φ is an R -automorphism of $R[X]$. Then the following conditions are equivalent

- i) φ is a non-trivial Galois automorphism of $R[X]$
- ii) $\varphi(X) = X + a_0$, for some $a_0 \in U(Z)$, and the characteristic of R is a prime integer p .

Now we are in position to give a description of a Galois group of $R[X]$. Recall that a p -elementary abelian group is a group which is isomorphic to a direct product

of cyclic groups of order p . We have

Proposition 3.5. Assume that the characteristic of R is p^e and G is a Galois group of $R[X]$. Then G is a p -elementary abelian group.

Proof. We know that G is a Galois group of $Z[X]$. Denote by $\bar{Z}$ the factor ring Z/N and consider the group $\bar{G}$ of $\bar{Z}$ -automorphisms of $\bar{Z}[X]$ induced by G . It is easy to see that $\bar{G}$ is a Galois group of $\bar{Z}[X]$ which is isomorphic to G . So we may assume that Z is a reduced ring of characteristic p . In this case, for every $\varphi \in G$, $\varphi \neq 1$, we have $\varphi(X) = X + a_\varphi$, for some $a_\varphi \in U(Z)$. Also, $\varphi \circ \psi(X) = X + (a_\psi + a_\varphi)$. Therefore the group G is isomorphic to a subgroup of the abelian group $(Z, +)$. The result is now evident.

Now we can give a representation of all the Galois groups in the reduced case. Assume that V is a non-empty subset of units of Z . We say that $H = V \cup \{0\}$ is an *additive group of units* of Z if for every $u, v \in H$ we have $u - v \in H$.

If H is a finite additive group of units of Z , for any $u \in H$ we define an R -automorphism of $R[X]$ by $\varphi_u(X) = X + u$. Then it is clear that $\{\varphi_u : u \in H\}$ is a Galois group of $R[X]$ which is isomorphic to H . The converse is apparent from the proof of Proposition 3.5. Then we have

Corollary 3.6. Assume that Z is a reduced ring. Then the above correspondence is a one-to-one correspondence between the set of all the Galois groups of $R[X]$ and the set of all the finite additive groups of units of Z .

Remark 3.7. It is clear that in the general case if G is a Galois group of $R[X]$, then G is isomorphic to a finite additive group of units of Z/N . But we do not know

whether any such a group can be realized as a Galois group of $R[X]$.

- We finish the paper with some examples, remarks and questions.

First, by Theorem 3.3 if a Galois automorphism of $R[X]$ exists, then the characteristic of R is p^e , for a prime p and $e \geq 1$. The following examples show that any such a characteristic is possible.

Example 3.8. Let R be any ring of characteristic 2^e , $e \geq 1$, and let φ be the R -automorphism of $R[X]$ defined by $\varphi(X) = 1 - X$. Then φ is a Galois automorphism.

Example 3.9. Let R be any ring of characteristic p^2 , where p is any prime integer and let φ be the R -automorphism of $R[X]$ defined by $\varphi(X) = 1 + X + pX^{p-1}$. We show that φ is a Galois automorphism. Put $\tau(X) = X + 1$ and $g = X^{p-1}$. Using an induction argument we obtain $\varphi^i(X) = \tau^i(X) + p \sum_{j=0}^{i-1} \tau^j(g)$, for $1 \leq i \leq p$. Then

$\varphi^i(X) - X$ is invertible for $1 \leq i \leq p-1$ and $\varphi^p(X) = p + X + p \sum_{j=0}^{p-1} \tau^j(g)$. Thus it is

enough to show that $p + p \sum_{j=0}^{p-1} \tau^j(g) = 0$ in $R[X]$. In fact, $\sum_{j=0}^{p-1} \tau^j(g) = \sum_{j=0}^{p-1} (X+j)^{p-1} =$

$\sum_{j=0}^{p-1} c_j s_{p-1-j} X^j$, where c_j is a combinatorial number with $c_{p-1} = p$, $s_j = \sum_{\ell=1}^{p-1} \ell^j$, for

$1 \leq j \leq p-1$, and $c_0 = s_0 = 1$. Clearly $s_1 \equiv 0 \pmod{p}$. Now we use the formula

$\binom{j+1}{j} s_1 + \binom{j+1}{j-1} s_2 + \cdots + \binom{j+1}{2} s_{j-1} + \binom{j+1}{1} s_j = p^{j+1} - p$, for any $j = 1, \dots, p-2$

([3], E16, p. 17). Taking $j = 2$ we obtain $s_2 \equiv 0 \pmod{p}$. Continuing this way,

taking successively $j = 3, \dots, p-2$ we prove that $s_j \equiv 0 \pmod{p}$ for $1 \leq j \leq p-2$.

Also $s_{p-1} = \sum_{\ell=1}^{p-1} \ell^{p-1} \equiv (p-1) \pmod{p}$. Consequently, $p \sum_{j=0}^{p-1} \tau^j(g) = p(p-1) = -p$

and the proof is complete.

The following example shows that there always exists a ring R of characteristic

p^e such that $R[X]$ has a Galois automorphism.

Example 3.10. Let A be a commutative ring of characteristic p^e and denote by I the ideal of the polynomial ring $A[t]$ generated by the polynomial $h = \sum_{i=1}^p \binom{p}{i} t^{i-1}$. Put $R = A[t]/I$ and $\alpha = t + I \in R$. Then the characteristic of R is p^e and $\alpha \in N(R)$ because $\alpha^{p-1} = -\sum_{i=1}^{p-1} \binom{p}{i} \alpha^i = pb$, for some $b \in R$. Then $\varphi(X) = a + X + \alpha X$ defines an R -automorphism of $R[X]$. It is easy to check that if $a \in U(R)$, then φ is a Galois automorphism of $R[X]$.

Remark 3.11. The above examples and several other particular cases we have considered, suggest that for every ring R of characteristic p^e there should exist Galois automorphisms of $R[X]$. However we were unable to prove this conjecture.

Remark 3.12. Assume that G and H are Galois groups of $R[X]$ and $R[X]^G = R[X]^H$. If R is a connected ring, it follows from the results in [2] that $G = H$. However the result is not true in general. In fact, let R be a commutative ring of characteristic p , $\varphi(X) = X + a$, for $a \in U(R)$, and $\{e_1, \dots, e_{p-1}\}$ a family of orthogonal idempotents whose sum is 1. Put $\sigma = \sum_{i=1}^{p-1} e_i \varphi^i$. Then we easily see that σ is also a Galois automorphism and $\prod_{i=0}^{p-1} \varphi^i(X) = \prod_{j=0}^{p-1} \sigma^j(X)$. Thus $R[X]^{(\varphi)} = R[X]^{(\sigma)}$, where (φ) and (σ) are the cyclic groups generated by φ and σ , respectively.

Remark 3.13. If R is a non-commutative ring and G is a Galois group of $R[X]$, then G is a Galois group of $Z[X]$ and $R[X] = R \otimes_Z Z[X]$. Then, this is an example in which the results on Galois theory for $R[X]$ over $R[X]^G$ are trivial extensions of the results for $Z[X]$ over $Z[X]^G$ ([5], Theorem 2.1).

Question. It should be interesting to obtain a description of the R -automorphisms of $R[X]$ of order p when the characteristic of R is p^e . We could not give an answer

to this question.

References

- [1] J. B. Castillon, Groupe fini d'automorphismes des anneaux de polynômes et de series formelles, Bull. Sc. Math., 2a. Serie, 95 (1971), 237-240.
- [2] S. U. Chase, D. K. Harrison and A. Rosenberg, Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. 52 (1965), 15-33.
- [3] L. Childs, A concrete introduction to higher algebra, Springer-Verlag, New York (1979).
- [4] M. M. Dowlen, On the R -automorphisms of $R[X]$, J. Algebra 89 (1984), 323-334.
- [5] M. Ferrero, Galois theory by reduction to the center, Math. Notae 25 (1976), 19-27.
- [6] R. W. Gilmer, R -automorphisms of $R[X]$, Proc. London Math. Soc. (3) 18 (1968), 328-336.
- [7] Y. Miyashita, Finite outer Galois theory of non-commutative rings, J. Fac. Sc. Hokkaido Univ., Ser I, 19 (1966), 114-134.

Instituto de Matemática
Universidade Federal do Rio Grande do Sul
91509-900 - Porto Alegre, RS
Brazil

Instituto de Matemática, Estatística,
e Ciência da Computação
Universidade Estadual de Campinas
13081-970 - Campinas, SP
Brazil

RELATÓRIOS DE PESQUISA — 1993

- 01/93 On the Convergence Rate of Spectral Approximation for the Equations for Non-homogeneous Asymmetric Fluids — *José Luiz Boldrini and Marko Rojas-Medar.*
- 02/93 On Fraisse's Proof of Compactness — *Xavier Caicedo and A. M. Sette.*
- 03/93 Non Finite Axiomatizability of Finitely Generated Quasivarieties of Graphs — *Xavier Caicedo.*
- 04/93 Holomorphic Germs on Tsirelson's Space — *Jorge Mujica and Manuel Valdivia.*
- 05/93 Zitterbewegung and the Electromagnetic Field of the Electron — *Jayme Vaz Jr. and Waldyr A. Rodrigues Jr.*
- 06/93 A Geometrical Interpretation of the Equivalence of Dirac and Maxwell Equations — *Jayme Vaz Jr. and Waldyr A. Rodrigues Jr.*
- 07/93 The Uniform Closure of Convex Semi-Lattices — *João B. Prolla.*
- 08/93 Embedding of Level Continuous Fuzzy Sets and Applications — *Marko Rojas-Medar, Rodney C. Bassanezi and Heriberto Román-Flores.*
- 09/93 Spectral Galerkin Approximations for the Navier-Stokes Equations: Uniform in Time Error Estimates — *Marko A. Rojas-Medar and José Luiz Boldrini.*
- 10/93 Semigroup Actions on Homogeneous Spaces — *Luiz A. B. San Martin and Pedro A. Tonelli.*
- 11/93 Clifford Algebra Approach to the Barut-Zanghi Model as a Hamiltonian System — *Jayme Vaz Jr. and Waldyr A. Rodrigues Jr.*
- 12/93 Propagation of Scalar Waves in Layered Media — *Lúcio Tunes dos Santos and Martin Tygel.*
- 13/93 On the Convergence of the NMO-Power Series for a Horizontally Stratified Medium — *Martin Tygel.*
- 14/93 Convergence Rates in the Sobolev H' -Norm of Approximations by Discrete Convolutions — *Sônia M. Gomes.*
- 15/93 On the Choice of the Space Dimension in Ill-Posed Problems — *Cristina Cunha.*
- 16/93 Elliptic Equations in R^2 with Non-linearities in the Critical Range — *D. G. de Figueiredo, O. H. Miyagaki and B. Ruf.*
- 17/93 Drug Kinetics and Drug Resistance in Optimal Chemotherapy — *M. I. S. Costa, J. L. Boldrini and R. C. Bassanezi.*
- 18/93 Chemotherapeutic Treatments Involving Drug Resistance and Level of Normal Cells as a Criterion of Toxicity — *M. I. S. Costa, J. L. Boldrini and R. C. Bassanezi.*
- 19/93 Bifurcation of Singularities of Reversible Systems — *Marco Antonio Teizeira.*

- 20/93 **Sistemas Não Lineares e Fractais** — *Lúcio Tunes dos Santos.*
- 21/93 **New Integral Representation of the Solution of Schrödinger Equation with Arbitrary Potential** — *Rodolfo L. Monaco and Waldyr A. Rodrigues Jr.*
- 22/93 **The Module of Derivations of a Stanley-Reisner Ring** — *Paulo Brumatti and Aron Simis.*
- 23/93 **On the Convergence Rate of Spectral Approximation for the Equations for Chemical Active Fluid** — *Marko Rojas-Medar and Sebastián A. Lorca.*
- 24/93 **Sufficient Conditions for Minima of some Translation Invariant Functionals** — *Orlando Lopes.*
- 25/93 **A Constrained Minimization Problem with Integrals on the Entire Space** — *Orlando Lopes.*
- 26/93 **O Pensamento Reducionista na Filosofia de Niels Bohr** — *José Emilio Maiorino.*
- 27/93 **On the first curve of the Fučík spectrum of an elliptic operator** — *D.G. de Figueiredo and J.-P. Gossez.*
- 28/93 **Generalização dos Testes de Shirley e de House** — *Belmer Garcia Negrillo.*
- 29/93 **Compacidad y Compactificación en Teoría de Modelos** — *J. C. Cifuentes.*
- 30/93 **Global Strong Solutions of the Equations for the Motion of Nonhomogeneous Incompressible Fluids** — *José Luiz Boldrini and Marko Rojas-Medar.*
- 31/93 **A Equação de Laplace no Universo de de-Sitter-Castelnuovo** — *D. Gomes e E. Capelas de Oliveira.*
- 32/93 **Klein-Gordon Wave Equation in the de Sitter Universe** — *E. Capelas de Oliveira and E.A. Notte Cuello.*
- 33/93 **Mittag-Leffler Methods in Analysis** — *Jorge Mujica.*
- 34/93 **The Initial Value Problem for a Generalized Boussinesq Model** — *Sebastián A. Lorca and José Luiz Boldrini.*
- 35/93 **Problemas Minimax e Aplicações** — *José Mario Martínez, Lúcio Tunes dos Santos e Sandra Augusta Santos.*
- 36/93 **An Extension of the Theory of Secant Preconditioners** — *José Mario Martínez.*
- 37/93 **Convergence Estimates for the Wavelet-Galerkin Method: Superconvergence at the Node Points** — *Sônia M. Gomes.*
- 38/93 **An Error Estimate Uniform in Time for Spectral Semi-Galerkin Approximations of the Nonhomogeneous Navier-Stokes Equations** — *J. L. Boldrini and M. Rojas-Medar.*
- 39/93 **More About the Time Analysis of Tunnelling Processes** — *Vladislav S. Olkhovsky and Erasmo Recami.*
- 40/93 **Zero-Point Anomaly** — *José Alexandre Nogueira and Adolfo Maia Jr.*
- 41/93 **On a System of Evolution Equations of Magnetohydrodynamic Type** — *José Luiz Boldrini and Marko Rojas-Medar.*

- 42/93** Generalized Zeldovich's Regularization of the Vacuum Energy — *José Alexandre Nogueira and Adolfo Maia Jr.*
- 43/93** Global Strong Solution of the Equations for the Motion of a Chemical Active Fluid — *M.A. Rojas-Medar and S.A. Lorca.*
- 44/93** A Theorem of Finiteness for Fat Bundles — *Lucas M. Chaves.*
- 45/93** Partículas Elementares como Micro-Universos — *E. Recami, V. T. Zanchin and M. T. Vasconcelos.*
- 46/93** Micro-Universes and "Strong Black-Holes": A Purely Geometric Approach to Elementary Particles — *E. Recami, F. Raciti, W.A. Rodrigues Jr. and V. T. Zanchin.*
- 47/93** The Tolman "Antitelephone" Paradox: Its Solution by Tachyon Mechanics — *Erasmus Recami.*
- 48/93** Radial Symmetry of Minimizers for Some Translation and Rotation Invariant Functionals — *Orlando Lopes.*
- 49/93** A Riemann Integral Approach to Feynman's Path Integral — *Rodolfo L. Monaco, Roberto E. Lagos and Waldyr A. Rodrigues Jr.*
- 50/93** The Relationship between Electromagnetism and Quantum Mechanics, and a Non-Linear Dirac Equation — *C. Daviau, Waldyr A. Rodrigues Jr. and Jayme Vaz Jr.*
- 51/93** A New Approach for the JWKB Theory — *R.L. Monaco and E. Capelas de Oliveira.*
- 52/93** An Error Estimate Uniform in Time for Spectral Galerkin Approximations for the Equations for the Motion of a Chemical Active Fluid — *Marko A. Rojas-Medar and Sebastián A. Lorca.*