

GALOIS EXTENSIONS OF GRADED RINGS

LHOUSAIN EL FADIL

RÉSUMÉ. Nous étudions la notion de séparabilité et les propriétés galoisiennes des produits croisés, et en particulier pour des extensions fortement graduées.

ABSTRACT. We investigate separability and Galois theory of crossed product extensions. In particular, we generalize some separability and Galois theory results on graded field extensions.

Introduction

Let $(\Gamma, +)$ be an abelian group and R be a unitary commutative graded ring with respect to Γ , that is, $R = \bigoplus_{\sigma \in \Gamma} R_{\sigma}$ such that for every $(\sigma, \tau) \in \Gamma^2$, R_{σ} is a R_0 -submodule of R and $R_{\sigma}R_{\tau} \subseteq R_{\sigma+\tau}$. Let

$$\Gamma_R = \{\sigma \in \Gamma \mid R_{\sigma} \neq 0\} \quad \text{and} \quad R^h = \bigcup_{\sigma \in \Gamma} R_{\sigma},$$

where R^h is the set of homogeneous elements of R . For every non-zero homogeneous element x in R_{σ} , we write $\deg(x) = \sigma$ and call it the *degree* of x . The graded ring R is said to be a *strongly graded ring* with respect to the group Γ if every non-zero homogeneous component of R contains an invertible element. When this occurs, Γ_R is a subgroup of Γ , called the *graded group* of R , and for every $\sigma \in \Gamma_R$, R_{σ} is a free R_0 -module of rank 1. So, for every $\sigma \in \Gamma_R$, there exists a non-zero element $u_{\sigma} \in R_{\sigma}$ such that $R_{\sigma} = R_0 u_{\sigma}$. Let $(\sigma, \tau) \in \Gamma_R^2$. Since $\deg(u_{\sigma} u_{\tau}) = \sigma + \tau$, there exists a map $c : \Gamma_R^2 \longrightarrow R_0^*$, defined by $u_{\sigma} u_{\tau} = c_{\sigma, \tau} u_{\sigma+\tau}$, where R_0^* is the group of the invertible elements of R_0 . In that way, R is a crossed product of Γ and R_0 , that we shall denote by $R_0[\Gamma_R, c]$. The graded ring R is said to be a *graded field* if $1 \neq 0$ and every non-zero homogeneous element of R is invertible. In particular, every graded field is a strongly graded ring, R_0 is a field and R_{σ} is a R_0 -vector space of dimension 1, for every $\sigma \in \Gamma_R$.

Throughout this paper, R is a strongly graded ring with graded group $\Gamma_R = \Gamma$, which is an arbitrary abelian group. For every $\sigma \in \Gamma$, let $u_{\sigma} \in R_{\sigma}$ be an invertible element. Then, $R_{\sigma} = R_0 u_{\sigma}$. In Section 1, for a graded R -module M , we give a criterion to test if M is a free R -module. In particular, we obtain Corollary 2, given in [1, p. 30], and Proposition 2.1, given in [7]. In the second section, we investigate separability of strongly graded extensions. We characterize separability of a graded ring extension via its ramification index and its homogeneous component of degree 0. We generalize some separability results given in [7] and in [4]. In the third section, we assume that R_0 is a

principal domain, and we show that every homogeneous element which is integral over R has its minimal polynomial over R . We characterize separability of such an element via its minimal polynomial. We conclude this paper with Theorem 4.4, in which we characterize Galois strongly graded extensions.

1. Strongly graded extensions

Let Λ be a Γ -set. A *graded R -module M with respect to Λ* is an R -module with a direct sum decomposition as abelian groups $M = \bigoplus_{\lambda \in \Lambda} M_\lambda$ such that for every (σ, λ) in $\Gamma \times \Lambda$, M_λ is a subgroup of M and $R_\sigma M_\lambda \subset M_{\sigma * \lambda}$. Set $\Lambda = \bigcup_{i \in I} \Gamma \lambda_i$ (disjoint). For every $i \in I$, let $M_i = \bigoplus_{\sigma \in \Gamma} M_{\sigma * \lambda_i}$. Then every M_i is a graded submodule of M and $M = \bigoplus_{i \in I} M_i$.

Lemma 1.1. *Let M be a graded R -module, with respect to a faithful cyclic Γ -set Λ . Also, let $\lambda \in \Lambda$ and $(e_j)_{j \in J}$ be a subset of M_λ . Then $(e_j)_{j \in J}$ is a R -free set (resp. a generator set) of the R -module M if and only if it is a R_0 -free (resp. a generator set) of the R_0 -module M_λ .*

Proof. Assume that $(e_j)_{j \in J}$ is a set of generators of the R_0 -module M_λ . Since every u_σ is an invertible element, $u_\sigma M_\lambda = M_{\sigma * \lambda}$. So, $(u_\sigma e_j)_{j \in J}$ is a set of generators of the R_0 -module $M_{\sigma * \lambda}$, and then M is generated by $(e_j)_{j \in J}$ as an R -module.

Conversely, let $m \in M_\lambda$. Since $(e_j)_{j \in J}$ is a set of generators of the R -module M , there exists $(r_1, \dots, r_n) \in R^n$ such that $m = \sum_{j=1}^n r_j e_j$. Consider its λ -homogeneous component. Then there exists $(x_1, \dots, x_n) \in R_0^n$ such that $m = \sum_{j=1}^n x_j e_j$. Besides this, let $(x_1, \dots, x_n) \in R^n$ be such that $\sum_{j=1}^n x_j e_j = 0$. For every $1 \leq j \leq n$, let $x_j = \sum_{\sigma \in \Gamma} x_{j,\sigma}$ be its decomposition as a sum of homogeneous elements of R . For every $\sigma \in \Gamma$, consider the $\sigma * \lambda$ -homogeneous component of $\sum_{j=1}^n x_j e_j = 0$. Then

$$\sum_{j=1}^n u_\sigma^{-1} x_{j,\sigma} e_j = 0.$$

So, for every $1 \leq j \leq n$, we have $x_{j,\sigma} = 0$. Consequently, $x_j = 0$ for every $1 \leq j \leq n$, and then $(e_j)_{j \in J}$ is a R -free set. $\square$

Proposition 1.2. *Let M be a graded R -module with respect to a faithful Γ -set Λ . Let $\Lambda = \bigcup_{i \in I} \Gamma * \lambda_i$ (disjoint union). For every $i \in I$, let $M_i = \bigoplus_{\sigma \in \Gamma} M_{\sigma * \lambda_i}$. If M_{λ_i} is a free R_0 -module for every $i \in I$, then M is a graded free R -module. In particular, if R is a graded field, then every graded R -module is a free R -module.*

Proof. Since $M = \bigoplus_{i \in I} M_i$ and M_i is a graded R -module for every $i \in I$, we can assume without loss of generality that Λ is a faithful transitive Γ -set. Then we can use Lemma 1.1 to conclude the proof. $\square$

Let S be a strongly graded ring with graded group Δ . We say that S/R is a *strongly graded extension with graded groups Γ and Δ respectively* if Γ is a normal subgroup of Δ , S is a faithful R -algebra and for every $\sigma \in \Gamma$, we have $R_\sigma \subseteq S_\sigma$.

Corollary 1.3. *Let S/R be a strongly graded extension. If S_0 is a free R_0 -module, then S is a free R -algebra.*

Proof. Let Δ be the graded group of S and $\Delta/\Gamma = \{\bar{\sigma}_i \mid i \in I\}$. Then $S = \bigoplus_{i \in I} S_i$, where $S_i = \bigoplus_{\sigma \in \Gamma} S_{\sigma + \sigma_i}$ for every $i \in I$. Since S/R is a strongly graded extension, for every $\sigma \in \Delta$, there exists an invertible element w_σ of S_σ such that

$$S = \bigoplus_{\sigma \in \Delta} S_0 w_\sigma.$$

So, for every $i \in I$, we have $S_i \simeq S_0 \otimes_{R_0} R$. Consequently, if S_0 is a free R_0 -module, then S_i is a free R -module. Therefore, if S_0 is a free R_0 -module, then S is a free R -algebra. $\square$

Let S/R be a strongly graded extension with graded groups Γ and Δ respectively. For a subgroup Λ such that $\Gamma \subseteq \Lambda \subseteq \Delta$, we define $S(\Lambda) := \bigoplus_{x \in \Lambda} S_x$. In particular, $S(\Gamma)$ is a graded ring with graded group Γ , and we have $R \subseteq S(\Gamma) \subseteq S$. In that way, we split the extension S/R into the two strongly graded extensions $R \subset S(\Gamma)$ and $S(\Gamma) \subset S$. The first one is made of graded rings which are graded over the same group Γ , while in the second one $S(\Gamma)$ and S have the same homogeneous components of degree 0, namely S_0 .

Lemma 1.4. *Let S/R be a strongly graded extension with graded groups Γ and Δ respectively. Then S is a crossed product of $S(\Gamma)$ by the group Δ/Γ . In particular, S is a free $S(\Gamma)$ -module.*

Proof. We can define a new grading on S over the group Δ/Γ by taking

$$S_\sigma := \bigoplus_{x \in \sigma} S_x$$

for every $\sigma \in \Delta/\Gamma$. Obviously S is a Δ/Γ -graded ring whose homogeneous component of degree 0 is $S(\Gamma)$. For every $\sigma \in \Delta/\Gamma$, fix $x \in \sigma$ and $u_x \in S_x \subset S_\sigma$ an invertible element. For each $(\sigma, \tau) \in (\Delta/\Gamma)^2$ there exists $c_{\sigma, \tau} \in S(\Gamma)_0 \setminus \{0\}$ such that $u_\sigma u_\tau = c_{\sigma, \tau} u_{\sigma + \tau}$. The commutativity and associativity of S imply that

$$c_{\sigma, \tau} = c_{\tau, \sigma} \quad \text{and} \quad c_{\sigma, \tau} \cdot c_{\sigma + \tau, \tau'} = c_{\tau, \tau'} \cdot c_{\sigma, \tau + \tau'}$$

for all $(\sigma, \tau, \tau') \in (\Delta/\Gamma)^3$. Hence S is a crossed product of $S(\Gamma)$ by the group Δ/Γ . $\square$

The following corollary generalizes Corollary 2 given in [1, p. 30], and Proposition 2.1 given in [7].

Corollary 1.5. *Let S/R be a strongly graded extension with graded groups Γ and Δ respectively such that S_0 is a free R_0 -module of finite rank and $[\Delta : \Gamma]$ is finite. Then S is a free R -module of finite rank and*

$$[S : R] = [S_0 : R_0][\Delta : \Gamma].$$

Remark 1.6. $[\Delta : \Gamma]$ is called the *ramification index* of the extension S/R and $[S_0 : R_0]$ is called its *residual degree*. The terminology is borrowed from algebraic number theory though it is only remotely related.

2. Separability of strongly graded extensions

In [7], Hwang and Wadsworth have given some separability results for graded field extensions S/R with graded groups Γ and Δ respectively, such that Δ is a torsion free abelian group. In that case, since S_0 is a domain, so are S and R . We have generalized this result to any extension of graded field in [4], that is, when the graded group is not necessarily torsion free. In this section, we give some separability results of strongly graded extensions with respect to arbitrary abelian groups. In particular, we obtain the separability results given in [7] and in [4].

Let S be a free R -algebra of finite rank. Every $x \in S$ induces an R -homomorphism l_x of S defined by $l_x(s) = xs$ for every $s \in S$. Let $T_{S/R}(x) = \text{tr}(l_x)$ be the trace of l_x . For a free R -submodule M of S , $T_{S/R}$ induces a bilinear form of M by $T_{M/R}(x, y) = T_{S/R}(xy)$ for every $(x, y) \in M^2$. The determinant of the bilinear form $T_{M/R}$ with respect to a R -basis $(e_1, \dots, e_n)$ of M is denoted by $D(e_1, \dots, e_n)$ and called the *discriminant* of $(e_1, \dots, e_n)$. The discriminant plays a key role to investigate the separability of commutative algebras. For more details, see [6, 5].

Lemma 2.1. *Let S/R be a strongly graded extension such that S_0 is a free R_0 -module. If S/R is separable, then S is a free R -module of finite rank.*

Proof. By Corollary 1.3, it follows that S is a free R -module. Then by [9, Proposition III.3.2], it follows that S is a finitely generated R -module. $\square$

In the sequel of the paper, S/R is a strongly graded extension such that S_0 is a free R_0 -module of finite rank and Δ/Γ is a finite group. In particular, S is a free R -module of finite rank.

Theorem 2.2. *Let S/R be a strongly graded extension with graded groups Γ and Δ respectively. Then S/R is separable if and only if S_0/R_0 is separable and $[\Delta : \Gamma]$ is an invertible element of R_0 .*

Proof. From [9, Theorem III 4.7, p. 89], S/R is separable if and only if the trace map $T_{S/R}$ induces a non-singular bilinear form of S . Let $\Delta/\Gamma = \{\bar{\sigma}_1, \dots, \bar{\sigma}_n\}$, and for every $1 \leq i \leq n$, let $w_{\sigma_i} \in S_{\sigma_i}$ be an invertible element. Specify $\sigma_1 = 0$ and $w_{\sigma_1} = 1$. Then S is a free $S(\Gamma)$ -module with basis $(w_{\sigma_1}, w_{\sigma_2}, \dots, w_{\sigma_n})$. Let M be the R -module generated by $(w_{\sigma_1}, w_{\sigma_2}, \dots, w_{\sigma_n})$. So, $S \simeq S(\Gamma) \otimes_R M$ as R -modules. By [6, Proposition 3, p. 95],

$$D_R(S) = (D_R(S(\Gamma)))^n (D_R(M))^f,$$

where $f = [S_0 : R_0]$. Consequently, $D_R(S) = R$ if and only if $D_R(M) = R$ and $D_R(S(\Gamma)) = R$. Since $S(\Gamma) \simeq S_0 \otimes_{R_0} R$, by [6, Proposition 1, p. 95],

$$D_R(S(\Gamma)) = D_{R_0}(S_0)R.$$

Since R_0 is a field, $D_R(S(\Gamma)) = S(\Gamma)$ if and only if $D_{R_0}(S_0) = R_0$, that is, if and only if S_0/R_0 is separable. Besides this, for every (i, j) , there exists an invertible element c_{σ_i, σ_j} of $S(\Gamma)$ such that $w_{\sigma_i} w_{\sigma_j} = c_{\sigma_i, \sigma_j} w_{\sigma_i + \sigma_j}$. Hence,

$$T_{S/S(\Gamma)}(u_{\sigma_i} u_{\sigma_j}) = n c_{\sigma_i, \sigma_j} \delta_0^{\sigma_i + \sigma_j}.$$

Consequently, the determinant of the bilinear form $T_{M/R}$, with respect to the basis $(u_{\sigma_1}, \dots, u_{\sigma_n})$, is $D(u_{\sigma_1}, \dots, u_{\sigma_n}) = sn^n$, where s is an invertible element of R . So, $D_R(M) = R$ if and only if n is invertible in R_0 . $\square$

Corollary 2.3. *Let S/R be a strongly graded extension.*

- (1) *S/R is separable if and only if $S(\Gamma)/R$ and $S/S(\Gamma)$ are separable.*
- (2) *$S/S(\Gamma)$ is separable if and only if Δ/Γ is a finite group and $[\Delta : \Gamma]$ is invertible in R_0 .*
- (3) *$S(\Gamma)/R$ is separable if and only if S_0/R_0 is separable.*

Proof. (1) Keeping the same notations as in the previous theorem, we have

$$D_R(S) = (D_R(S(\Gamma)))^n (D_R(M))^f,$$

where $f = [S_0 : R_0]$. So, $D_R(S) = R$ if and only if $D_R(M) = R$. Since S is an $S(\Gamma)$ -module generated by M , we have $S \simeq S(\Gamma) \otimes_R M$ as R -modules. Hence

$$D_{S(\Gamma)}(S) = D_R(M)S(\Gamma).$$

Consequently, $D_R(M) = R$ if and only if $D_{S(\Gamma)}(S) = S(\Gamma)$, that is, if and only if $S/S(\Gamma)$ is separable.

(2) This follows from $S_0 = S(\Gamma)_0$.

(3) This follows from the fact that $S(\Gamma)$ and R have the same graded group. $\square$

Corollary 2.4. *Let S/R be a strongly graded extension. Then S/R is separable if and only if S_p/R_p is separable for every maximal ideal p of R_0 .*

Proof. By [9, Proposition III.2.4], if S/R is separable, then so is S_p/R_p for every maximal ideal p of R_0 .

Conversely, assume that S_p/R_p is separable for every maximal ideal p of R_0 . Then, by Theorem 2.2, S_{0p}/R_{0p} is separable for every maximal ideal p of R_0 and $[\Delta : \Gamma]$ is an invertible element of R_0 . So, S/R is separable. $\square$

Examples 2.5. (1) Let A/T be a commutative ring extension such that A is a free T -module of finite rank. Let $R = T[X, X^{-1}]$ and $S = A[X^{\frac{1}{n}}, X^{-\frac{1}{n}}]$. Then S/R is separable if and only if A/T is separable and n is invertible in T .

(2) In particular, if T is a field of characteristic p , then S/R is separable if and only if A/T is separable and p does not divide n .

(3) Let Γ and Δ be two abelian groups such that $\Gamma \subset \Delta$ and $[\Delta : \Gamma]$ is a finite. Then $A[\Delta]/T[\Gamma]$ is separable if and only if A/T is separable and $[\Delta : \Gamma]$ is invertible in T . In particular, if T is a field of characteristic p , then $A[\Delta]/T[\Gamma]$ is separable if and only if A/T is separable and p does not divide $[\Delta : \Gamma]$.

3. Separability and polynomial

In this section we assume that R_0 is a principal domain and S is a graded free R -algebra. We show that every homogeneous element of S which is integral over R has

its minimal polynomial over R . We characterize the separability of such elements and of simple Galois extensions.

Let $r \in \Delta$, and $P = \sum_{i=0}^n a_i X^i$ be a polynomial of $R[X]$ of degree n . Then P is said to be r -homogenizable if each a_i is a homogeneous element of R and for every (i, j) such that $a_i \neq 0$ and $a_j \neq 0$, we have $\deg(a_i) + ir = \deg(a_j) + jr$. Set $\lambda = \deg(a_n) + nr$. Then λ is called the *grade* of the homogenizable polynomial P . For every $\lambda \in \Gamma\langle r \rangle$, let $R[X]_\lambda$ be the set of r -homogenizable polynomials of grade λ . Then $R[X] = \sum_{\lambda \in \Gamma\langle r \rangle} R[X]_\lambda$ is a graded ring with respect to $\Gamma\langle r \rangle$, which we will denote

$R[X]^{(r)}$. In that way, P is a homogeneous element of grade λ of $R[X]^{(r)}$. In particular, every polynomial of $R[X]$ splits as a sum of homogenizable polynomials of $R[X]^{(r)}$.

Let $\alpha \in S$, and I_α be the kernel of the homomorphism $s_\alpha : R[X] \longrightarrow R[\alpha]$, defined by $s_\alpha(P(X)) = P(\alpha)$. If α is integral over R , then $I_\alpha \neq 0$. Moreover, if I_α is a principal ideal of $R[X]$, then I_α is generated by a monic polynomial, which is called the *minimal polynomial* of α over R .

Proposition 3.1. *Let $\alpha \in S$ be a homogeneous element of degree σ , which is integral over R . If R_0 is a principal domain, then the minimal polynomial of α over R is homogenizable.*

Proof. First we show that $R[\alpha]$ is a graded R -algebra. Let $x = \sum_{i=0}^n r_i \alpha^i \in R[\alpha]$. For every i , decompose r_i as a sum of homogeneous elements of R . Since α is a homogeneous element of S ,

$$x = \sum_{g \in \Gamma\langle \sigma \rangle} P_g(\alpha),$$

where every $P_g(X)$ is a σ -homogenizable polynomial of $R[X]$. Hence $R[\alpha]$ contains the homogeneous components of x , and then it is a graded R -algebra with respect to the semigroup $\Gamma\langle \sigma \rangle$.

Besides this, since α is integral over R , $R[\alpha]$ is a finitely generated R -module. The fact that R_0 is a principal domain and every homogeneous component of $R[\alpha]$ is a torsion free finitely generated R_0 -module implies that every homogeneous component of $R[\alpha]$ is a free R_0 -module. So, by Proposition 1.2, $R[\alpha]$ is a free R -module of finite rank.

Let $f_\alpha(X)$ be the characteristic polynomial of $l_\alpha : R[\alpha] \longrightarrow R[\alpha]$, the R -endomorphism defined by $l_\alpha(x) = \alpha x$. By an account of rank, $f_\alpha(X)$ is a monic polynomial with minimal degree, of $R[X]$, which annihilates α . The Euclidean algorithm implies that I_α is a principal ideal generated by $f_\alpha(X)$. So $f_\alpha(X)$ is the minimal polynomial of α over R . Let $\mu_\alpha(X)$ be the $n\sigma$ -homogeneous component of $f_\alpha(X)$ in the graded ring $R[X]^{(\sigma)}$. Then $\mu_\alpha(X)$ is a monic polynomial of $R[X]$, of the same degree as $f_\alpha(X)$, and such that $\mu_\alpha(\alpha) = 0$. The uniqueness of the minimal polynomial then implies that $f_\alpha(X) = \mu_\alpha(X)$ is a homogenizable polynomial. $\square$

Proposition 3.2. *Let $\alpha \in S$ be a homogeneous element of degree σ , which is integral over R . Then $R[\alpha]/R$ is separable if and only if the discriminant of $\mu_\alpha(X)$ is invertible in R .*

Proof. Let $x_1, \dots, x_n$ be the roots of $\mu_\alpha(X)$ in some commutative extension of R , counted with its multiplicity order. Since $R[\alpha]/R$ is separable, $T_{R[\alpha]/R}$ induces a non-singular bilinear form of $R[\alpha]$. Hence the discriminant $D(1, \alpha, \dots, \alpha^{n-1})$ is invertible in R , where n is the degree of $\mu_\alpha(X)$. Consequently, for every maximal ideal $\mathcal{P}$ of R ,

$$D(\alpha, \dots, \alpha^{n-1}) \neq 0 \pmod{\mathcal{P}},$$

that is, $\bar{\mu}_\alpha(X)$ is a separable polynomial over $R/\mathcal{P}$. Hence $\bar{\mu}_\alpha(X)$ is square-free, that is,

$$\prod_{i \neq j} (x_i - x_j) \neq 0 \pmod{\mathcal{P}}$$

for every maximal ideal $\mathcal{P}$ of R . Thus $\prod_{i \neq j} (x_i - x_j)$ is invertible in R .

Conversely, let $\mu_\alpha(X)$ be invertible in R . Then

$$\prod_{i \neq j} (x_i - x_j) \neq 0 \pmod{\mathcal{P}},$$

for every maximal ideal $\mathcal{P}$ of R , that is, $\bar{\mu}_\alpha(X)$ is a separable polynomial and then $D(1, \alpha, \dots, \alpha^{n-1})$ is invertible in R , that is, $R[\alpha]/R$ is separable. $\square$

4. Galois extension of strongly graded rings

In this section we investigate the Galois theory of strongly graded extensions. In particular, we investigate the Galois theory results given in [7].

Let A be a commutative free R -algebra and G be a finite subgroup of $\text{Aut}_R(A)$ such that $A^G = R$. Denote $A^{(G)}$ the A -algebra with basis $\{e_\sigma \mid \sigma \in G\}$, where e_σ is the idempotent $(\delta_\tau^\sigma)_{\tau \in G}$. Recall that A/R is said to be a G -Galois extension if the following homomorphism h is an isomorphism of A -algebras

$$\begin{aligned} h: A \otimes_R A &\longrightarrow A^{(G)} \\ x \otimes y &\longmapsto \sum_{\sigma \in G} x\sigma(y)e_\sigma. \end{aligned}$$

Proposition 4.1. *Let T/R be a totally ramified graded ring extension ($S_0 = R_0$) with graded groups Γ and Δ , such that Δ is a torsion free abelian group. Let $s \in S_\sigma$ be an invertible homogeneous element, which is integral over R . Let n be the cardinal order of the group $\Gamma\langle\sigma\rangle/\Gamma$. Then $R[s]/R$ is a Galois extension if and only if n is invertible in R_0 and R_0 contains a n -th primitive root ζ_n of 1. In this case, the Galois group of $R[s]/R$ is $G = \{g_1, \dots, g_n\}$, where $g_i(s) = \zeta_n^i s$.*

Proof. Let $a = s^n$. Since the grade of a is $n\sigma \in \Gamma$, there exists $v \in R[s]_0$ such that $a = vu_{n\sigma}$. Since $S_0 = R[s]_0 = R_0$, we have $v \in R$, and then $a \in R$. So,

$$\mu_s(X) = X^n - a$$

is the minimal polynomial of s over R . Since $R[s]/R$ is a Galois extension, it is separable, and then n is invertible in R_0 . Let G be a finite subgroup of $\text{Aut}_R(R[s])$ such that $R[s]/R$ is a G -Galois extension. Then the order of G is equal to n . Hence $\mu_s(X)$ splits in $R[s]$, with simple roots $s_1, \dots, s_n$, where $\frac{s_1}{s}, \dots, \frac{s_n}{s}$ are the distinct roots of $X^n - 1$. Consequently, $\zeta_n \in R[s]_0 = R_0$.

Conversely, assume that n is invertible in R_0 and that R_0 contains ζ_n . Then $s, \zeta_n s, \dots, \zeta_n^{n-1} s$ are the distinct roots of $\mu_s(X)$. Let $G = \langle \sigma \rangle$, where $\sigma(s) = \zeta_n s$. Then G is a finite subgroup of $\text{Aut}_R(R[s])$. Let $y = \sum_{i=0}^{n-1} r_i s^i \in R[s]$. For every $0 \leq k \leq n-1$,

$$\sigma^k(y) = r_0 + \sum_{i=1}^{n-1} r_i \zeta_n^{ik} s^i.$$

So, if $y \in R[s]^G$, then $y = r_0 \in R$, that is, $R[s]^G = R_0$. We compute $\det(h)$, the determinant of the homomorphism h of $R[s] \otimes_R R[s]$ into $R[s]^{(G)}$, and obtain

$$\det(h) = \begin{vmatrix} 1 & s & \cdots & s^{n-1} \\ 1 & \zeta_n s & \cdots & (\zeta_n s)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{n-1} s & \cdots & \zeta_n^{(n-1)^2} s^{n-1} \end{vmatrix} = s^{n(n+1)/2} \prod_{1 \leq i < j \leq n} (\zeta_n^i - \zeta_n^j).$$

Since s is an invertible element and $\prod_{1 \leq i < j \leq n} (\zeta_n^i - \zeta_n^j)$ divides n in R , $\det(h)$ is an invertible element of R , and then $R[s]/R$ is a G -Galois extension. $\square$

For two commutative free R -algebras A and B of rank n and m respectively, let G_1 (resp. G_2) be a finite subgroup of $\text{Aut}_R(A)$ (resp. of $\text{Aut}_R(B)$) such that $A^{G_1} = R$ and $B^{G_2} = R$. Then $G_1 \times G_2$ is a finite subgroup of $\text{Aut}_R(A \otimes_R B)$ such that $(A \otimes_R B)^{G_1 \times G_2} = R$.

Lemma 4.2. *Under the above hypotheses, $A \otimes_R B$ is a $G_1 \times G_2$ -Galois extension over R if and only if A/R is a G_1 -Galois extension and B/R is a G_2 -Galois extension.*

Proof. Consider the following three homomorphisms:

$$\begin{aligned} h_A : A \otimes A &\longrightarrow A^{(G_1)}, & h_B : B \otimes B &\longrightarrow B^{(G_2)}, \\ x \otimes y &\longmapsto \sum_{\sigma \in G_1} x\sigma(y)e_\sigma & x \otimes y &\longmapsto \sum_{\sigma \in G_2} x\sigma(y)e_\sigma \end{aligned}$$

and

$$\begin{aligned} h : A \otimes_R B \otimes_R A \otimes_R B &\longrightarrow A \otimes_R B^{(G_1 \times G_2)} \\ (a \otimes b) \otimes (a' \otimes b') &\longmapsto \sum_{(\sigma, \tau) \in G_1 \times G_2} a\sigma(a') \otimes b\tau(b') \cdot e_{\sigma, \tau}. \end{aligned}$$

From [2, pp. 101 and 157], $h = h_A \otimes h_B$ and $\det(h) = (\det(h_A))^m (\det(h_B))^n$. Consequently, h is an isomorphism if and only if h_A and h_B are isomorphisms. $\square$

Proposition 4.3. *Let S/R be a strongly graded extension with ramification index 1. Then S/R is a Galois extension if and only if S_0/R_0 is a Galois extension.*

Proof. Since $\Gamma_S = \Gamma$, we have $S \simeq S_0 \otimes_{R_0} R$. Consequently, since R is a free R_0 -algebra, S/R is a Galois extension if and only if S_0/R_0 is a Galois extension. $\square$

The following result generalizes Proposition 3.3, given in [7].

Theorem 4.4. *Let T/R be a totally ramified a strongly graded extension ($T_0 = R_0$) with graded groups Γ and Δ , such that T is a finitely generated R -module and Δ is a torsion free abelian group. Let l be the exponent of Δ/Γ . Then T/R is a Galois*

extension if and only if l is invertible in R_0 and R_0 contains a primitive l -th root ζ_l of 1.

Proof. Let $\Delta/\Gamma = \langle \bar{\sigma}_1 \rangle \cdots \langle \bar{\sigma}_r \rangle$. For $1 \leq i \leq r$, pick u_i any homogeneous invertible element of T of degree σ_i . Since $T = \sum_{\sigma \in \Delta/\Gamma} Ru_\sigma$, the multiplication in T induces an isomorphism of R -algebras

$$\mu : R[u_1] \otimes \cdots \otimes R[u_r] \longrightarrow T.$$

Consequently, T/R is a Galois extension if and only if $R[u_i]/R$ is a Galois extension for every $1 \leq i \leq r$. From Proposition 4.3, $R[u_i]/R$ is a Galois extension if and only if d_i is invertible in R_0 and R_0 contains ζ_{d_i} , where $d_i = [R[u_i] : R]$. Consequently, T/R is a Galois extension if and only if l is invertible in R_0 and R_0 contains ζ_l . $\square$

REFERENCES

- [1] M. Boulagouaz, *Le gradué d'une algèbre à division valuée*, Comm. Algebra **23** (1995), no. 11, 4275–4300.
- [2] N. Bourbaki, *Éléments de mathématique*, Algèbre, Chapitres 1 à 3, Hermann, Paris 1970, xiii+635 pp.
- [3] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Mathematics **181**, Springer-Verlag, Berlin-New York, 1971, iv+157 pp.
- [4] L. El Fadil, *Separability of graded fields*, Int. Math. Forum **1** (2006), no. 1-4, 191–197.
- [5] L. El Fadil, *Discriminant and separability*, preprint CRM 547 (Juliol 2003).
- [6] L. El Fadil and M. Charkani, *Generalization of the discriminant and applications*, Arab. J. Sci. Eng. Sect. A Sci. **29** (2004), no. 1, 93–98.
- [7] Y.-S. Hwang and A. R. Wadsworth, *Algebraic extensions of graded and valued fields*, Comm. Algebra **27** (1999), no. 2, 821–840.
- [8] G. Karpilovsky, *The algebraic structure of crossed products*, North-Holland Mathematics Studies, **142**, Notas de Matemática, **118**, North-Holland Publishing Co., Amsterdam, 1987, x+348 pp.
- [9] M.-A. Knus and M. Ojanguren, *Théorie de la descente et algèbres d'Azumaya*, Lecture Notes in Mathematics **389**, Springer-Verlag, Berlin-New York, 1974, iv+163 pp.
- [10] C. Năstăsescu and F. Van Oystaeyen, *Graded ring theory*, North-Holland Mathematical Library, **28**, North-Holland Publishing Co., Amsterdam-New York, 1982, ix+340 pp.
- [11] C. Năstăsescu, M. Van den Bergh and F. Van Oystaeyen, *Separable functors applied to graded rings*, J. Algebra **123** (1989), no. 2, 397–413.