

# Discriminant and Separability

L. EL FADIL

Departement of Mathematics,  
Faculty of Sciences Dhar-Mehraz,  
P.O. Box 1796 Fes-Atlas,  
Fes-Morocco  
lhouelfadil@hotmail.com

## Abstract

The classical notion of the discriminant of a number field was generalized both to commutative free  $R$ -algebras with finite rank and to  $R$ -subalgebra of a *separable*  $K$ -algebra with finite dimension, where  $K$  is the quotient field of a Dedekind domain  $R$ . In this paper, we define the discriminant ideal to a projective sub-module of constant rank of an  $R$ -algebra. As applications, we characterize separable polynomials over an  $\mathcal{R}$ -ring.

## Introduction

Let  $L/K$  be a finite separable extension of fields. Then the trace and norm maps of  $L$  are defined by:  $T_{L/K}(x) = \sum_{i=1}^n \sigma_i(x)$  and  $N_{L/K}(x) = \prod_{i=1}^n \sigma_i(x)$  for all  $x \in L$ , where  $\sigma_1, \sigma_2, \dots, \sigma_n$  are the  $K$ -isomorphisms of  $L$  into its algebraic closure. The trace map of  $L$  induces a non-singular bilinear form of  $L^2$  defined by:  $T_{L/K}(x, y) = T_{L/K}(xy)$  for every  $(x, y)$  in  $L^2$ . When  $K = \mathbb{Q}$  and  $L$  is a number field,  $O_L$  denotes the integral closure of  $\mathbb{Z}$  in  $L$ . Then  $O_L$  is a free  $\mathbb{Z}$ -algebra of rank  $n = [L : \mathbb{Q}]$ . The determinant of the bilinear form  $T_{L/K}$  with respect to a  $\mathbb{Z}$ -basis  $(e_1, \dots, e_n)$  of  $O_L$  is called the discriminant of  $(e_1, \dots, e_n)$  and is denoted by  $D(e_1, \dots, e_n)$ . The principal ideal of  $\mathbb{Z}$  generated by  $D(e_1, \dots, e_n)$  is independent of the choice of the  $\mathbb{Z}$ -basis of  $O_L$  and called the discriminant of the number field  $L$ . The classical notion of the discriminant of a number field was generalized both to commutative free  $R$ -algebras with finite rank and to  $R$ -subalgebra of a *separable*  $K$ -algebra with finite dimension, where  $K$  is the quotient field of

a Dedekind domain  $R$  (See [1], [2], [3], [4], [7], [5] and [6]). In this paper, we define the discriminant ideal to a projective sub-module of constant rank of an  $R$ -algebra. As applications, we characterize separable polynomials over an  $\mathcal{R}$ -ring.

Throughout this paper,  $R$  will denote a commutative ring,  $M$  a projective  $R$ -module of constant rank  $n$  and  $u$  is an endomorphism of  $M$ .  $\max(R)$  is the set of maximal ideals of  $R$ . For a maximal ideal  $\mathcal{P}$  of  $R$ , set  $M_{\mathcal{P}}$  the scalar extension of  $M$  by  $R_{\mathcal{P}}$  and  $u_{\mathcal{P}}$  the  $R_{\mathcal{P}}$ -endomorphism induced by  $u$ .

The first section deals with trace and norm maps in a projective sub-module of constant rank of an  $R$ -algebra. We first extend them to projective sub-module of constant rank of an  $R$ -algebra and then we define the discriminant ideal of a such sub-module. In the second section, we give examples and applications. We achieve the paper by characterizing separable polynomials over an  $\mathcal{R}$ -ring in the third section.

## 1 Norm and trace

Let  $R$  be a domain with quotient field  $K$ ,  $M$  a projective  $R$ -module of constant rank  $n$  and  $u$  an  $R$ -endomorphism of  $M$ . Let  $\mathcal{P}$  be a maximal ideal of  $R$ . Then  $M_{\mathcal{P}}$  is a free  $R_{\mathcal{P}}$ -module of rank  $n$ . Let  $(e_1, \dots, e_n)$  be an  $R_{\mathcal{P}}$ -basis of  $M_{\mathcal{P}}$ . Then  $(e_1, \dots, e_n)$  is a  $K$ -basis of  $KM$ . Consequently, for every maximal ideal  $\mathcal{P}$  of  $R$ , the  $R_{\mathcal{P}}$ -endomorphism  $u_{\mathcal{P}}$ , induced by  $u$ , and the  $K$ -endomorphism  $u_K$ , induced by  $u$ , have the same characteristic polynomial  $C_u(X) \in R[X]$ . The polynomial  $C_u(X)$  is called the characteristic polynomial of  $u$ . Set  $C_u(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$  the characteristic polynomial of  $u$ . Define  $\text{tr}(u) = -a_{n-1}$  the trace of  $u$  and  $\det(u) = (-1)^n a_0$  the determinant of  $u$ .

Generally, let  $R$  be a commutative ring,  $M$  a projective  $R$ -module of constant rank  $n$  and  $u$  an endomorphism of  $M$ . If the characteristic polynomial of the  $R_{\mathcal{P}}$ -endomorphism  $u_{\mathcal{P}}$  does not depend of the choice of the maximal ideal  $\mathcal{P}$  of  $R$ , in particular if  $R$  is a domain, then we define  $\text{tr}(u)$  and  $\det(u)$  as the trace and the determinant of the endomorphism  $u_{\mathcal{P}}$  respectively, for an arbitrary maximal ideal  $\mathcal{P}$  of  $R$ .

Let  $S$  be a  $K$ -algebra and  $M$  a projective submodule, of  $KS$ , of constant rank  $n$ . For every  $x \in M$ ,  $x$  induces an  $R$ -endomorphism  $l_x$  of  $M$  defined by  $l_x(m) = xm$ . Define  $T_{M/R}(x) = \text{tr}(l_x)$  the trace of  $x$  and if  $l_x$  has its characteristic polynomial in  $R[X]$ , then define  $N_{M/R}(x) = \det(l_x)$  the norm of  $x$ . These notions generalize the classical notions, in particular if  $L/K$  is a separable extension of degree  $n$  and  $M$  is a projective submodule, of  $L$ , of constant rank  $n$ , then the trace and norm maps of  $M$  are defined by:  $T_{M/K}(x) = \sum_{i=1}^n \sigma_i(x)$  and  $N_{M/K}(x) = \prod_{i=1}^n \sigma_i(x)$ , for all  $x \in L$ , where

$\sigma_1, \sigma_2, \dots, \sigma_n$  are the  $K$ -isomorphisms of  $L$  into its algebraic closure.

We start this section by the following examples illustrating our studies.

### Examples

1) Let  $S$  be a projective  $R$ -algebra of constant rank  $n$  and  $x \in R$ . Since  $C_x(X) = (X - x)^n$ , then  $T_{S/R}(x) = nx$  and  $N_{S/R}(x) = x^n$ .

2) Let  $S/R$  be an extension of commutative rings such that  $S$  is a projective  $R$ -module of constant rank. Let  $G$  be a finite sub-group of  $\text{Aut}_R(S)$  such that  $S^G = R$ , where  $S^G$  is the ring of all elements of  $S$  which are fixed by every element of  $G$ . Set  $S^{(G)}$  the  $S$ -algebra with a basis constituting by orthogonal idempotents  $\mathcal{E} = \{u_\sigma \mid \sigma \in G\}$ . Recall that  $S/R$  is a  $G$ -Galois extension if and only if  $h : S \otimes S \rightarrow S^{(G)}$ , defined by  $h(x \otimes y) = \sum_{\sigma \in G} x\sigma(y)u_\sigma$  is an  $S$ -isomorphism (see [8]). Then

**Proposition 1** *Let  $S/R$  be a  $G$ -Galois extension. Then  $C_{l_x}(X) = \prod_{\sigma \in G} (X - \sigma(x))$  for all  $x \in S$ . In particular,  $T_{S/R}(x) = \sum_{\sigma \in G} \sigma(x)$  and  $N_{S/R}(x) = \prod_{\sigma \in G} \sigma(x)$  for all  $x \in S$ .*

**Proof.** Since  $S$  is a faithfully-flat  $R$ -algebra (see [8, lemma 1. 11, page 5]), it suffices check these results by scalar extension by  $S$ . Thanks to the isomorphism  $h$ ,  $S \otimes S$  is a free  $S$ -module with rank  $n = [G : 1]$  and  $G$  operates over  $S \otimes S$  by  $\sigma(x \otimes y) = x \otimes \sigma(y)$ . Since  $l_{1_S \otimes x} = l_{x \otimes 1_S}$ , we compute the characteristic polynomial  $C_{1_S \otimes x}(X)$  of  $l_{1_S \otimes x}$ . Thanks to the isomorphism  $h$ , we identify  $1_S \otimes x$  with  $\sum_{\sigma \in G} \sigma(x)u_\sigma$ . Then  $x.u_\tau = \tau(x)u_\tau$ . Consequently, the matrix of  $l_{1_S \otimes x}$  with respect to the basis  $\mathcal{E}$  is  $(\tau(x)\delta_{\tau,\sigma})_{(\tau,\sigma) \in G^2}$ . Hence  $C_{l_{1_S \otimes x}}(X) = \prod_{\sigma \in G} (X - \sigma(x))1_S$ . Finally,  $C_{l_x}(X) = \prod_{\sigma \in G} (X - \sigma(x))$ .

### 1.1 Discriminant ideal

Let  $S$  be an  $R$ -algebra and  $M$  a projective sub-module of constant rank  $n$  of  $S$ . The trace map  $T_{M/R}$  induces a bilinear form of  $M^2$  defined by  $T_{M/R}((x, y)) = T_{M/R}(xy)$  for all  $(x, y) \in M^2$ . If  $M$  is a free  $R$ -module of rank  $n$  then the determinant of the bilinear form  $T_{M/R}$  with respect to an  $R$ -basis  $(e_1, \dots, e_n)$  of  $M$  is denoted by  $D(e_1, \dots, e_n)$  and called the discriminant of  $(e_1, \dots, e_n)$ . In general way, for  $(a_1, \dots, a_n) \in M^n$ . The discriminant of  $(a_1, \dots, a_n)$  is the determinant  $D(a_1, \dots, a_n)$  of the matrix  $(T_{M/R}(a_i a_j))_{i,j}$  and the discriminant ideal of  $M$  over  $R$  is to be the ideal of  $R$  generated by all  $D(a_1, \dots, a_n)$ , where  $(a_1, \dots, a_n)$  runs over  $M^n$ . This will be denoted by  $D_R(M)$  ( see [9]).

**Proposition 2** *Let  $M_1$  and  $M_2$  be two projective sub-modules, of  $S$ , of constant ranks  $m$  and  $r$  respectively. Then*

1) If  $M_1$  and  $M_2$  are mutually orthogonal, then

$$D_R(M_1 + M_2) = D_R(M_1)D_R(M_2).$$

2)  $D_R(M_1 \otimes M_2) = (D_R(M_1))^r (D_R(M_2))^m$ .

**Proof.** Since  $\bigoplus_{\mathcal{P} \in \max(R)} R_{\mathcal{P}}$  is a faithfully-flat  $R$ -algebra, we can assume that  $M_1$  and  $M_2$  are two free sub-modules of  $S$  of ranks  $m$  and  $r$  respectively. Let  $\{e_1, \dots, e_m\}$  be an  $R$ -basis of  $M_1$  with dual basis  $\{e_1^*, \dots, e_m^*\}$  and  $\{v_1, \dots, v_r\}$  be an  $R$ -basis of  $M_2$  with dual basis  $\{v_1^*, \dots, v_r^*\}$ .

1) Since  $M_1$  and  $M_2$  are mutually orthogonal, then the determinant of the bilinear form  $T_{(M_1+M_2)/R}$  with respect to the basis  $\{(e_1, 0), \dots, (e_m, 0)\} \cup \{(0, v_1), \dots, (0, v_r)\}$  is

$$\det(T_{M_1/R}(e_i e_j))_{1 \leq i, j \leq m} \det(T_{M_2/R}(v_i v_j))_{1 \leq i, j \leq r}.$$

2) For  $1 \leq i \leq m$  and  $1 \leq j \leq r$ , define  $e_i^* * v_j^*$  by  $e_i^* * v_j^*(x \otimes y) = e_i^*(x)v_j^*(y)$  for all  $(x, y) \in M_1 \times M_2$ . Then  $\{e_i^* * v_j^*, 1 \leq i \leq m, 1 \leq j \leq r\}$  is an  $R$ -basis of  $M_1 \otimes M_2$  with dual basis  $\{e_i^* * v_j^*, 1 \leq i \leq m, 1 \leq j \leq r\}$ . Hence  $T_{M_1 \otimes M_2/R}(x \otimes y) = \sum_{i,j} e_i^* * v_j^*((x \otimes y)(e_i \otimes v_j)) = \sum_{i,j} e_i^*(x e_i) v_j^*(y v_j) = \sum_{i=1}^m e_i^*(x e_i) \sum_{j=1}^r v_j^*(y v_j) = T_{M_1/R}(x) T_{M_2/R}(y)$ . Set  $T_{M_1/R}(e_i e_j) = t_{ij}$ ,  $T_{M_2/R}(v_k v_l) = s_{kl}$ ,  $A = (t_{ij})_{1 \leq i, j \leq m}$  and  $B = (s_{kl})_{1 \leq k, l \leq r}$ . Then  $D_R(M_1 \otimes M_2) = \det((x_{IJ})_{I,J})R$ , where  $x_{I,J} = t_{ij} s_{kl}$ ,  $I = (i, k)$  and  $J = (j, l)$ . By [[10], page 157 and page 101],  $(x_{IJ})_{I,J} = A \otimes B$  and  $\det(A \otimes B) = (\det(A))^r (\det(B))^m$ . Consequently,  $D_{M_1 \otimes M_2/R} = (D_{M_1/R})^r (D_{M_2/R})^m$ .

## 2 Examples and applications

1) We give a method for computing the discriminant ideal of polynomial algebras over a domain.

Let  $f \in R[X]$  be a monic polynomial of degree  $n$ . Let  $x_1, \dots, x_n$  be its roots counted with multiplicity order in some commutative ring. Then  $\text{Disc}(f) := \text{Res}(f, f') = \prod_{i \neq j} (x_i - x_j)$ .

Let  $R$  an integrally domain with quotient field  $K$  and  $L/K$  a separable extension. If  $L = K[x]$ , where  $x$  is an integral element over  $R$  with minimal polynomial  $f$ , then  $T_{L/K}(x) = \sum_{i=1}^n \sigma_i(x)$ , where  $\sigma_1, \sigma_2, \dots, \sigma_n$  are the  $K$ -isomorphisms of  $L$  in its algebraic closure. In the other hand, the discriminant  $R(S_f)$  is the principal ideal of  $R$  generated by  $\text{Disc}(f) = \prod_{i=1}^n \prod_{j \neq i} (\sigma_i(x) - \sigma_j(x))$ . In this section, we extend this result to extensions over a domain. More precisely, we show that if  $R$  is a domain and

$f \in R[X]$  is a monic polynomial, then  $D_R(S_f)$  is generated by  $\text{Disc}(f) = \prod_{i=1}^n \prod_{j \neq i} (x_i - x_j)$ .

**Theorem 1** *Let  $R$  be a domain with quotients field  $k$  and  $f \in R[X]$  a monic polynomial of degree  $n$ . Then*

$$D(1, \bar{X}, \dots, (\bar{X})^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{S_f/R}(f'(\bar{X})).$$

**Proof.** Let  $x_1, \dots, x_n$  be the roots of  $f$  in some commutative extension  $T$  of  $R$  and  $P \in R[X]$ . Since the  $R$ -endomorphism  $l_{P(\bar{X})}$  and the  $k$ -endomorphism  $l'_{P(\bar{X})}$  of  $kS_f$  induced by  $l_{P(\bar{X})}$  operate with the same manner over  $(1, \bar{X}, \dots, \bar{X}^{n-1})$ , then they have the same characteristic polynomial. Consequently, we can assume that  $R$  is a field. Moreover the trace of an endomorphism does not modify after scalar extension, so we can assume that the roots  $x_1, \dots, x_n$  of  $f$  are in  $k$ . For  $1 \leq i \leq r$ , denote  $E_i = \ker(u - x_i \text{id})^{e_i}$  the characteristic space of the endomorphism  $l'_{\bar{X}}$  associated to the eigenvalue  $x_i$  and let  $\{u_1^i, \dots, u_{e_i}^i\}$  be a  $k$ -basis of  $E_i$  such that  $\bar{X}u_1^i = x_i u_1^i$  and for  $2 \leq s \leq r$ ,  $\bar{X}u_s^i - x_i u_s^i \in \sum_{j=1}^{s-1} Ru_1^j$ . Then  $P(\bar{X})u_1^i = P(x_i)u_1^i$  and for  $2 \leq s \leq r$ ,  $P(\bar{X})u_s^i - P(x_i)u_s^i \in \sum_{j=1}^{s-1} Ru_1^j$ . Hence  $P(x_1), \dots, P(x_r)$  are the roots of the characteristic polynomial  $C_{P(\bar{X})}(X)$  with multiplicity order  $e_1, \dots, e_r$  respectively, i.e.,  $C_{P(\bar{X})}(X) = \prod_{i=1}^r (X - P(x_i))^{e_i}$ . Consequently,

$$T_{S_f/R}(P(\bar{X})) = - \sum_{i=1}^n P(x_i) \quad \text{and} \quad N_{S_f/R}(P(\bar{X})) = (-1)^n \prod_{i=1}^n P(x_i).$$

$$\begin{aligned} D(1, \bar{X}, \dots, \bar{X}^{n-1}) &= \det(T_{S_f/R}((\bar{X})^{i+j})) = (-1)^n \det\left(\sum_{k=1}^n x_k^{i+j}\right) \\ &= (-1)^n \det((x_k^j)_{k,j}) \det((x_k^i)_{i,k}) = (-1)^n \det((x_k^j)_{k,j})^2. \end{aligned}$$

Using the Vandermande determinant, we have

$$D(1, \bar{X}, \dots, \bar{X}^{n-1}) = (-1)^n \prod_{i=1}^n \prod_{j \neq i} (x_i - x_j) = (-1)^{\frac{n(n-1)}{2}} N_{S_f/R}(f'(\bar{X})).$$

2) We find, partially, the Maschke's Theorem by using the discriminant ideal.

Let  $R$  be a domain and  $G$  a finite abelian group of cardinal order  $n$ .

- a) Set  $G = \langle \sigma_1 \rangle \times \dots \times \langle \sigma_r \rangle$ . Then  $R[G] \simeq R[\sigma_1] \otimes \dots \otimes R[\sigma_r]$ . Let  $\sigma \in G$  with order  $e$ . Since  $1, \sigma, \dots, \sigma^{e-1}$  is an  $R$ -basis of  $R[\sigma]$  then  $X^e - 1$  is the minimal polynomial of  $\sigma$  over  $R$ . Consequently,  $R[\sigma] \simeq R[X]/(X^e - 1)$ . Hence  $D_R(R[\sigma]) = e^e R$ . By the proposition 6,  $D_R(R[G]) = n^n R$ .

- b) Recall that, a commutative projective  $R$ -algebra  $S$  of constant rank is separable over  $R$  if and only if  $D_R(S) = R$  (see [9]). Then  $R[G]$  is a separable  $R$ -algebra if and only if  $n$  is invertible in  $R$ .
- c) In particular, if  $K$  is a field of characteristic  $p$ , then  $K[G]$  is a separable  $K$ -algebra if and only if  $p$  does not divide  $n$ . Hence we find also the Maschke's theorem: If  $p$  does not divide  $n$ , then  $K[G]$  is a semi-simple  $K$ -algebra.
- 3) Let  $S$  be a commutative projective  $R$ -algebra of constant rank and  $G$  a finite subgroup of  $\text{Aut}_R(S)$  such that  $S^G = R$ . Let  $\mathcal{P}$  be a maximal ideal of  $R$  and  $\mathcal{B}$  a maximal ideal of  $S$  above  $\mathcal{P}$ . Set  $D(\mathcal{B}/R) = \{\sigma \in G, \sigma(\mathcal{B}) \subset \mathcal{B}\}$  the splitting group of  $\mathcal{B}$ . Then

$$\begin{array}{ccc} \text{red} : D(\mathcal{B}/R) & \longrightarrow & \text{Aut}_{k(\mathcal{P})}(S/\mathcal{B}) \\ \sigma & \longmapsto & \bar{\sigma} : \end{array} \quad \begin{array}{ccc} S/\mathcal{B} & \longrightarrow & S/\mathcal{B} \\ \bar{x} & \longmapsto & \overline{\sigma(x)} \end{array}$$

is a homomorphism of groups its kernel is  $I(\mathcal{B}/R) = \{\sigma \in G \mid (\sigma - 1_G)(\mathcal{B}) \subset \mathcal{B}\}$ .  $I(\mathcal{B}/R)$  the inertia group of  $\mathcal{B}$ .

**Proposition 3** *Under the above hypothesis, let  $\mathcal{P}$  be a maximal ideal of  $R$  and  $\mathcal{B}$  a maximal ideal of  $S$  above  $\mathcal{P}$ . Set  $G/D(\mathcal{B}/R) = \{\bar{\sigma}_1, \dots, \bar{\sigma}_r\}$ . If the  $T_{S/R}$  induces a non-singular bilinear form of  $\bar{S}$ , then  $\mathcal{P}S = \prod_{i=1}^r \sigma_i(\mathcal{B})$ .*

**Proof.** Since  $T_{S/R}$  induces a non-singular bilinear form of  $\bar{S}$ ,  $\bar{S}/k(\mathcal{P})$  is separable. Hence  $\bar{S} = K_1 \times \dots \times K_r$ . Consequently,  $\mathcal{P}S = \prod_{i=1}^r \mathcal{B}_i$ , where  $\mathcal{B}_1, \dots, \mathcal{B}_s$  are the maximal ideals of  $S$  above  $\mathcal{P}$ . Since  $S^G = R$ ,  $G$  acts transitively over the maximal ideals  $\mathcal{B}_1, \dots, \mathcal{B}_s$ . Hence for every  $\mathcal{B}_i$ , there exists  $\sigma_j$  such that  $\mathcal{B}_i = \sigma_j(\mathcal{B})$ . Moreover if  $j \neq k$ , then  $\sigma_j(\mathcal{B}) \neq \sigma_k(\mathcal{B})$ . Consequently,  $\mathcal{P}S = \prod_{i=1}^r \sigma_i(\mathcal{B})$ .

### 3 Separable polynomials over an $(\mathcal{R})$ -ring

Let  $R$  be a domain with fractions field  $K$  and  $f \in R[X]$  a monic polynomial.  $f$  is called a separable polynomial if the  $R$ -algebra  $S_f$  is separable. That is equivalently to  $N_{S_f/R}(f'(\bar{X}))$  is an invertible element in  $R$ .

Let  $R$  be a Dedekind domain.  $R$  will be called an  $(\mathcal{R})$ -ring if for every field extension  $L/K$ ,  $D_R(O_L) = R$  implies  $L = K$ , where  $O_L$  is the integral clature of  $R$  in  $L$ .

We characterize the commutative projective separable algebras finitely generated as module over an  $(\mathcal{R})$ -ring.

**Proposition 4** *Let  $R$  be an  $(\mathcal{R})$ -ring with fractions field  $K$ . The only commutative projective separable algebras finitely generated as module over  $R$  are of the form  $R^n$ , where  $n \in \mathbb{N}^*$ .*

**Proof.** Let  $S$  be a such  $R$ -algebra. Then  $KS/K$  is separable. Hence  $KS = K_1 \times \cdots \times K_r$ , where  $K_i/K$  is a separable field extension for every  $i$ . Consequently,  $S = S_1 \times \cdots \times S_r$ . Since  $S$  is a commutative projective  $R$ -algebra of constant rank, then for every  $1 \leq i \leq r$ ,  $S_i$  is a commutative projective  $R$ -algebra of constant rank. Since  $D_R(S) = \prod_{i=1}^r D_R(S_i) = R$ , then  $D_R(S_i) = R$  for every  $1 \leq i \leq r$ . Since  $R$  is a Dedekind domain and  $D_R(S_i)$  is square free, then  $S_i$  is the integral clature of  $R$  in  $K_i$  for each  $i$ . The fact that  $R$  is an  $(\mathcal{R})$ -ring implies that  $S_i = R$  for every  $1 \leq i \leq r$ .

The previous Proposition allows to us to characterize separable monic polynomials over an  $(\mathcal{R})$ -ring.

**Proposition 5** *Let  $R$  be an  $(\mathcal{R})$ -ring with quotients fields  $k$ . The only monic separable polynomials over  $R$  are of the form  $f = \prod_{i=1}^n (X - a_i)$ , where  $(a_1, \dots, a_n) \in R^n$  and  $\prod_{i \neq j} (a_i - a_j)$  is invertible in  $R$ .*

**Proof.** Let  $f \in R[X]$  be a monic separable polynomial and set  $f = \prod_{i=1}^r P_i^{e_i}$  its the factorization of irreducible polynomials in  $K[X]$ . Since  $R$  is integrally closed, then every  $P_i \in R[X]$ . Since  $f$  is separable over  $R$ , then for every  $1 \leq i \leq r$ ,  $e_i = 1$ . As  $R$  is an  $(\mathcal{R})$ -ring, every  $P_i$  is with degree 1. Finally,  $\text{Disc}(f) = \prod_{i \neq j} (a_i - a_j)$  is invertible in  $R$ .

**Theorem 2** *The only monic separable polynomials over  $R$  are of the following forms:*

- 1)  $X - a$  and  $(X - a)(X - (a + 1))$ , where  $a \in R$  if  $R = \mathbb{Z}$  or  $R = \mathbb{Z}[\sqrt{-2}]$ .
- 2)  $X - a$ ,  $(X - a)(X - (a + 1))$  and  $(X - a)(X - (a + i))$ , where  $a \in R$  if  $R = \mathbb{Z}[i]$ .
- 3)  $X - a$  and  $(X - a)(X - (a + \mu))$ , where  $a \in \mathbb{Z}[\sqrt{2}]$  and  $\mu$  is an invertible element of  $\mathbb{Z}[\sqrt{2}]$  if  $R = \mathbb{Z}[\sqrt{2}]$ .

**Proof.** We show that these domains are  $(\mathcal{R})$ -rings.

Let  $m \in \mathbb{Z}$  be an integer square free such that  $m = 2$  or  $3$  modulo  $4$ . Then  $\mathbb{Z}[\sqrt{m}]$  is a Dedekind domain. Set  $K = \mathbb{Q}[\sqrt{m}]$  and let  $L/K$  be an unramified number field extension. Then  $D_{\mathbb{Z}[\sqrt{m}]}(O_L) = \mathbb{Z}[\sqrt{m}]$ . From [[1], page 17],  $D_{\mathbb{Z}}(O_L) = N_{K/\mathbb{Q}}(D_{\mathbb{Z}[\sqrt{m}]}(O_L))(D_{\mathbb{Z}}(\mathbb{Z}[\sqrt{m}]))^{[L:K]}$ . Set  $n = [L : K]$ , then  $D_{\mathbb{Z}}(O_L) = (4m)^{\frac{n}{2}} \mathbb{Z}$ . By [[7], page 70, corollaire 2],  $(\frac{\pi}{4})^{r_2} \leq \frac{n!}{n^n} \mid 4m \mid^{\frac{n}{4}}$ , where  $n = r_1 + r_2$ ,  $r_1$  is the number of  $\mathbb{Q}$ -algebra isomorphisms of  $L$

in  $\mathbb{R}$ . So,  $(\frac{\pi}{4})^{\frac{n}{2}} \frac{n^n}{n!} \leq |4m|^{\frac{n}{4}}$ . If  $m \in \{1, 2, -2\}$ , then  $(\frac{\pi}{4})^{\frac{n}{2}} \frac{n^n}{n!} \leq 8^{\frac{n}{4}}$ . Hence  $n \leq 3$  and then  $L = K$ . Consequently,  $\mathbb{Z}[\sqrt{2}]$ ,  $\mathbb{Z}[i]$  and  $\mathbb{Z}[i\sqrt{2}]$  are  $(\mathcal{R})$ -rings. For  $R = \mathbb{Z}$  see [7], page 71.

To achieve the proof, it suffices to determinate the invertible elements of these domains.

## References

- [1] J. W. Cassels and A. Frohlich. Algebraic number theory, Academic Press, London and New York, 1967.
- [2] A. Frohlich and M.J. Taylor. Algebraic number theory, Cambridge Studies in Advanced Mathematics 27, CUP, 1992.
- [3] G. Janusz, Algebraic Number Theory, Academic Press, New York, 1973.
- [4] S. Lang. Algebraic number theory, Springer-Verlag, Berlin Heidelberg, New York, Paris, Tokyo, 1986.
- [5] J. P. Serre, Corps locaux, Hermann, Paris, 1968.
- [6] O. Zariski and P. Samuel, Commutative Algebra, Springer-Verlag, Berlin, New York, GTM 28, 1991.
- [7] P. Samuel, Théorie algébrique des nombres, Hermann Paris, 2<sup>eme</sup> édition revue et corrigée, 1971.
- [8] C. Greither. Cyclic Galois extension of commutative ring, Lect. notes in maths vol: 1534, Springer-Verlag Berlin, Heidelberg, New York, 1992.
- [9] M. Charkani and L. El Fadil. Generalization of the discriminant and applications. (to appear in the forth issue of ajse).
- [10] N. Bourbaki, Algèbre ch. 1-3, DIFFUSION. C.C.L.S. Paris, 1970.
- [11] M. A. Knus et M. Ojanguren, Théorie de la descente et algèbres d'Azumaya, Lect. notes in math. Vol. 389 Springer-Verlag, Berlin, Heidelberg, New York, 1974.