ON CYCLIC QUARTIC EXTENSIONS WITH NORMAL BASIS

Miguel Ferrero
Antonio Paques
and
Andrzej Solecki

RELATÓRIO TÉCNICO Nº 15/90

Abstract. Let R be a commutative ring with 2 being a unit in R. We give a complete description of all cyclic quartic extensions of R having a normal basis. We also give a description of the group $NB(\mathbb{Z}/4\mathbb{Z}, R)$ of all the $R[\mathbb{Z}/4\mathbb{Z}]$-isomorphism classes of these cyclic quartic extensions of R.

Instituto de Matemática, Estatística e Ciência da Computação
Universidade Estadual de Campinas
13.081, Campinas, S.P.
BRASIL

Março – 1990

On Cyclic Quartic Extensions With Normal Basis

Miguel Ferrero
Instituto de Matemática - UFRGS
90.049 - Porto Alegre, RS - Brazil

Antonio Paques
IMECC - UNICAMP
13.081 - Campinas, SP - Brazil

Andrzej Solecki
Departamento de Matemática - UFSC
88.049 - Florianópolis, SC - Brazil

Abstract. Let R be a commutative ring with 2 being a unit in R. We give a complete description of all cyclic quartic extensions of R having a normal basis. We also give a description of the group $NB(\mathbb{Z}/4\mathbb{Z}, R)$ of all the $R[\mathbb{Z}/4\mathbb{Z}]$-isomorphism classes of these cyclic quartic extensions of R.

Introduction

Throughout this paper R is a commutative ring with 2 being a unit in R. By a cyclic quartic extension A of R we mean a commutative Galois extension of R in the sense of [1] with a cyclic Galois group $\langle \sigma \rangle$ generated by an R-automorphism σ of A whose order is 4. Such an A is an $R[\langle \sigma \rangle]$-module in a natural way and we say that A *has a normal basis over* R if A is a free $R[\langle \sigma \rangle]$-module of rank 1. The purpose of this paper is to study cyclic quartic extensions of R which have normal basis.

For any commutative ring T we will denote by T^* the multiplicative group of all the units of T and by T^{*2} the subgroup of the squares of the elements of T^*.

Let $S = R[X]/(X^2+1) = R[i]$, where i denotes the coset of X modulo (X^2+1). In §1 we construct for every pair $(u, v) \in R^* \times S^*$ a cyclic quartic extension $A_{u,v}$ of R which has a normal basis and, conversely, we show that any cyclic quartic extension of R which has a normal basis is isomorphic to one extension of this type. We also prove that under certain conditions $A_{u,v}$ is isomorphic to the R-algebra $R[Z]/(Z^4+bZ^2+c)$ for some $b, c \in R^*$ with $c(b^2-4c) \in R^{*2}$. In particular, all cyclic quartic extensions of R can be described by this way when R is an LG-ring [2] such that $|R/\mathcal{P}| > 5$

This research was partially supported by CNPq, FAPERGS, FAPESP and FINEP (Brazil).

for every maximal ideal $\mathcal{P}$ of R. We also establish conditions for $A_{u,v}$ to be either a field, a connected ring, a local ring or an integral domain.

In §2, as an application of the main results of §1, we prove that the group $NB(\mathbb{Z}/4\mathbb{Z}, R)$ of all the $R[\mathbb{Z}/4\mathbb{Z}]$–isomorphism classes of cyclic quartic extensions of R having a normal basis is isomorphic to a quotient of the group $R^* \times S^*$.

Throughout this paper a cyclic quartic extension A of R with Galois group $\langle \sigma \rangle$ will be denoted by (A, σ). Unadorned $\otimes$ will mean $\otimes_R$.

1. The structure of a cyclic quartic extension with normal basis

The R–algebra $S = R[X]/(X^2+1) = R[i]$, where $i = X + (X^2+1)$, is a (Galois) quadratic extension of R with Galois group generated by the obvious R–automorphism. We will denote by N the norm mapping from S to R, i.e., $N(r_0 + r_1 i) = r_0^2 + r_1^2$.

Let $(u, v) \in R^* \times S^*$, where $v = r_0 + r_1 i$. We put $a = N(v) \in R^*$ and $D_a = R[X]/(X^2 - a) = R[x]$, where $x = X + (X^2 - a)$. Denote by $M = Re_0 \oplus Re_1$ a free R–module of rank 2 with a basis $\{e_0, e_1\}$ over R and set $A_{u,v} = D_a \oplus M$ as R–module. Hence, $A_{u,v}$ is a free R–module of rank 4 with a basis $\{1, x, e_0, e_1\}$ over R. It is easy to check that the following relations define on $A_{u,v}$ an structure of commutative R–algebra:

$$x^2 = a,\ \ e_0^2 = u(1 + a^{-1} r_0 x),\ \ e_1^2 = u(1 - a^{-1} r_0 x),\ \ e_0 e_1 = a^{-1} u r_1 x,$$
$$x e_0 = r_0 e_0 + r_1 e_1 \qquad \text{and} \qquad x e_1 = r_1 e_0 - r_0 e_1.$$

Also, the mapping $\rho : A_{u,v} \to A_{u,v}$ defined by $\rho|_R = id$, $\rho(x) = -x$, $\rho(e_0) = e_1$ and $\rho(e_1) = -e_0$ is a (well–defined) R–algebra automorphism of $A_{u,v}$ whose order is 4.

Lemma 1.1. $(A_{u,v}, \rho)$ is a cyclic quartic extension of R which has a normal basis.

Proof. From the above definitions it trivially follows that the fixed subring $A_{u,v}^{\rho} = \{t \in A_{u,v} : \rho(t) = t\}$ equals R. Now, let $\alpha = 4^{-1}(1 + x + e_0 - e_1)$ and $\alpha_i = \rho^i(\alpha)$, $0 \le i \le 3$. Clearly $\{\alpha_i : 0 \le i \le 3\}$ is a normal basis of $A_{u,v}$ over R and the following relations hold:

$$\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 = 1,\quad (\alpha_0 + \alpha_2) - (\alpha_1 + \alpha_3) = x \qquad \text{and}$$
$$(\alpha_0 - \alpha_2)^2 + (\alpha_1 - \alpha_3)^2 = 2^{-1}(e_0^2 + e_1^2) = u$$

The determinant of the circulant matrix $m(\alpha) = (\rho^{j-i}(\alpha))$, $0 \le i, j \le 3$, is $\det(m(\alpha)) = [(\alpha_0+\alpha_2)^2 - (\alpha_1+\alpha_3)^2][(\alpha_0-\alpha_2)^2 + (\alpha_1-\alpha_3)^2] = xu \in A_{u,v}^*$. Hence, $m(\alpha)$ is invertible and $[m(\alpha)]^{-1}$ is also circulant, say $[m(\alpha)]^{-1} = (\beta_{i-j(\mathrm{mod}\,4)})$, $0 \le i, j \le 3$. Thus, we get $\sum_{i=0}^{3} \rho^j(\alpha_i)\beta_i = \delta_{0,j}$. The proof is complete by ([1], Theorem 1.3.b)).

Before proving the next theorem we recall that two commutative ring extensions (A, σ) and (B, τ) of R with fixed R-automorphisms σ and τ, respectively, are *isomorphic* if there exists an R-algebra isomorphism $\varphi : A \longrightarrow B$ such that $\varphi \circ \sigma = \tau \circ \varphi$.

Now we have the main result of this section.

Theorem 1.2. Let (A, σ) be a commutative ring extension of R with an R-automorphism σ of A. Then, (A, σ) is a cyclic quartic extension of R having a normal basis if and only if (A, σ) is isomorphic to $(A_{u,v}, \rho)$ for some $(u, v) \in R^* \times S^*$.

Proof. Let (A, σ) be a cyclic quartic extension of R and let D be the fixed subring A^{σ^2} of A. Then, by the results in [1] it follows that A is a quadratic extension of D with Galois group $\langle \sigma^2 \rangle$, D is a quadratic extension of R with Galois group $\langle \sigma|_D \rangle$, $D = R \oplus X(D)$ as R-modules and $A = D \oplus X(A)$ as D-modules. where $X(D) = \{t \in D : \sigma(t) = -t\}$ and $X(A) = \{t \in A : \sigma^2(t) = -t\}$.

Now, suppose that $\{\alpha_i = \sigma^i(\alpha) : 0 \le i \le 3\}$ is a normal basis of A over R. Then, by Proposition 3.1 of [4], $\det(\sigma^{i+j}(\alpha)) = -[(\alpha_0+\alpha_2)^2 - (\alpha_1+\alpha_3)^2][(\alpha_0-\alpha_2)^2 + (\alpha_1-\alpha_3)^2] \in A^*$. We also may assume that $\sum_{i=0}^{3} \alpha_i = 1$.

By setting $x = (\alpha_0 + \alpha_2) - (\alpha_1 + \alpha_3)$, $x^2 = a$, $e_0 = (\alpha_0 - \alpha_2) + (\alpha_1 - \alpha_3)$ and $e_1 = \sigma(e_0)$ we easily get $a \in R^*$, $X(D) = Rx$, $D = R[x] \simeq R[X]/(X^2 - a)$ and $X(A) = Re_0 \oplus Re_1$. Also, since $\sigma(x) = -x$, $\sigma^2(xe_0) = -xe_0$, $\sigma^2(e_0^2) = e_0^2$, $\sigma^2(e_0e_1) = e_0e_1$ and $\sigma(e_0e_1) = -e_0e_1$, it follows that $xe_0 \in X(A)$, $e_0^2 \in D$ and $e_0e_1 \in X(D)$. From these conditions, by using the relations $ae_0 = x(xe_0)$, $xe_0^2 = (xe_0)e_0$ and $x(e_0e_1) = (xe_0)e_1$, we get unique elements $r_0, r_1 \in R$ and $u \in R^*$ such that

$$\begin{aligned}
xe_0 &= r_0e_0 + r_1e_1, & xe_1 &= -\sigma(xe_0) = r_1e_0 - r_0e_1,\\
a &= r_0^2 + r_1^2 = N(v), \quad \text{for} & v &= r_0 + r_1 i \in S^*,\\
e_0^2 &= u(1 + a^{-1}r_0x), & e_1^2 &= \sigma(e_0^2) = u(1 - a^{-1}r_0x) \quad \text{and}\\
e_0e_1 &= a^{-1}ur_1x. & &
\end{aligned}$$

Therefore, (A, σ) is clearly isomorphic to the cyclic quartic extension $(A_{u,v}, \rho)$ of R.

The converse holds by Lemma 1.1.

Remark 1.3. It is clear that the pair $(u, v) \in R^* \times S^*$ constructed in the above theorem depends on the choice of the normal basis. Also, the pair which corresponds to $(A_{u,v}, \rho)$ defined in Lemma 1.1 with respect to the basis given in the lemma is clearly (u, v).

From now on we will keep the above notations. If (A, σ) and a normal basis $\{\alpha_i = \sigma^i(\alpha) : 0 \le i \le 3\}$ of A over R with $\sum_{i=0}^{3} \alpha_i = 1$ are given, the basis $\{1, x, e_0, e_1\}$ as constructed in the above theorem will be called *the canonical basis* *associated with* (A, σ, α).

Now we have

Proposition 1.4. $A_{u,v} = R[e_0]$ if and only if $r_0 r_1 \in R^*$. Moreover, in this case $e_0^4 = 2ue_0^2 - a^{-1}(r_1 u)^2$ and $\rho(e_0) = \varepsilon(r_0 r_1)^{-1}(r_0^2 + a)e_0 - \varepsilon a(r_0 r_1 u)^{-1} e_0^3$, where $\varepsilon \in R^*$ is some solution of the equation $\varepsilon^2 = 1$.

Proof. From the equations stated in the beginning of this section it trivially follows that

$$\begin{aligned} e_0^4 &= 2ue_0^2 - a^{-1}(r_1 u)^2 \\ 2a^{-1} r_0 u x &= e_0^2 - e_1^2 = (e_0 - \rho(e_0))(e_0 - \rho^3(e_0)) \qquad \text{and} \\ 4a^{-1} r_1 u x &= 4e_0 e_1 = (e_0 - \rho^2(e_0))(\rho(e_0 - \rho^2(e_0))). \end{aligned}$$

On the other hand, by ([4], Corollary 2.2) $A_{u,v} = R[e_0]$ if and only if $(e_0 - \rho^i(e_0)) \in A_{u,v}^*$, for $1 \le i \le 3$. Then the first part follows since 2, u, a and x are units in $A_{u,v}$.

Also, since $A_{u,v}$ is a quadratic extension of $D_a = A_{u,v}^{\rho^2}$ with Galois group $\langle \rho^2 \rangle$, if $r_1 \in R^*$ we similarly get $A_{u,v} = D_a[e_0] = D_a \oplus D_a e_0$.

Now, assume $r_0 r_1 \in R^*$. Since $\rho(e_0) = e_1 \in X(A_{u,v}) = D_a e_0$, there exists $d \in D_a$ such that $\rho(e_0) = de_0$. Moreover, from $e_0^2 = u(1 + a^{-1} r_0 x)$ and $\rho^2(e_0) = -e_0$ we easily get $d\rho(d) = -1$ and $d^2(1 + a^{-1} r_0 x) = 1 - a^{-1} r_0 x$. Put $d = d_0 + d_1 x$, with $d_0, d_1 \in R$. Then, we have $d_0^2 - d_1^2 a = -1$, $d_0^2 + d_0 d_1 r_0 = 0$ and $d_1^2 r_0 + d_0 d_1 = 0$. If $\mathcal{P}$ is a maximal ideal of R and $d_0 \in \mathcal{P}$, then $d_1 \in \mathcal{P}$ and so $-1 \in \mathcal{P}$. Consequently, d_0 is a unit in R and it follows $d_1 = -d_0 r_0^{-1}$ and $d_0 = \varepsilon r_0 r_1^{-1}$ where $\varepsilon \in R^*$ satisfies $\varepsilon^2 = 1$. Thus $\rho(e_0) = r_1^{-1}\varepsilon(r_0 - x)e_0$. From $e_0^2 = u(1 + a^{-1} r_0 x)$ we get $x = a(r_0 u)^{-1}(e_0^2 - u)$ and hence $\rho(e_0) = \varepsilon(r_0 r_1)^{-1}(r_0^2 + a)e_0 - \varepsilon a(r_0 r_1 u)^{-1} e_0^3$, which completes the proof.

A slight reformulation of the above proposition gives the following interesting

Corollary 1.5. If $r_0 r_1 \in R^*$ then there exist $b, c \in R^*$ such that $c(b^2 - 4c) \in R^{*2}$ and $A_{u,v} \simeq R[Z]/(Z^4 + bZ^2 + c) = R[z]$, where $z = Z + (Z^4 + bZ^2 + c)$. Moreover, under this isomorphism the R-automorphism ρ of $A_{u,v}$ corresponds to the R-automorphism σ of $R[z]$ given by $\sigma(z) = \lambda^{-1}(b^2 - 2c)z + \lambda^{-1} bz^3$, where $\lambda \in R^*$ is some solution of the equation $\lambda^2 = c(b^2 - 4c)$.

Proof. It is enough to write (in Proposition 1.4) $-2u = b$ and $a^{-1}(r_1 u)^2 = c$ and to consider the mapping $e_0 \mapsto z$ from $A_{u,v}$ to $R[z]$.

The following proposition gives the converse of Corollary 1.5.

Proposition 1.6. Suppose that $b, c \in R$ and $A = R[Z]/(Z^4 + bZ^2 + c) = R[z]$, where $z = Z + (Z^4 + bZ^2 + c)$. If $b, c \in R^*$ and $c(b^2 - 4c) \in R^{*2}$, then A is a cyclic quartic extension of R with Galois group generated by $\sigma : z \mapsto \lambda^{-1}(b^2 - 2c)z + \lambda^{-1}bz^3$, where $\lambda \in R^*$ is a solution of the equation $\lambda^2 = c(b^2 - 4c)$. Furthermore, A has a normal basis over R and (A, σ) is isomorphic to $(A_{u,v}, \rho)$ with $u = -2^{-1}b$ and $v = (2c)^{-1}\lambda - i$.

Proof. Let $\lambda \in R^*$ a solution of the equation $\lambda^2 = c(b^2 - 4c)$ and put $t = \lambda^{-1}(b^2 - 2c)z + \lambda^{-1}bz^3 \in A$. We can easily check that $t^2 = -(b + z^2)$ and $t^4 + bt^2 + c = 0$. From this it follows that σ defined by $\sigma|_R = id$ and $\sigma(z) = t$ is a (well-defined) R-algebra homomorphism of A. Then, $\sigma^2(z) = \lambda^{-1}(b^2 - 2c + b\sigma(z^2))\sigma(z) = -\lambda^{-2}(2c + bz^2)(b^2 - 2c + bz^2)z = -\lambda^{-2}(b^2 - 4c)cz = -z$. Therefore, $\sigma^4 = id$ and so σ is an R-automorphism of order 4. Also, by using $\sigma^2(z) = -z$ and $\sigma(z^2) = -(b + z^2)$ we easily see that the fixed subring A^σ equals R.

Put $y = -\lambda^{-1}b(z^2 + 2^{-1}b)$, $f_0 = z$ and $f_1 = \sigma(z)$. It follows that $f_0^2 - f_1^2 = -2\lambda b^{-1}y$, $y^2 = (4c)^{-1}b^2$ and $f_0^2 f_1^2 = c$. Hence, $(f_0 - \sigma(f_0))(f_0 - \sigma^2(f_0))(f_0 - \sigma^3(f_0)) \in A^*$. Then, (A, σ) is a cyclic quartic extension of R by ([1], Theorem 1.3 (f)).

Finally, since $\{1, y, f_0, f_1\}$ is a basis of A over R we get a normal basis by writing $\alpha = 4^{-1}(1 + y + f_0 - f_1)$ and considering $\{\sigma^i(\alpha) : 0 \le i \le 3\}$. The last claim is immediate.

In general, there exist cyclic quartic extensions (A, σ) of R having normal basis such that for any representation $(A, \sigma) \simeq (A_{u,v}, \rho)$ the corresponding $v = r_0 + r_1 i$ satisfies $r_0 r_1 \notin R^*$. Take, for example, $R = \mathbb{F}_3$ or $\mathbb{F}_5$, $A = R \times R \times R \times R$ and σ the cyclic shift, where $\mathbb{F}_p$ denotes the finite field with p elements.

Nevertheless, there is an interesting case in which we can always get a representation of the type given in Proposition 1.6. Following [2] R is called an *LG*-ring if whenever a polynomial $f \in R[X_1, \ldots, X_n]$ represents a unit over $R_{\mathcal{P}}$, for every maximal ideal $\mathcal{P}$ of R, then f represents a unit over R. *LG*-rings include semilocal rings or, more generally, rings which are von Neumann regular modulo their Jacobson radical.

Corollary 1.7. Assume that R is an *LG*-ring such that $|R/\mathcal{P}| > 5$, for every maximal ideal $\mathcal{P}$ of R. Then every cyclic quartic extension of R is of the type described in Proposition 1.6.

Proof. Since R is an *LG*-ring, every cyclic quartic extension (A, σ) of R has a normal basis ([4], Theorem 3.2). Thus, given a normal basis $\{\alpha_i = \sigma^i(\alpha) : 0 \le i \le 3\}$ of A over R, with $\sum_{i=0}^{3} \alpha_i = 1$, let $\{1, z, e_0, e_1\}$ be the canonical basis associated with (A, σ, α) and $(u, v) \in R^* \times S^*$ the corresponding pair, $v = r_0 + r_1 i$.

Assume $r_0 r_1 \notin R^*$. We show is always possible to obtain another canonical basis $\{1, y, f_0, f_1\}$ of A over R for which $y f_0 = s_0 f_0 + s_1 f_1$, with $s_0 s_1 \in R^*$. This fact completes the proof.

For, take $y = z$, $f_0 = \lambda_0 e_0 + \lambda_1 e_1$, and $f_1 = \sigma(f_0) = -\lambda_1 e_0 + \lambda_0 e_1$, where $\lambda_0, \lambda_1 \in R$. The set $\{1, y, f_0, f_1\}$ is a basis of A over R if and only if $\lambda = \lambda_0^2 + \lambda_1^2 = \det \begin{pmatrix} \lambda_0 & -\lambda_1 \\ \lambda_1 & \lambda_0 \end{pmatrix} \in R^*$. Moreover, in this case $\{1, y, f_0, f_1\}$ is the canonical basis associated with (A, σ, β), where $\beta = 4^{-1}(1 + y + f_0 - f_1)$. Also, we can check that $yf_0 = s_0 f_0 + s_1 f_1$ with $s_0 = \lambda^{-1}[r_0(\lambda_0^2 - \lambda_1^2) + 2r_1\lambda_0\lambda_1]$ and $s_1 = \lambda^{-1}[r_1(\lambda_0^2 - \lambda_1^2) - 2r_0\lambda_0\lambda_1]$. So, in order to get our aim it suffices to verify that the polynomial $f = (X_0^2 + X_1^2)[r_0(X_0^2 - X_1^2) + 2r_1X_0X_1][r_1(X_0^2 - X_1^2) - 2r_0X_0X_1] \in R[X_0, X_1]$ represents a unit over $R_{\mathcal{P}}$, for every maximal ideal $\mathcal{P}$ of R. Since $r = r_0 + r_1 i \in S^*$ and $|R/\mathcal{P}| > 5$, we have $f \not\equiv 0 \pmod{\mathcal{P}R[X_0, X_1]}$ for such a $\mathcal{P}$ and the result easily follows.

In the rest of this section we will deal with the conditions for a cyclic quartic extension of R having a normal basis to be a field (resp. a connected ring, a local ring, an integral domain). Firstly, we need the following

Lemma 1.8. Assume that R is a connected ring and let (A, σ) be a cyclic quartic extension of R. Then, $A^{\sigma^2} \simeq R \times R$ if and only if there exists a (Galois) quadratic extension D of R such that $A \simeq D \times D$.

Proof. Suppose that $A^{\sigma^2} \simeq R \times R$. We may assume $A^{\sigma^2} = R \times R = R\varepsilon_1 \oplus R\varepsilon_2$, with $\varepsilon_1 = (1, 0)$ and $\varepsilon_2 = (0, 1)$, and $\sigma(\varepsilon_1) = \varepsilon_2$. Then, $A = A\varepsilon_1 \oplus A\varepsilon_2$, $\sigma|_{A\varepsilon_1} : A\varepsilon_1 \rightleftarrows A\varepsilon_2$ and $\sigma^2|_{A\varepsilon_1} : A\varepsilon_1 \rightleftarrows A\varepsilon_1$. It is not difficult to see that $D = A\varepsilon_1$ is a quadratic extension of $R\varepsilon_1 \simeq R$, with the Galois group $\langle \sigma^2 \rangle$.

For the converse we may also assume $A = D \times D$. Since D is a (Galois) quadratic extension of R let τ denotes the generator of the corresponding Galois group of D.

Firstly, we show that D is either a connected ring or $D \simeq R \times R$. Suppose that D is not connected. Thus, $D = D\varepsilon_1 \oplus D\varepsilon_2$ where ε_1 and ε_2 are non-zero idempotents of D such that $\varepsilon_1 + \varepsilon_2 = 1$. Since R is connected it easily follows that $\tau(\varepsilon_1) = \varepsilon_2$ and consequently $R \simeq R\varepsilon_1 \simeq R\varepsilon_2$. Furthermore, $D\varepsilon_i$ is a Galois extension of $R\varepsilon_i$ $i = 1, 2$, by ([5], Proposition 1.3). Also, D is a projective R-module of rank 2, so each $D\varepsilon_i$ is a projective $R\varepsilon_i$-module of rank 1. Consequently, it follows from ([1], Lemma 1.6) that $D\varepsilon_i = R\varepsilon_i$, $i = 1, 2$. Then, $D = D\varepsilon_1 \oplus D\varepsilon_2 = R\varepsilon_1 \oplus R\varepsilon_2 \simeq R \times R$.

Now, if $D \simeq R \times R$ then $A = R\varepsilon_1 \oplus R\varepsilon_2 \oplus R\varepsilon_3 \oplus R\varepsilon_4$, where $\varepsilon_1, \varepsilon_2, \varepsilon_3$ and ε_4 are minimal idempotents of A, and σ is a cyclic permutation (of order 4) of them. In this case we have $A^{\sigma^2} \simeq R \times R$. If D is connected, the unique idempotents of A are $0 = (0, 0)$, $1 = (1, 1)$, $\varepsilon_1 = (1, 0)$ and $\varepsilon_2 = (0, 1)$. So, $A = D\varepsilon_1 \oplus D\varepsilon_2$ and σ is determined by $\sigma|_D$, $\sigma(\varepsilon_1)$ and $\sigma(\varepsilon_2)$. Since $\sigma|_D : D \to A$ is an R-algebra homomorphism, there exists an idempotent $\varepsilon \in A$ such that $\sigma|_D = \varepsilon\, id + (1 - \varepsilon)\tau$ ([1], Theorem 3.1). We have $\sigma(\varepsilon_1) = \varepsilon_2$, $\sigma(\varepsilon_2) = \varepsilon_1$ and either $\sigma|_D = \varepsilon_1 id + \varepsilon_2\tau$ or $\sigma|_D = \varepsilon_2 id + \varepsilon_1\tau$, because in the other cases we get $\sigma^2 = id$, a contradiction. Now, it easily follows that

$A^{\sigma^2} \simeq R \times R$, which completes the proof.

Corollary 1.9. Let (A, σ) be a cyclic quartic extension of R. Then, A is a connected ring (resp. a field, a local ring) if and only if A^{σ^2} is a connected ring (resp. a field, a local ring).

Proof. Assume that A is not connected and $D = A^{\sigma^2}$ is connected. Since A is a (Galois) quadratic extension of D, by similar arguments to those used in the proof of the preceding lemma we get $A \simeq D \times D$. Thus, $D = A^{\sigma^2} \simeq R \times R$ which is a contradiction.

If A^{σ^2} is a field, then A is a connected quadratic extension of a field and so A is a field.

Finally, if A^{σ^2} is a local ring, then R is also a local ring. If $\mathcal{P}$ is the maximal ideal of R, a straightforward argument (reduction module $\mathcal{P}$) assures us that A is a local ring with maximal ideal $\mathcal{P}A$.

The converses are obvious.

The proof of the following corollary is easy and it will be omitted here.

Corollary 1.10. Let $(u, v) \in R^* \times S^*$, with $N(v) = a$. Then,

(i) $A_{u,v}$ is a connected ring if and only if R is a connected ring and $a \notin R^{*2}$.

(ii) $A_{u,v}$ is a field if and only if R is a field and $a \notin R^{*2}$.

(iii) $A_{u,v}$ is a local ring if and only if R is a local ring with maximal ideal $\mathcal{P}$ and $a + \mathcal{P} \notin (R/\mathcal{P})^{*2}$.

(iv) $A_{u,v}$ is an integral domain if and only if R is an integral domain and $a \notin F^{*2}$, where F is the field of fractions of R.

2. The group $NB(\mathbb{Z}/4\mathbb{Z}, R)$

We denote by $NB(\mathbb{Z}/4\mathbb{Z}, R)$ the set of all $R[\mathbb{Z}/4\mathbb{Z}]$–isomorphism classes $[A, \sigma]$ of cyclic quartic extensions of R having normal basis. On $NB(\mathbb{Z}/4\mathbb{Z}, R)$ we define the usual operation $*$:

$$[A, \sigma] * [B, \tau] = [(A \otimes B)^{\sigma^{-1} \otimes \tau}, \sigma \otimes id].$$

Clearly, $((A \otimes B)^{\sigma^{-1} \otimes \tau}, \sigma \otimes id)$ is a cyclic quartic extension of R. Also, if $\{\alpha_i = \sigma^i(\alpha) : 0 \leq i \leq 3\}$ and $\{\beta_i = \tau^i(\beta) : 0 \leq i \leq 3\}$ are normal bases of A and B over R, respectively, then $\{\gamma_i = (\sigma^i \otimes id)(\gamma) : 0 \leq i \leq 3\}$ is a normal basis of $(A \otimes B)^{\sigma^{-1} \otimes \tau}$ over R, for $\gamma = \sum_{i=0}^{3} \sigma^{-i}(\alpha) \otimes \tau^i(\beta)$. It is known that $*$ endows $NB(\mathbb{Z}/4\mathbb{Z}, R)$ with an abelian group structure. Actually, $NB(\mathbb{Z}/4\mathbb{Z}, R)$ is a subgroup of the Harrison group

$T(\mathbb{Z}/4\mathbb{Z}, R)$ [3] of the $R[\mathbb{Z}/4\mathbb{Z}]$-isomorphism classes of cyclic quartic extensions of R.

The purpose of this section is to give a description of $NB(\mathbb{Z}/4\mathbb{Z}, R)$ by using the results obtained in the former section.

We begin this section with the following

Lemma 2.1. Let (A,σ) and (B,τ) be isomorphic cyclic quartic extensions of R. Let $\{\alpha_i = \sigma^i(\alpha) : 0 \le i \le 3\}$ and $\{\beta_i = \tau^i(\beta) : 0 \le i \le 3\}$ be normal bases of A and B over R, respectively, and assume that $\sum_{i=0}^3 \alpha_i = \sum_{i=0}^3 \beta_i = 1$. If (u,v) and (u_1,v_1) are the corresponding pairs in $R^* \times S^*$ obtained as in Theorem 1.2 for (A,σ,α) and (B,τ,β), respectively, then there exist $\lambda \in R^*$ and $w \in S^*$ such that $(u_1,v_1) = (N(w), \lambda w^2)(u,v)$.

Proof.

We may assume $(B,\tau) = (A,\sigma)$. Then there exist $\lambda_i \in R$, $0 \le i \le 3$, such that $\beta_j = \sum_{i=0}^3 \lambda_{i-j(\text{mod}4)}\alpha_i$, for $0 \le j \le 3$. So, $\det(\lambda_{j-i(\text{mod}\,4)}) = [(\lambda_0+\lambda_2)^2 - (\lambda_1+\lambda_3)^2]$ $[(\lambda_0-\lambda_2)^2 + (\lambda_1-\lambda_3)^2] \in R^*$. Also, from $\sum_{i=0}^3 \alpha_i = \sum_{i=0}^3 \beta_i = 1$ we get $\sum_{i=0}^3 \lambda_i = 1$. Hence, $\mu = (\lambda_0+\lambda_2) - (\lambda_1+\lambda_3) = (\lambda_0+\lambda_2)^2 - (\lambda_1+\lambda_3)^2 \in R^*$ and $w = (\lambda_0-\lambda_2) - (\lambda_1-\lambda_3)i \in S^*$. Put $\lambda = \mu N(w)^{-1}$.

Suppose that $\{1, x, e_0, e_1\}$ and $\{1, y, f_0, f_1\}$ are the canonical bases associated with (A,σ,α) and (A,σ,β), respectively. Then we have the following equations:

$$\begin{aligned} x &= (\alpha_0+\alpha_2) - (\alpha_1+\alpha_3), \quad y = (\beta_0+\beta_2) - (\beta_1-\beta_3) \\ e_0 &= (\alpha_0-\alpha_2) + (\alpha_1-\alpha_3), \quad f_0 = (\beta_0-\beta_2) + (\beta_1-\beta_3) \\ xe_0 &= r_0e_0 + r_1e_1, \quad yf_0 = s_0f_0 + s_1f_1, \\ e_0^2 &= u(1+a^{-1}r_0x) \quad \text{and} \quad f_0^2 = u_1(1+b^{-1}s_0y) \end{aligned}$$

where $v = r_0 + r_1 i$, $v_1 = s_0 + s_1 i$, $N(v) = a$ and $N(v_1) = b$. By replacing here $\beta_j = \sum_{i=0}^3 \lambda_{i-j(\text{mod}4)}\alpha_i$, $0 \le j \le 3$, we easily get

$$\begin{aligned} s_0 &= \mu N(w)^{-1}[((\lambda_0-\lambda_2)^2 - (\lambda_1-\lambda_3)^2)r_0 + 2(\lambda_0-\lambda_2)(\lambda_1-\lambda_3)r_1], \\ s_1 &= \mu N(w)^{-1}[((\lambda_0-\lambda_2)^2 - (\lambda_1-\lambda_3)^2)r_1 - 2(\lambda_0-\lambda_2)(\lambda_1-\lambda_3)r_0] \quad \text{and} \\ u_1 &= N(w)u. \end{aligned}$$

Therefore, $(u_1,v_1) = (N(w)u, \mu N(w)^{-1}w^2 v) = (N(w), \lambda w^2)(u,v)$. The proof is complete.

Let $W(R^*,S^*) = \{(N(w), \lambda w^2) : \lambda \in R^*,\ w \in S^*\}$. Clearly, $W(R^*,S^*)$ is a subgroup of $R^* \times S^*$ and we denote by $\mathcal{W}(R,S)$ the quotient group $R^* \times S^*/W(R^*,S^*)$. An element of $\mathcal{W}(R,S)$ will be denoted by $[u,v]$, for $(u,v) \in R^* \times S^*$. The following lemma gives some elementary properties of $\mathcal{W}(R,S)$.

Lemma 2.2.

(i) $[u, v]^4 = [1, 1]$, for any $[u, v] \in \mathcal{W}(R, S)$.

(ii) If $-1 \in R^{*2}$ then $\mathcal{W}(R, S) \simeq R^{*}/R^{*4}$.

(iii) $\mathcal{W}(R, S)$ is trivial if and only if $R^{*} = R^{*2}$.

(iv) $\mathcal{W}(R, S)$ has exponent 2 if and only if $R^{*2} = N(S^{*}) \subsetneq R^{*}$.

(v) $\mathcal{W}(R, S)$ has exponent 4 if and only if $R^{*2} \subsetneq N(S^{*})$.

Proof. (i) For $(u, v) \in R^{*} \times S^{*}$ take $w = N(v)u^{-2}v^{-2} \in S^{*}$ and $\lambda = N(v)^{-2}u^4 \in R^{*}$. Then, we have $[u, v]^4 = [u^4, v^4] = [N(w)u^4, \lambda w^2 v^4] = [1, 1]$.

(ii) Assume that $-1 = \zeta^2 \in R^{*2}$ and let $\varphi : R^{*} \longrightarrow \mathcal{W}(R, S)$ be the mapping defined by $\varphi(\lambda) = [1, v_\lambda]$, where $v_\lambda = 2^{-1}(1 + \lambda) + 2^{-1}\zeta(1 - \lambda)i$, for $\lambda \in R^{*}$. Clearly φ is a group homomorphism.

We show that $\ker\varphi = R^{*4}$. In fact, if $\lambda \in \ker\varphi$ then $[1, v_\lambda] = [1, 1]$ and there exist $\mu \in R^{*}$ and $w \in S^{*}$ such that $v_\lambda = \mu w^2$ and $N(w) = 1$. Consequently, we have $\lambda = N(v_\lambda) = \mu^2 N(w)^2 = \mu^2$ and $v_{\lambda^2} = v_\lambda^2 = \mu^2 w^4 = \lambda w^4$. Consider the R-algebra homomorphism $\theta : S \rightarrow R$ given by $\theta(i) = \zeta$. Thus we have $\lambda^2 = 2^{-1}(1 + \lambda^2) + 2^{-1}\zeta(1 - \lambda^2)\zeta = \theta(v_{\lambda^2}) = \theta(\lambda w^4) = \lambda\theta(w)^4$, which implies $\lambda = \theta(w)^4 \in R^{*4}$. Conversely, if $\lambda = \mu^4 \in R^{*4}$, then $[1, v_\lambda] = [1, \mu^{-2}v_\lambda] = [1, \mu^{-2}v_{\mu^4}] = [1, (\mu^{-1}v_{\mu^2})^2] = [1, 1]$, since $N(\mu^{-1}v_{\mu^2}) = 1$. So, $\lambda \in \ker\varphi$.

Finally, given $[u, v] \in \mathcal{W}(R, S)$, put $\lambda = u^2\theta(v^2)N(v)^{-1} \in R^{*}$, $\mu = u^2\theta(v)N(v)^{-1} \in R^{*}$ and $w = \bar{v}_{u^{-1}} = 2^{-1}(1 + u^{-1}) - 2^{-1}\zeta(1 - u^{-1})i \in S^{*}$. Then we have $N(w) = u^{-1}$, $v_\lambda = u^2\theta(v)N(v)^{-1}(\bar{v}_{u^{-1}})^2 v = \mu w^2 v$ and $\varphi(\lambda) = [1, v_\lambda] = [N(w)u, \mu w^2 v] = [u, v]$. Thus φ is surjective and induces a group isomorphism $R^{*}/R^{*4} \simeq \mathcal{W}(R, S)$.

(iii) Assume that $\mathcal{W}(R, S) = \{[1, 1]\}$. Then, for any $u \in R^{*}$, $(2u, i) \in \mathcal{W}(R, S)$ and so there exist $\lambda \in R^{*}$ and $w \in S^{*}$ such that $N(w) = 2u$ and $\lambda w^2 = i$. If $w = \mu_0 + \mu_1 i$ we easily get $\mu_0^2 = \mu_1^2$ and hence $2u = 2\mu_0^2$. Thus $u = \mu_0^2 \in R^{*2}$ and so $R^{*} = R^{*2}$. The converse follows trivially from (ii).

(iv) Assume that $R^{*2} = N(S^{*}) \subsetneq R^{*}$. Let $[u, v] \in \mathcal{W}(R, S)$ with $v = r_0 + r_1 i$ and $a = N(v) = \mu^2 \in R^{*2}$. Take $\lambda = u^2 a^{-1} \in R^{*}$ and $w = (u\mu)^{-1}(r_0 - r_1 i) \in S^{*}$. Then $N(w) = u^{-2}$ and we easily get $[u, v]^2 = [u^2, v^2] = [N(w)u^2, \lambda w^2 v^2] = [1, 1]$. The assertion follows from (iii).

Conversely, suppose that $\mathcal{W}(R, S)$ has exponent 2. Let $v = r_0 + r_1 i \in S^{*}$ with $N(v) = a$ and take $\lambda = 2^{-1}a^{-2} \in R^{*}$ and $w = (r_0 + r_1) + (r_0 - r_1)i \in S$. Thus $N(w) = 2a \in R^{*}$ (so $w \in S^{*}$) and $[1, 1] = [1, v]^2 = [1, v^2] = [N(w), \lambda w^2 v^2] = [2a, i]$. Following the same way as in (iii) we get $a \in R^{*2}$. This obviously gives $N(S^{*}) = R^{*2} \subsetneq R^{*}$.

(v) It is a trivial consequence of (i), (iii) and (iv).

For any cyclic quartic extension (A, σ) of R, which has a normal basis, choose one of such bases $\{\alpha_i = \sigma^i(\alpha) : 0 \leq i \leq 3\}$ of A over R with $\sum_{i=0}^{3}\alpha_i = 1$. Denote by (u_A, v_A) the corresponding pair in $R^{*} \times S^{*}$ obtained from (A, σ, α) as usually. We define $\psi : NB(\mathbb{Z}/4\mathbb{Z}, R) \to W(R,S)$ by $\psi([A,\sigma]) = [u_A, iv_A]$. This is a well-defined mapping by Lemma 2.1. Now we have the main result of this section.

Theorem 2.3. The mapping $\psi : NB(\mathbb{Z}/4\mathbb{Z}, R) \to W(R,S)$ is an isomorphism of abelian groups.

Proof. We firstly show that ψ is a group homomorphism. Given $[A,\sigma], [B,\tau] \in NB(\mathbb{Z}/4\mathbb{Z}, R)$, let $\{\alpha_i = \sigma^i(\alpha) : 0 \le i \le 3\}$ and $\{\beta_i = \tau^i(\beta) : 0 \le i \le 3\}$ be normal bases of A and B over R, respectively, with $\sum_{i=0}^{3} \alpha_i = \sum_{i=0}^{3} \beta_i = 1$. So, $\{\gamma_i = (\sigma^i \otimes id)(\gamma) : 0 \le i \le 3\}$ with $\gamma = \sum_{i=0}^{3} \sigma^{-i}(\alpha) \otimes \tau^i(\beta)$ is a normal basis of $C = (A \otimes B)^{\sigma^{-1} \otimes \tau}$ over R and $\sum_{i=0}^{3} \gamma_i = 1$. Consider $\{1, x, e_0, e_1\}$, $\{1, y, f_0, f_1\}$ and $\{1, z, g_0, g_1\}$ the canonical bases associated with (A, σ, α), (B, τ, β) and $(C, \sigma \otimes id, \gamma)$, respectively. Let (u_A, v_A), (u_B, v_B) and (u_C, v_C) the corresponding pairs in $R^* \times S^*$. By a direct computation we easily see that $z = x \otimes y$, $g_0 = 2^{-1}[e_0 \otimes (f_0 - f_1) - e_1 \otimes (f_0 + f_1)]$, $u_C = u_A u_B$ and $v_C = i v_A v_B$. Thus, $\psi([A,\sigma] \cdot [B,\tau]) = \psi([C, \sigma \otimes id]) = [u_C, i v_C] = [u_A u_B, -v_A v_B] = [u_A, i v_A][u_B, i v_B] = \psi([A,\sigma])\psi([B,\tau])$.

Clearly, ψ is surjective since $\psi([A_{u,-iv}, \rho]) = [u, v]$ for any $[u, v] \in W(R,S)$ (Remark 1.3).

Finally, we show that ψ is injective. Suppose that $[A,\sigma] \in \ker\psi$. Thus $[u_A, i v_A] = [1, 1]$ and there exist $\lambda \in R^*$ and $w \in S^*$ such that $N(w)u_A = 1$ and $\lambda w^2 v_A = -i$. Put $w = \mu_0 + \mu_1 i$ and define $\lambda_0 = 4^{-1}(1 + \lambda N(w) + 2\mu_0)$, $\lambda_1 = 4^{-1}(1 - \lambda N(w) - 2\mu_1)$, $\lambda_2 = 4^{-1}(1 + \lambda N(w) - 2\mu_0)$ and $\lambda_3 = 4^{-1}(1 - \lambda N(w) + 2\mu_1)$. Then $\sum_{i=0}^{3} \lambda_i = 1$, $w = (\lambda_0 - \lambda_2) - (\lambda_1 - \lambda_3)i$ and $\lambda N(w) = (\lambda_0 + \lambda_2) - (\lambda_1 + \lambda_3) \in R^*$. It follows that the circulant matrix $(\lambda_{j-i (\mathrm{mod}\, 4)})$, $0 \le i, j \le 3$, is invertible and it allows us to define another normal basis $\{\beta_i = \sigma^i(\beta) : 0 \le i \le 3\}$ of A over R with $\sum_{i=0}^{3} \beta_i = 1$, where $\beta = \sum_{i=0}^{3} \lambda_i \alpha_i$. Consequently, a pair (u_1, v_1) is obtained in $R^* \times S^*$ from (A, σ, β). Now, the proof of Lemma 2.1 gives us $(u_1, v_1) = (N(w), \lambda w^2)(u_A, v_A) = (1, -i)$. Therefore, the corresponding canonical basis $\{1, y, f_0, f_1\}$ associated with (A, σ, β) satisfies $y^2 = N(-i) = 1$, $f_0^2 = f_1^2 = 1$, $yf_0 = -f_1$, $yf_1 = -f_0$ and $f_0 f_1 = -y$. Since $\beta = 4^{-1}(1 + y + f_0 - f_1)$ it is now easy to verify that $\{\beta_0, \beta_1, \beta_2, \beta_3\}$ is a set of pairwise orthogonal idempotents of A whose sum equals 1. Hence, (A, σ) is naturally isomorphic to $(R \times R \times R \times R$, cyclic shift$)$ and the proof is complete.

As a consequence of Lemma 2.2 and Theorem 2.3 we have the following corollary, whose part (i) is well-known.

Corollary 2.4.

(i) If $-1 \in R^{*2}$ then $NB(\mathbb{Z}/4\mathbb{Z}, R) \simeq R^*/R^{*4}$.

(ii) $NB(\mathbb{Z}/4\mathbb{Z}, R)$ is trivial if and only if $R^* = R^{*2}$.

(iii) $NB(\mathbb{Z}/4\mathbb{Z}, R)$ has exponent 2 if and only if $R^{*2} = N(S^*) \subsetneq R^*$.

(iv) $NB(\mathbb{Z}/4\mathbb{Z}, R)$ has exponent 4 if and only if $R^{*2} \subsetneq N(S^*)$.

References

[1] S. U. CHASE, D. K. HARRISON and A. ROSENBERG; Galois theory and Galois cohomology of commutative rings, Mem. AMS 52 (1968), 1-19.

[2] D. R. ESTES and R. M. GURALNICK; Module equivalences: local to global when primitive polynomials represent units, J. of Algebra 77 (1982), 138-157.

[3] D. K. HARRISON; Abelian extensions of commutative ring, Mem. AMS 52 (1968), 66-79.

[4] A. PAQUES: On the Primitive Element and Normal Basis Theorems, Comm. in Algebra, 16 (1988), 443-455.

[5] O. VILLAMAYOR and D. ZELINSKY; Galois theory for rings with finitely many idempotents, Nagoya Math. J. 27 (1966), 721-731.

RELATÓRIOS TÉCNICOS — 1990

01/90 — Harmonic Maps Into Periodic Flag Manifolds and Into Loop Groups — *Caio J. C. Negreiros.*

02/90 — On Jacobi Expansions — *E. Capelas de Oliveira.*

03/90 — On a Superlinear Sturm–Liouville Equation and a Related Bouncing Problem — *D. G. Figueiredo* and *B. Ruf.*

04/90 — $F-$ Quotients and Envelope of $F-$Holomorphy — *Luiza A. Moraes, Otília W. Paques* and *M. Carmelina F. Zaine.*

05/90 — S-Rationally Convex Domains and The Approximation of Silva-Holomorphic Functions by $S-$Rational Functions — *Otília W. Paques* and *M. Carmelina F. Zaine.*

06/90 — Linearization of Holomorphic Mappings On Locally Convex Spaces — *Jorge Mujica* and *Leopoldo Nachbin.*

07/90 — On Kummer Expansions — *E. Capelas de Oliveira.*

08/90 — On the Convergence of SOR and JOR Type Methods for Convex Linear Complementarity Problems — *Alvaro R. De Pierro* and *Alfredo N. Iusem.*

09/90 — A Curvilinear Search Using Tridiagonal Secant Updates for Unconstrained Optimization — *J. E. Dennis Jr., N. Echebest, M. T. Guardarucci, J. M. Martínez, H. D. Scolnik* and *C. Vacchino.*

10/90 — The Hypebolic Model of the Mean × Standard Deviation "Plane" — *Sueli I. R. Costa* and *Sandra A. Santos.*

11/90 — A Condition for Positivity of Curvature — *A. Derdzinski* and *A. Rigas.*

12/90 — On Generating Functions — *E. Capelas de Oliveira.*

13/90 — An Introduction to the Conceptual Difficulties in the Foundations of Quantum Mechanics a Personal View — *V. Buonomano.*

14/90 — Quasi-Invariance of product measures Under Lie Group Perturbations: Fisher Information And L^2-Differentiability — *Mauro S. de F. Marques* and *Luiz San Martin.*