GALOIS EXTENSION OF CP-GRADED RING EXTENSIONS

L HOUSSAIN EL FADIL

Abstract. In this paper, we investigate galois theory of CP-graded ring extensions. In particular, we generalize some galois results given in [1, 2] and, without restriction to nor graded *fields* nor *torsion free* of the grade groups, we show that some results of graded field extensions given in [3] hold.

Introduction

Let $(\Gamma, +)$ be an abelian group and R a unitary commutative graded ring with respect to Γ, i.e., $R = \oplus_{\sigma\in\Gamma} R_\sigma$ such that R_σ is a R_0-submodule of R and $R_\sigma R_\tau \subset R_{\sigma+\tau}$ for every $(\sigma, \tau) \in \Gamma^2$. Set $\Gamma_R = \{\sigma \in \Gamma \mid R_\sigma \neq 0\}$ and $R^h = \cup_{\sigma\in\Gamma} R_\sigma$ the set of homogeneous elements of R. For every nonzero homogeneous element $x \in R_\sigma$, we write $deg(x) = \sigma$ and we call it the degree of x. If every homogeneous component of R contains an invertible element, then R will call a CP-graded ring. When this occurs, Γ_R is a subgroup of Γ, called the grade of R, and for every $\sigma \in \Gamma_R$, R_σ is a free R_0-module of rank 1, which is generated by an invertible element u_σ. Since for every $(\sigma, \tau) \in \Gamma^2$, $deg(u_\sigma u_\tau) = \sigma + \tau$, there exists a map $c : \Gamma^2 \longrightarrow U(R_0)$ defined by $u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma+\tau}$, where $U(R)$ is the set of invertible element of R. In that way, the CP-graded ring will be denoted by $R_0[\Gamma, c]$. The graded ring R is said to be a graded field if every nonzero homogeneous element in R is invertible. In that case, R_0 is a field and for every $\sigma \in \Gamma$, R_σ is an R_0-vector space of dimension 1.

In [3] Hwang and Wadsworth have given some results of graded fields extensions. Since their goal is to describe an algebraic extension theory of graded fields analogous to what is known for valued fields, they assumed that the grade groups are abelian *torsion free*. In [1, 2], without restriction to *torsion free* of the grade groups, we have shown that some results of graded field extensions given in [3] hold. In this paper, we generalize some of these results to CP-graded ring extensions over a graded field and we give some other results.

Throughout this paper, $R = \sum_{\sigma \in \Gamma} R_0 u_\sigma$ is a graded field with grade group $\Gamma_R = \Gamma$ and S is a commutative graded ring extension, over R, with grade group $\triangle$. In the first section, we show that every homogeneous element of S, which is integral over R has its minimal polynomial over R, and then we characterize separability of such an element. Also, we characterize simple galois extensions of graded rings. In the second section, we characterize separability of CP-graded ring extensions via the discriminant ideal. In particular, we generalize separability results of graded fields given in [2] to any CP-graded algebra over a graded field. We finalize by a classification theorem. In the third section, we investigate galois extensions of CP-graded ring extensions. In particular, without restriction to nor graded *fields* nor *torsion free* of the grade groups, we show some galois results given in [1] and [3] hold.

Prelimenaries

The following proposition generalizes [4, Theorem 3, p. 29].

Proposition 0. 1. *Let S/R be a CP-graded ring extension. Then S is a free R-module such that $[S : R] = [S_0 : R_0][\triangle : \Gamma]$.*

Proof. For a subgroup Λ such that $\Gamma \subseteq \Lambda \subseteq \triangle$, we define $S(\Lambda) := \oplus_{x \in \Lambda} S_x$. In particular, $S(\Gamma)$ is a graded ring with grade group Γ, and we have $R \subseteq S(\Gamma) \subseteq S$. Define a new grading on S over the group $\triangle/\Gamma$ by taking $S_\sigma := \oplus_{x \in \sigma} S_x$, for every $\sigma \in \triangle/\Gamma$. Then S is a $\triangle/\Gamma$-graded ring, whose homogeneous component of degree 0 is $S(\Gamma)$. Since every homogeneous component of S contains an invertible element, $S/S(\Gamma)$ is a CP-graded ring with grade group $\triangle/\Gamma$. In particular, S is a free $S(\Gamma)$-module with a basis $\{w_\sigma\, ,\, \sigma \in \triangle/\Gamma\}$. On the other hand, for every $x \in \Gamma$, let $u_x \in R_x$ be an invertible element, then $S_x = u_x.S_0$. Hence the multiplication of S induces an isomorphism of graded rings $S_0 \otimes_{R_0} R \simeq S(\Gamma)$. In that way, we split the extension S/R into two graded ring extensions $R \subset S(\Gamma)$ and $S(\Gamma) \subset S$. ■

Assume that S is a finitely generated R-module, then $[\triangle : \Gamma]$ is called the ramification index of the extension S/R and $[S_0 : R_0]$ is called its residue degree.
The extension S/R is called a totally ramified graded ring extension if S is a finitely generated R-module and $[S : R] = [\triangle : \Gamma]$, i.e., $S_0 = R_0$.

Recall that for a free R-algebra S of finite rank, every $x \in S$ induces an R-homomorphism l_x of S defined by $l_x(s) = xs$ for every $s \in S$. Define $T_{S/R}(x) = tr(l_x)$ the trace of l_x. Let M be a free R-submodule of S. Then $T_{S/R}$ is a linear form of S, which induces a bilinear form of M defined 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 an R-basis $(e_1,...,e_n)$ of M is denoted by $D(e_1,...,e_n)$, and called the discriminant of $(e_1,...,e_n)$. The discriminant ideal of the R-module M is the principal ideal generated by $D(e_1,...,e_n)$, where $(e_1,...,e_n)$ is an R-basis of M. For more details see [5, 6].

1. Simple extensions of graded rings

In [3], Hwang and Wadsworth have shown that if R is a graded field with grade group is a torsion free abelian group, then R is an integrally closed domain. So every homogeneous integral element of S over R has its minimal polynomial in $R[X]$. In this section, without restriction to *torsion free* of the grade group of R, we extend this result, and then we characterize separability of such an element.

Let $\sigma \in \triangle$ and $P = \sum_{i=0}^{n} a_i X^i$ be a polynomial of $R[X]$ of degree n. P is said to be a σ-homogeneous polynomial if every $a_i \neq 0$, a_i is an homogeneous element of R and for every (i,j) such that $a_i \neq 0$ and $a_j \neq 0$, $deg(a_i) + i\sigma = deg(a_j) + j\sigma$. Let $\lambda = deg(a_n) + n\sigma$, will call the grade of the polynomial P. For every $\lambda \in \Gamma < \sigma >$, let $R[X]_\lambda$ be the set of σ-homogeneous polynomials, of $R[X]$, of grade λ. Then $R[X] = \sum\limits_{\lambda \in \Gamma<\sigma>} R[X]_\lambda$ is a graded ring with respect to the semigroup $\Gamma < \sigma >$, which will denote $R[X]^{(\sigma)}$. In that way $P(X)$ is an homogeneous element of degree λ in the graded ring $R[X]^{(\sigma)}$. In particular, every polynomial of $R[X]$ splits as a sum of σ-homogeneous polynomials of $R[X]$.

Proposition 1. 2. *Let α be an homogeneous element of S of degree σ. If α is integral over R, then α has the minimal polynomial over R, which is σ-homogeneous. So the ideal $I(\alpha) = \{P \in R[X] \,|\, P(\alpha) = 0\}$ of $R[X]$ is a principal ideal of $R[X]$, which is generated by a monic σ-homogeneous polynomial.*

Proof. 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 an homogeneous element of S, $x = \sum\limits_{g \in \Gamma<\sigma>} P_g(\alpha)$, where every $P_g(X)$ is a σ-homogeneous polynomial of $R[X]$, of grade g. Hence $R[\alpha]$ contains the homogeneous components of x. Consequently, $R[\alpha]$ is a graded R-algebra with respect to the semigroup $\Gamma < \sigma >$. Since α is integral over R, $R[\alpha]$ is a finitely generated R-module. From [4, Theorem 3, p. 29], $R[\alpha]$ is a free R-module of finite rank. Let $P_\alpha(X) = det(XI_S - l_\alpha)$ be the characteristic polynomial of the R-homomorphism l_α of $R[\alpha]$, defined by $l_\alpha(x) = \alpha.x$. Since the degree of the polynomial $P_\alpha(X)$ is $[R[\alpha] : R]$, $P_\alpha(X)$ is the minimal polynomial of α over R. Let $\mu_\alpha(X)$

be the $n\sigma$-homogeneous component of $P_\alpha(X)$ in the graded ring $R[X]^{(\sigma)}$. Then $\mu_\alpha(X)$ is a monic polynomial of $R[X]$, of the same degree as $P_\alpha(X)$, such that $\mu_\alpha(\alpha) = 0$. The uniqueness of the minimal polynomial implies that $P_\alpha(X) = \mu_\alpha(X)$ is a σ-homogeneous polynomial. ■

Corollary 1. 3. *Let $s \in S_\sigma$ be an invertible homogeneous element, which is integral over R. Then*
1) $R[s]$ is a CP-graded ring with grade group $\Gamma < \sigma >$.
2) Let d be the cardinal order of $\Gamma < \sigma > /\Gamma$, a a nonzero homogeneous element of R of degree $d\sigma$ and $[R[s] : R] = n$. If s is invertible, then $\mu_s(X) = a^{\frac{n}{d}} H(a^{-1}X^d)$ is the minimal polynomial of s over R, where $H(X) \in R_0[X]$ is the minimal polynomial of $a^{-1}s^d$ over R_0. In particular, $R[s]_0 = R_0[a^{-1}s^d]$.

Proof. 1) Since s is integral over R, from Proposition 1.2, $R[s]$ is a free graded R-algebra of finite rank. Let $\mu_s(X) = X^n + ... + a_0$ be the minimal polynomial of s. Since s is invertible, a_0 is a nonzero homogeneous element of R, and then it is invertible in R. Hence $s^{-1} = -a_0^{-1}(s^{n-1}+...+a_1) \in R[s]$. Therefore, $R[s] = \sum_{g\in\Gamma<\sigma>} R_g$ is a CP-graded ring with grade group $\Gamma < \sigma >$, where $R_g = \sum_{\tau+n\sigma=g} R_\tau s^n$ for every $g \in \Gamma < \sigma >$. From Proposition 0.1, $[R[s] : R] = [R[s]_0 : R_0][\Gamma < \sigma >: \Gamma]$.
2) Set $a_n = 1$ and let $0 \le i < j \le n$ such that $a_i \neq 0$ and $a_j \neq 0$. Since $\mu_s(X)$ is a σ-homogeneous polynomial, $(i-j)\sigma = deg(a_j)-deg(a_i) \in \Gamma$, and then d divides $i - j$. In particular, since $a_0 \neq 0$, if $a_i \neq 0$, then d divides i. So, $\mu_s(X) = \sum_{i=0}^m a_{di}X^{di}$. Therefore, $\mu_s(X) = b\sum_{i=0}^m b^{-1}a^i a_{di}(a^{-1}X^d)^i = bP((a^{-1}X^d))$, where $b = a^{\frac{n}{d}}$ and $n = [R[s] : R]$. On the other hand, since $deg(a^{-1}s^d) = -d\sigma + d\sigma = 0$ and $deg(b^{-1}a^i a_{di}) = (i.d - n)\sigma + deg(a_{di}) = 0$, $P(X) \in R_0[X]$ and $R_0[a^{-1}s^d] \subset R[s]_0$. An account of degree implies that $P(X)$ is the minimal polynomial of $a^{-1}s^d$ over R, and then $R[s]_0$ is a free $R_0[a^{-1}s^d]$-module of rank 1, i.e., $R[s]_0 = R_0[a^{-1}s^d]$. ■

Remark 1. 4. *Preserving notations of the proof of corollary 1.3, let $s \in S_\sigma$ be an invertible homogeneous element which is integral over R. Then $\mu_s(X) = bP(a^{-1}X^d)$, where $P(X)$ is the minimal polynomial of $a^{-1}s^d$ over R. In particular, if $s^d \in R$, then $\mu_s(X) = X^d - s^d$*

Proposition 1. 5. *Let $s \in S_\sigma$ be an homogeneous element which is integral over R. Then $R[s]/R$ is separable if and only if the minimal polynomial $\mu_s(X)$, of s over R, is square free.*

Proof. From [5, propostion 5, p 97], $R[s]/R$ is separable if and only if $D_R(R[s]) = R$. On the other hand, since $R[s] \simeq R[X]/(\mu_s(X)) = R[\bar{X}]$,

$D_R(R[s]) = det(\mu'_s(\bar{X}))R$, where $det(\mu'_s(\bar{X}))$ is the determinant of the endomorphism $l_{\mu'_s(\bar{X})}$, of $R[\bar{X}]$, defined by the multiplication by $\mu'_s(\bar{X})$. So, $R[s]/R$ is separable if and only if $det(\mu'_s(\bar{X}))$ is invertible in R. Let $\mu_s(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$. As $\mu_s(X)$ is a σ-homogeneous polynomial, for every $a_i \neq 0$, $deg(a_i) + i\sigma = n\sigma$. Hence for every $a_i \neq 0$, $deg(a_i) + (i-1)\sigma = (n-1)\sigma$, i.e., $\mu'_s(X)$ is a σ-homogeneous polynomial of grade $(n-1)\sigma$. Consequently, $\mu'_s(\bar{X})$ is a homogeneous element of $R[\bar{X}]$ of degree $(n-1)\sigma$, and then $det(\mu'_s(\bar{X}))$ is a homogeneous element of R. Since R is a graded field, $det(\mu'_s(\bar{X}))$ is invertible in R if and only if $det(\mu'_s(\bar{X})) \neq 0$. From [7, (53), A IV.79], that is equivalently to $\mu_s(X)$ is square free. ■

Corollary 1. 6. *If S is a domain, then for every homogeneous element $\alpha \in S$, which is integral over R, $R[\alpha]/R$ is separable if and only if α is a simple root of its minimal polynomial.*

Proof. Let K be the quotient field of R and $\mu_\alpha(X)$ the minimal polynomial of α over R. The fact that $[K[\alpha] : K] = [R[\alpha] : R]$ implies that $\mu_\alpha(X)$ is the minimal polynomial of α over K. Since S is a domain, $\mu_\alpha(X)$ is an irreducible polynomial of $R[X]$. Hence α is a simple root of its minimal polynomial if and only if $\mu_\alpha(X)$ is square free. ■

Let A be a commutative free R-algebra and G a finite subgroup of $\mathcal{A}ut_R(A)$ such that $A^G = R$, where $A^G = \{a \in A \,|\, \sigma(a) = a \; forall\, \sigma \in G\}$. Denote $A^{(G)}$ the A-algebra with basis $\{e_\sigma | \sigma \in G\}$, where e_σ is the idempotent $(\delta^\sigma_\tau)_{\tau \in G}$, where $\delta^\sigma_\tau = 1$ if $\tau = \sigma$ and $\delta^\sigma_\tau = 0$ elsewhere. Recall that A/R is said to be a G-galois extension if the following homomorphism h is an isomorphism of A-algebras

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

The following Proposition gives a criterion to test if $R[s]/R$ is a galois extension.

Proposition 1. 7. *Let T/R be a totally ramified graded ring extension with respect to a torsion free abelian group and let $s \in T_\sigma$ be an invertible homogeneous element. Let n be the cardinal order of the group $\Gamma < \sigma > /\Gamma$. Then $R[s]/R$ is a galois extension if and only if n is invetible in R_0 and R_0 contains ζ_n a n^{th} primitive root of 1.*
In that case, the galois group of $R[s]/R$ is $G = \{g_1, ..., g_n\}$, where $g_i(s) = \zeta_n^i s$.

Proof. Let $a = s^n$. Since $deg(a) = n\sigma \in \Gamma$, there exists $v \in R[s]_0$ such that $a = vu_{n\sigma}$. Since $S_0 = R[s]_0 = R_0$, $v \in R$, and then $a \in R$. From Remark 1.4, $\mu_s(X) = X^n - a$ is the minimal polynomial of s over R. As $R[s]/R$ is a galois extension, it is separable, and then n is invertible in the field R_0. Let G be a finite subgroup of $\mathcal{A}ut_R(R[s])$ such that $R[s]/R$ is a G-galois extension. Then the cardinal order of G is equal to n. Hence $\mu_s(X)$ splits in $R[s]$, with simple roots $s_1, ..., s_n$, where $\frac{s_1}{s}, ..., \frac{s_n}{s}$ are the distinct roots of $X^n - 1$. Since $\triangle$ is a a torsion free abelian group, $\zeta_n \in R[s]_0 = R_0$. Conversely, assume that n is invetible in R_0 and R_0 contains ζ_n. Then $s, \zeta_n s, ..., \zeta_n^{n-1} s$ are the distinct roots of $\mu_s(X)$. Set $G =< \sigma >$, where $\sigma(s) = \zeta_n s$. Then G is a finite subgroup of $\mathcal{A}ut_R(R[s])$. 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 $y = r_0 \in R$, i.e., $R[s]^G = R_0$. We compute $det(h)$, the determinant of the homomorphism h of $R[s] \otimes_R R[s]$ into $R[s]^{(G)}$, we obtain

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

Since s is an invertible element and $\prod_{1 \leq i < j \leq n} (\zeta_n^i - \zeta_n^j) \in R$ is a nonzero homogeneous element of degree 0, $det(h)$ is an invertible element of R, and then $R[s]/R$ is a $G-$galois extension. ■

2. Separable CP-graded ring extensions

In [2], without restrictions to torsion free of graded groups, we have generalized some separability results given in [3]. In this section, we investigate separability of CP-graded ring extensions. We finalize by a classification Theorem.

Lemma 2. 8. *If S/R is separable, then S is a free R-module of finite rank.*

Proof. From Proposition 0.1, S is a free R-module. So by [8, Proposition III.3.2], if S/R is separable, then S is a finitely generated R-module.■

In the sequel of the paper, S/R is a CP-graded ring extension such that S is a finitely generated R-module. Set $\triangle/\Gamma = \{\bar{\sigma}_1, ..., \bar{\sigma}_n\}$. For every i, fix w_{σ_i} an homogeneous element, of S, of degree σ_i. Specify $\sigma_1 = 0$ and $w_0 = 1$. Then $(w_{\sigma_1}, ..., w_{\sigma_n})$ is a $S(\Gamma)$-basis of S.

The following Theorem gives a criterion to test if a CP-graded ring extension is separable.

Theorem 2. 9. *Let S/R be a CP-graded ring extension such that S is a finitely generated R-module. Then S/R is separable if and only if S_0/R_0 is separable and $[\triangle : \Gamma]$ is invertible in R_0.*

Proof. We use a discriminant computation; let M be the R-submodule of S, generated by $(w_{\sigma_1}, ..., w_{\sigma_n})$. Then $S \simeq S(\Gamma) \otimes_R M$ as R-modules. From [6, Proposition 2], we have $D_R(S) = (D_R(S(\Gamma)))^n (D_R(M))^f$, where $f = [S_0 : R_0]$. Since $S(\Gamma) \simeq S_0 \otimes_{R_0} R$, $D_R(S(\Gamma)) = D_{R_0}(S_0)R$. On the other hand, for every (i, j), there exists c_{σ_i,σ_j} an invertible element of $S(\Gamma)$ such that $w_{\sigma_i} w_{\sigma_j} = c_{\sigma_i,\sigma_j} w_{\sigma_i+\sigma_j}$. Hence $T_{S/S(\Gamma)}(w_{\sigma_i} w_{\sigma_j}) = nc_{\sigma_i,\sigma_j} \delta_0^{\sigma_i+\sigma_j}$, where $\delta^\sigma_\tau = 0$ if $\tau \neq \sigma$ and $\delta^\sigma_\tau = 1$ elsewhere. Consequently, the determinant of the bilinear form $T_{S/S(\Gamma)}$, with respect to the basis $(w_{\sigma_1} ..., w_{\sigma_n})$, is $D(w_{\sigma_1} ..., w_{\sigma_n}) = sn^n$, where s is an invertible element of $S(\Gamma)$. Consequently, $D_R(S) = n^{nf}(D_{R_0}(S_0))^n R$. Therefore, $D_R(S) = R$ if and only if n is invertible in R_0 and $D_{R_0}(S_0)R = R$. As R_0 is a field, that means that n is invertible in R_0 and S_0/R_0 is separable. ■

Corollary 2. 10. *Let S/R be a CP-graded ring extension such that S is a finitely generated R-module.*
1) If S/R is a totally ramified CP-graded ring extension, then S/R is separable if and only if $[\triangle : \Gamma]$ is invertible in R_0. In particular, $S/S(\Gamma)$ is separable if and only if $[\triangle : \Gamma]$ is invertible in R_0.
2) If $\triangle = \Gamma$, then S/R is separable if and only if S_0/R_0 is separable. In particular, $S(\Gamma)/R$ is separable if and only if S_0/R_0 is separable.
3) S/R is separable if and only if $S(\Gamma)/R$ and $S/S(\Gamma)$ are separable.

Proposition 2. 11. *Let R be a domain graded field with quotient field K and S/R a CP-graded ring extension such that S is a finitely generated R-module. Then S/R is separable if and only if KS/K is separable.*

Proof. In the proof of Theorem 2.9, we have shown that $D_R(S) = n^{nf}(D_{R_0}(S_0))^n R$, where $f = [S_0 : R_0]$. Since every R-basis of S is a K-basis of KS, $D_K(KS) = D_R(S)K$. Therefore $D_K(KS) = n^{nf}(D_{R_0}(S_0))^n K$. Consequently, KS/K is separable if and only if n is invertible in R and $D_{R_0}(S_0) = R_0$, i.e., S/R is separable. ■

The following Theorem gives a classification of separable CP-graded algebras over a domain graded field.

Theorem 2. 12. *Let R be a domain graded field and S/R a CP-graded ring extension. Then S/R is separable if and only if $S = \oplus_{i=1}^r S_i$, where*

S_i/R is a separable graded field extension for each i.
Within a isomorphism, this decomposition is unique.

Proof. Let K be the quotient field of R and assume that S/R is separable. Then KS/K is separable too. Hence $KS = \times_{i=1}^{r} K_i$, where K_i/K is a separable extension of fields for each i. So, $S = \times_{i=1}^{r} S_i$, where $S_i = S \cap K_i$ for every i. Let $1 \leq i \leq r$; to show that S_i is a graded subalgebra of S, it suffices to show that for every $x \in S_i$, S_i contains the homogeneous components of x in S. Let $x = \sum_\sigma x_\sigma \in S_i$ and $1 = e_1 + ... + e_r \in \times_{i=1}^{r} S_i$, where e_i is the unit of S_i for every i. Decompose every e_k as a sum of homogeneous elements of S. Since 1 is an homogeneous element of degree 0, every homogeneous component of every e_k is an homogeneous element of degree 0, and then every e_k is an homogeneous element of degree 0. Furthermore, since $x \in S_i$, $x = x.e_i = \sum_\sigma x_\sigma e_i$, where $x_\sigma e_i$ is an homogeneous element of degree σ for every σ. The uniqueness of a such decomposition implies that $x_\sigma e_i = x_\sigma$ for every σ. Since $e_i S_j = \delta_i^j S_j$, where $\delta_i^j = 1$ if $i = j$ and $\delta_i^j = 0$ elsewhere, $x_\sigma e_i \in S_i$ for every σ, and then $x_\sigma \in S_i$ for every σ. On the other hand, let s be a nonzero homogeneous element of S_i. Since S is a finitely generated R-module, s is integral over R. Let $\mu_s(X) = X^n + ... + a_0$ its minimal polynomial over R. Since S_i is a domain, a_0 is a nonzero homogeneous element of R, and then it is invertible in R. So, s invertible in $R[s]$ ($s^{-1} = -a_0(a_{n-1}s^{n-2} + ... + a_1)$). As S_i is a faithful R-algebra, $R[s] \subset S_i$. Hence s invertible in S_i, and hence S_i is a graded field. Since $KS_i = K_i$ and K_i/K is separable, from Proposition 2.11, S_i/R is separable too.
Conversely, assume that $S = \oplus_{i=1}^{r} S_i$, where S_i/R is a separable graded field extension for each i. Then $D_R(S) = \prod_{i=1}^{r} D_R(S_i) = R$, i.e., S/R is separable. ∎

3. Galois extension of CP-graded rings

In this section, we give a classification theorem of CP-graded ring extensions over a graded field which is a domain.

Theorem 3. 13. *Let S/R be a CP-graded ring extension such that R is a domain. Then S/R is a galois extension if and only if $S \simeq S_1^r$, where S_1/R is a galois extension of graded fields and $r \in \mathbb{N}^*$.*

Proof. Since S/R is a galois extension, then it is separable. From Thorem 2.12, $S = S_1^{e_1} \times ... \times S_r^{e_r}$, where S_i/R is a separable graded field extension for each i and $S_i \not\simeq S_j$ for $i \neq j$. Let G be a finite subgroup of $\mathcal{A}ut_R(S)$ such that S/R is a $G-$galois extension. Then for every $\sigma \in G$ for every i, $\sigma(S_i^{r_i}) = S_i^{r_i}$. Let σ_i be the restriction of σ to $S_i^{r_i}$ and $G_i = \{\sigma_i \mid \sigma \in G\}$. Then G_i is a finite subgroup of $\mathcal{A}ut_R(S_i^{r_i})$ and $S^G =$

$\oplus_{i=1}^{r}(S_i^{r_i})^{G_i} = \oplus_{i=1}^{r}T_i$. Since S/R is a $G-$galois extension, $r = 1$ and $(S_1^{r_1})^{G_1} = R$. On the other hand, since $G =< \tau > \mathcal{A}ut_R(S_1)$, where τ is a permutation of $\{e_1, ..., e_{r_1}\}$ and e_i is the idempotent $(\delta_i^j)_{1\leq j\leq r_1}$ of $S_1^{r_1}$. The fact that $S^G = R$ implies that $S_1^{\mathcal{A}ut_R(S_1)} = R$. Since S_1/R is separable and S_1 is a domain, from [9, Theorem 2.1, p. 7], S_1/R is a galois extension.
Conversely, assume that $S \simeq S_1^r$, where S_1/R is a G_1-galois extension of graded fields. Let $\tau \in \mathcal{A}ut_R(S_1^r)$ defined by $\tau(e_i) = e_{i+1}$ for every $i \in \mathbb{Z}/r\mathbb{Z}$. Let $G = \{\sigma\circ\tau^i \,|\, i \in \mathbb{Z}/r\mathbb{Z}\,,\ \sigma \in G_1\}$. Let $\mathcal{B}$ be a maximal ideal of S_1^r. Without loss generality, we can assume that $\mathcal{B} = S_1 \times ... \times S_1 \times \mathcal{P}$, where $\mathcal{P}$ is a maximal ideal of S_1. From [9, Theorem 2.1, p. 7], it suffices to show that for any $g \in G$, $g((x_1, ..., x_r)) - (x_1, ..., x_r) \in \mathcal{B}$ for every $(x_1, ..., x_r) \in S$, implies that $g = id_S$. Let $\sigma\tau^i \in G$ such that $\sigma\tau^i((x_1, ..., x_r)) - (x_1, ...x_r) \in \mathcal{B}$ for every $(x_1, ..., x_r) \in S$.
1^{st} case $i = 0$, then $\sigma(x_1) - x_1 \in \mathcal{P}$ for every $x_1 \in S_1$. Since S_1/R is a galois extension, from [9, Theorem 1.6, p. 2], $\sigma = id_{S_1}$, and then $\sigma\tau^i = id_S$.
2^{nd} case $i \neq 0$, then $(\sigma(x) - y) \in \mathcal{P}$ and $(x - \sigma^{-1}(y)) \in \mathcal{P}$ for every $(x, y) \in S_1^2$. Hence $(\sigma(x) - y) - (x - \sigma^{-1}(y)) \in \mathcal{P}$ for every $(x, y) \in S_1^2$. For $y = 0$, we obtain $(\sigma(x) - x) \in \mathcal{P}$ for every $x \in S_1$. From [9, Theorem 1.6, p. 2], since S_1/R is a galois extension, $\sigma = id_{S_1}$, and hence $x \in \mathcal{P}$ for every $x \in S_1$. That is impossible, and then $i = 0$. Consequently, S/R is a galois extension. ■

References

[1] L. El fadil, Galois Theory of graded fields, (to appear in International Journal of Commutative Rings).

[2] L. El fadil, Separability of graded fields, (to appear in International Mathematical Journal).

[3] Y. S. Hwang and A. R. Wadsworth, Algebraic extensins of graded and valued fields, Comm.in Algebra, 27(2),(1999), 821-840.

[4] M. Boulagouaz, The graded and tame extensions, Lect. Notes in Pure and Appl. math., Marcel Dekker, (153)(1994), 27-40.

[5] L. El Fadil and M. Charkani. Generalization of the discriminant and applications, The Arabian Journal for Science and Engineering, (1A)29, 2004, 93-98.

[6] L. El fadil, Discriminant and separability. (Preprint n : 547, Jul 2003 Centre de Recerca Matematica, Barcelona)

[7] N. Bourbaki, Algèbre ch. 4 à 7, Paris New York Barcelone Milan Mexico Rio de Daneiro, Masson, 1981.

[8] M. A. Knus and M. Ojanguren, Théorie de la descente et algèbres d'Azummaya, Lect. Notes in Math., v. 389, Springer-Verlag Berlin, Heidelberg, New York, 1974.

[9] C. Greither, Cyclic galois extensions of commutative rings, Lect. Notes in Math., 1534, Springer-Verlag Berlin Heidelberg, New York, (1992).

L houssain EL FADIL,
Lycée Reda Slaoui (CPGE),
B.P. 3149, Talborjt, Agadir
Agadir-Morocco