

I. Del Corso

## ON KRONECKER'S USE OF INDETERMINATE COEFFICIENTS

**Abstract.** In this paper we present some results of Kronecker on divisor theory using the modern terminology of ideals. This approach, although restrictive in several respects, makes some of the fundamental ideas of Kronecker's theory much more apparent and allows to improve upon many classical results. We also include a survey of some results we obtained in [10] using Kronecker's method of indeterminate coefficients.

### 1. Introduction

Towards the middle of the last century, Kummer discovered that the ring of integers of a cyclotomic field does not have the unique factorization property.

Kummer introduced the concept of "ideal numbers" to recover some of the structural properties of the usual integers in the ring of integers of the cyclotomic field.

Kronecker's theory of divisors and Dedekind's theory of ideals arose as attempts to do the same in a more general context.

To recover some good property resembling unique factorization, it is necessary to enlarge the set of elements under consideration and to generalize the concept of divisibility to this new set of elements.

Dedekind generalized the concept of number to that of ideal, and proved that each ideal factors uniquely into prime ideals in any number ring (see [7]). The theory of Dedekind domains as it is known today, is based on Dedekind's ideas and results.

Kronecker considered [14] a more general problem and a context more general than number fields (see [11] for a recent presentation of Kronecker's paper). The primary objective of his theory is to extend the set of elements and the concept of divisibility in such a way that any finite set of elements, all of which are algebraic over a field  $K$ , has a greatest common divisor.

Let  $R$  be a PID, and let  $K$  be its quotient field; Kronecker's *divisors* are precisely

all the possible gcd's of finite sets of algebraic elements over  $K$ . A divisor is *integral* if it is the gcd of elements which are integral over the ring  $R$ .

The divisors can be represented as equivalence classes of polynomials and a given polynomial represents the class of the divisor associated with the set of its coefficients.

More precisely, the equivalence relation is defined in the following way:

**DEFINITION 1.1.** *Let  $F$  be a finite extension of  $K$  and let  $S$  be the integral closure of  $R$  in  $F$ . Let  $\underline{u} = \{u_1, \dots, u_t\}$  be a set of indeterminates. The polynomial  $f \in S[\underline{u}]$  is called **primitive** if  $N_{F/K}(f(\underline{u})) \in R[\underline{u}]$  is primitive i.e. if the gcd of its coefficients is 1.*

Let  $f_1, f_2 \in F[\underline{u}]$ ; then  $f_1$  and  $f_2$  represent the same divisors if there exist  $g_1, g_2 \in S[\underline{u}]$  primitive such that  $f_1 g_1 = f_2 g_2$ . We denote by  $[f]$  the divisor represented by  $f$ .

We say that  $[f_1] | [f_2]$  if the quotient of the usual division is of the form  $g(\underline{u})/h(\underline{u})$  with  $g, h \in S[\underline{u}]$  and  $h(\underline{u})$  primitive. Finally we say that  $[f_1] || [f_2]$  if  $[f_1] | f$  for any representative  $f$  of  $[f_2]$ .

Actually Kronecker did not define the divisors as equivalence classes of polynomials, but as equivalence classes of rational functions having as numerator any polynomial with algebraic coefficients and as denominator a primitive polynomial. It is clear that the primitive polynomials are the units for this divisibility, hence any divisor has polynomial representatives and the definitions just given do not change when introducing these new elements.

With these definitions of divisors and divisibility Kronecker proved that the divisor  $[f]$  is the greatest common divisor of the coefficients of any polynomial representing the divisor.

Although his context is much more general, Kronecker's theory was presented in several respects as an alternative to Dedekind's theory of ideals. Kronecker considered the theory of ideals too abstract, but, in addition to this philosophical difference, he pointed out the true limit of Dedekind's theory. Dedekind's theory leads to the study of a number ring through the minimal polynomial of an integral generator of its quotient field. This method is exhaustive only in the case when the number ring is monogenic, i.e. when it is completely represented by an integral element. On the other hand, Kronecker's method is based on the use of indeterminates to construct new elements: in this context it is natural to consider a *generic element* of the ring, i.e., a linear combination with indeterminate coefficients of the elements of an integral basis. Kronecker's theory leads to the inspection of a number ring through the minimal polynomial of a generic element. The minimal polynomials of the algebraic integers, used by Dedekind, can then be seen as specializations of the minimal polynomial of the generic element. But - as Kronecker observes - considering

the specializations only is often misleading since some relevant information may be left hidden. For example, from the minimal polynomial of a generic element one can obtain the explicit factorization of any rational prime in any number ring, while considering the specifications only may not be enough.

In the case of one dimensional rings, the method of indeterminate coefficients can be significantly improved, since in many cases the same information can be obtained by considering as a generic element a linear combination of a set of algebra generators (instead of an integral basis) and with coefficients which are distinct monomials (instead of distinct variables) (see for example [9]).

The paper is organized as follows.

In Section 2 we recall some classical definitions and results of the theory of Dedekind domains we shall use in the paper.

In Section 3 we firstly introduce some general notation. Let  $A$  be a commutative ring we call a polynomial of  $A[\underline{u}]$  primitive if the ideal generated by its coefficients is the whole ring  $A$ , and we denote by  $A(\underline{u})$  the localization at primitive polynomials of the ring  $A[\underline{u}]$ . We also recall some properties of the ring  $A(\underline{u})$ , some of which can be found also in [16], [1] and [12].

Using this notation we can present some of the Kronecker results concerning one dimensional rings, in terms of ideals (see also [6], [18], [12]). Even if reading Kronecker's theory in terms of ideals is limitative in many respects, however this approach makes some of the fundamental ideas of Kronecker's theory much more apparent and allows to improve upon many classical results.

Using the modern terminology, the properties of Kronecker's divisibility can be expressed by a generalized version of the Gauss lemma (Lemma 3.1), which turns out to be a fundamental tool in this theory.

Let  $S$  be a Dedekind domain: from the definitions just given it easily follows that the divisors of  $S$  are exactly the principal ideals of the ring  $S(\underline{u})$ . Since  $S(\underline{u})$  is a principal ideal domain and the extension of ideals from  $S$  to  $S(\underline{u})$  is an isomorphism between the groups of the fractional ideals of these rings (see Corollary 3.6), it follows that the divisors of  $S$  correspond to the ideals of  $S$ . A fundamental result of Kronecker's theory is that a divisor really represents the greatest common divisor of the coefficients of any polynomial in the class of that divisor. In this paper this will follow from Theorem 3.7: in fact, this theorem ensures that the ring  $S(\underline{u})$  is a principal ideal domain and in particular that each polynomial generates in  $S(\underline{u})$  the same ideal of that generated by its coefficients, hence it represents their gcd.

Moreover, the Dedekind domain  $S(\underline{u})$  turns out to be monogenic, then its ideals can be studied by means of the classical theory. This allows to study also the ideals of  $S$ .

In Section 4 we present some of the results of [10]: we consider the general case of orders in Dedekind domains. In this case the generic element is not as nicely related to the ring itself as in the case of integrally closed rings; however, by a refinement of the method of indeterminate coefficients, we are able to generalize many results of Dedekind theory to all orders. In particular, we give an algorithm to derive a generating set for prime ideals of  $A$  and for the  $P$ -radical, when  $P$  is a prime ideal of  $R$ , and an algorithm for the primary decomposition of ideals of  $A$ . These algorithms generalize the well known algorithms for monogenic orders. Finally we state a generalized version of the Dedekind criterion for testing the maximality of an order  $A$ .

## 2. Classical results

Let  $R$  be a Dedekind domain and let  $K$  be its quotient field. Let  $F$  be a finite and separable extension of  $K$  of degree  $n$ . The integral closure  $S$  of  $R$  in  $F$  is a Dedekind domain. Denote by  $\sigma_1, \dots, \sigma_n$  the embeddings of  $F$  in a given algebraic closure of  $K$ . We denote by  $P$  a prime ideal of  $R$ , and the sign  $\bar{\phantom{x}}$  will indicate reduction modulo  $P$ . If  $X$  is an  $R$ -module,  $X_P$  will indicate the localization of  $X$  at  $P$ .

**DEFINITION 2.1.** *Let  $X \subseteq F$  be a finitely generated  $R$ -module.  $X$  is called **full** if it contains  $n$  linearly independent elements (over the field  $K$ ).*

*A full  $R$ -module  $\mathcal{O}$  of the field  $F$ , which is a ring and contains 1, is called an  **$R$ -order** of the field  $F$ . We say simply that  $\mathcal{O}$  is an  $R$ -order, without mentioning the field, when no confusion may arise.*

We recall that  $S$  is the maximal  $R$ -order of  $F$  (see [3], p.92 for the case of number fields; the same argument proves the general case).

**DEFINITION 2.2.** *An  $R$ -order  $\mathcal{O}$  is called  **$P$ -maximal order** if its localization at  $P$  is the maximal  $R_P$ -order of  $F$ , i.e., if  $\mathcal{O}_P = S_P$ .*

**DEFINITION 2.3.** *An  $R$ -order of the form  $R[\alpha]$  is called **monogenic**.*

Many properties of monogenic orders can be easily derived from the minimal polynomial of a generator. Unfortunately the ring  $S$  is not monogenic in general: this makes effective computations in  $S$  more complicated.

Suppose  $F = K(\xi)$  with  $\xi$  integral over  $R$ . In general  $R[\xi]$  is not a Dedekind domain; however, it is a noetherian integral domain of Krull dimension 1, hence its ideals have a unique primary decomposition. The prime ideals of  $R[\xi]$  and the primary decomposition of its ideals can be explicitly described in terms of the minimal polynomial  $T(x) \in R[x]$  of  $\xi$ .

Let  $\bar{\phantom{x}}$  denote the reduction modulo  $P$ ; let

$$(2.1) \quad \bar{T}(x) = \bar{T}_1(x)^{e_1} \cdots \bar{T}_r(x)^{e_r}$$

be the factorization of  $\bar{T}$  and denote by  $T_i(x)$  any monic representative of  $\bar{T}_i(x)$  in  $R[x]$ .

**PROPOSITION 2.1.** *The prime ideals of  $R[\xi]$  lying over  $P$  are exactly  $(P, T_i(\xi))$ . Moreover*

$$(2.2) \quad PR[\xi] = (P, T_1^{e_1}(\xi)) \cdots (P, T_r^{e_r}(\xi))$$

is the primary decomposition of the extension of  $P$  to  $R[\xi]$ .

*Proof.* The polynomials  $\bar{T}_i(x)$  are irreducible, hence  $(R/P)(x)/(\bar{T}_i(x))$  is a field for each index  $i$ . Since  $R[\xi]/(P, T_i(\xi)) \cong (R/P)(x)/(\bar{T}_i(x))$ , we get that  $Q_i = (P, T_i(\xi))$  is prime, and that  $(P, T_i^{e_i}(\xi))$  is  $Q_i$ -primary for each  $i$ .

Moreover, it is easy to see that

$$PR[\xi] \subseteq \bigcap_{i=1}^r (P, T_i^{e_i}(\xi)) = \prod_{i=1}^r (P, T_i^{e_i}(\xi)) \subseteq (P, T(\xi)) = PR[\xi]$$

and this proves (2.2).

Finally, taking the radical of both members in equation (2.2), one sees that the only primes in  $R[\xi]$  containing  $P$  are the  $Q_i$ . ■

**PROPOSITION 2.2.** *Let  $G(x) = T_1(x) \cdots T_r(x)$ ; then the  $P$ -radical  $\mathcal{J}_P$  of  $R[\xi]$  is given by  $\mathcal{J}_P = (P, G(\xi))$ .*

*Proof.* See [5] p.298. ■

Dedekind domains are characterized, in the class of all integral domains, by the unique factorization property of their ideals: the following theorem, due to Kummer, allows to compute explicitly the splitting of  $PS$  from the factorization modulo  $P$  of the polynomial  $T(x)$ , whenever the order  $R[\xi]$  is  $P$ -maximal. Nevertheless, it is important to note that there are cases in which no monogenic order is  $P$ -maximal (see [17], p.64): in such cases Kummer's theorem cannot be used to compute the factorization of  $PS$ .

**THEOREM 2.3 (KUMMER).** *Notation being as above, suppose  $R[\xi]$  to be  $P$ -maximal. Then*

$$PS = Q_1^{e_1} \cdots Q_r^{e_r}$$

where  $Q_i = (P, T_i(\xi))$ . Moreover, the inertial degree of  $Q_i$  over  $P$  is equal to the degree of  $T_i$ .

*Proof.* See [15], p.27. ■

The following criterion, due to Dedekind, allows to decide in a quite simple way whether  $R[\xi] = S$ ; more precisely, for each prime  $P \subset R$ , it gives a way to investigate whether  $R[\xi]$  is  $P$ -maximal or not, and if it is not, it gives an element belonging to  $S$  but not to  $R[\xi]$ , so that we can enlarge the order. The limit of this criterion is that it works only for monogenic orders and hence it cannot be applied more than once for the same prime  $P$ . In the case of number fields, however, there are algorithms for computing the maximal order, but none is so simple as Dedekind criterion (see for example [5] and [19]).

**THEOREM 2.4 (DEDEKIND).** *Suppose  $R$  to be a principal ideal domain and let  $P = (\pi)$ . Let  $H(x) \in R[x]$  be a monic lift of  $\bar{T}(x)/\bar{G}(x)$  (where  $G(x) = T_1(x) \cdots T_r(x)$ ) and set*

$$J(x) = (G(x)H(x) - T(x))/\pi \in R[x].$$

- (1)  $R[\xi]$  is  $P$ -maximal if and only if

$$(\bar{G}, \bar{H}, \bar{J}) = 1 \quad \text{in } (R/P)[x].$$

- (2) Let  $U$  be a monic lift of  $\bar{T}/(\bar{G}, \bar{H}, \bar{J})$  to  $R[x]$ , and let  $\mathcal{O} = R[\xi] + \frac{1}{\pi}U(\xi)R[\xi]$ .

Then  $\mathcal{O} \subseteq T$  and if  $m = \deg(\bar{G}, \bar{H}, \bar{J})$ , then  $\text{disc}_{F/K}(T) = P^{2m} \text{disc}_{F/K}(\mathcal{O})$ .

*Proof.* See [5], p.299, for the case  $R = \mathbb{Z}$ ; the same argument works for any principal ideal domain  $R$ . ■

### 3. Divisor theory for Dedekind domains

Let  $A$  be a commutative ring with identity and let  $\{u_1, \dots, u_t\}$  be a set of indeterminates. We write  $A[\underline{u}]$  instead of  $A[u_1, \dots, u_t]$ ; and we denote by  $\langle \underline{u} \rangle$  the monoid of the monic monomials in the indeterminates  $u_1, \dots, u_t$ .

**DEFINITION 3.1.** For  $f \in A[\underline{u}]$  denote by  $C(f)$  the ideal generated in  $A$  by the coefficients of  $f$ . The polynomial  $f$  is called *primitive* if  $C(f) = A$ .

The following generalization of the Gauss lemma (see [13] p.52) will guarantee that Kronecker's theory of divisibility preserves the good properties of the divisibility between integers.

**LEMMA 3.1.** *Let  $A$  be a commutative ring and let  $f, g \in A[\underline{u}]$ .*

- (i)  $C(fg) \subseteq C(f)C(g)$
- (ii) If  $C(f) = C(g) = A$ , then  $C(fg) = A$
- (iii) If  $A$  is a domain and  $C(f)$  is invertible, then  $C(fg) = C(f)C(g)$
- (iv) If  $A$  is a domain and  $(C(f), C(g)) = A$ , then  $C(fg) = C(f)C(g)$ .

*Proof.* Part (i) is trivial. Suppose  $C(fg)$  is not the whole ring; then it is contained in a maximal ideal  $M$  of  $A$ . Denote by  $\bar{\phantom{x}}$  the projection of  $A[\underline{u}]$  onto  $(A/M)[\underline{u}]$ , then  $\overline{f(\underline{u})g(\underline{u})} = \overline{f(\underline{u})} \overline{g(\underline{u})} = 0$ , hence either  $\overline{f(\underline{u})} = 0$  or  $\overline{g(\underline{u})} = 0$ , proving (ii).

The general case of part (iii) easily follows from the case when  $A$  is a local ring and  $C(f) = A$ . Moreover we can restrict to the case of polynomials in one indeterminate: in fact, for each substitution  $\varphi(u_i) = x^{n_i}$  we have  $C(\varphi(f)\varphi(g)) \subseteq C(fg)$ , and we may choose the  $n_i$  so that  $C(f) = C(\varphi(f))$  and  $C(g) = C(\varphi(g))$ ; hence, once proved  $C(f)C(g) = C(\varphi(f))C(\varphi(g)) = C(\varphi(f)\varphi(g))$  we get also the general case.

Under these assumptions, we claim that

$$(3.1) \quad C(g) = C(fg) + M C(g)$$

where  $M$  denotes the maximal ideal of  $A$ .

Let  $f(u) = \sum_{i=0}^n a_i u^i$  and  $g(u) = \sum_{j=0}^m b_j u^j$ ; condition  $C(f) = A$  ensures that not all  $a_i$  belong to  $M$ . Let  $a_k \notin M$ , with  $k$  minimum with respect to this property. Looking at the coefficient of  $u^k$  of  $f(u)g(u)$  it is trivial to verify that  $b_0 \in C(fg) + M C(g)$ , and, using an inductive argument we get  $b_j \in C(fg) + M C(g)$  for each  $j = 0, \dots, m$ . Finally, from equation (3.1), using Nakayama's lemma, we obtain  $C(fg) = C(g)$ , hence  $C(fg) = C(f)C(g)$ .

To prove (iv) it is enough to prove that

$$(3.2) \quad C(fg)A_Q = C(f)A_Q C(g)A_Q$$

for each prime ideal  $Q \subset A$ . Condition  $(C(f), C(g)) = A$  ensures that for each prime  $Q \subset A$ , either  $C(f) \not\subseteq Q$  or  $C(g) \not\subseteq Q$ , hence at least one between  $C(f)A_Q$  and  $C(g)A_Q$  is the whole ring  $A_Q$  and equation (3.2) follows from part (iii). ■

**COROLLARY 3.2.** *Let  $S$  be a Dedekind domain. Then  $C(fg) = C(f)C(g)$  for each  $f, g \in S[\underline{u}]$ .*

*Proof.* Since all ideals of a Dedekind domain are invertible, the corollary follows from part (iii) of Lemma 3.1. ■

**COROLLARY 3.3.** *Let  $A$  be an integral domain and let  $F$  be its quotient field. Let  $f, g \in A[\underline{u}]$  with  $g$  primitive. Suppose that  $g$  divides  $f$  in  $F[\underline{u}]$ ; then  $g$  divides  $f$  in  $A[\underline{u}]$ .*

*Proof.* Let  $h \in F[\underline{u}]$  such that  $f(\underline{u}) = g(\underline{u})h(\underline{u})$ , and let  $c \in A$  such that  $ch(\underline{u}) = h_1(\underline{u}) = \sum d_j \underline{u}^j \in A[\underline{u}]$ . Multiplying by  $c$  we get the following relation between polynomials of  $A[\underline{u}]$

$$cf(\underline{u}) = g(\underline{u})h_1(\underline{u})$$

Taking contents of both members, using hypothesis  $C(g) = A$  and Lemma 3.1 (iii), we obtain

$$(c)C(f) = C(gh_1) = C(g)C(h_1) = C(h_1)$$

and this guarantees that the coefficients of  $h_1$  are multiples of  $c$ , say  $d_i = \delta_i c$  (where  $\delta_i \in A$  and  $i = 1, \dots, m$ ), whence  $h(\underline{u}) = \sum_{i=1}^m \delta_i \underline{u}^{J_i} \in A[\underline{u}]$ . ■

Let  $A$  be an integral domain and let denote by  $T_{A[\underline{u}]}$  the set of primitive polynomials of  $A[\underline{u}]$ .

It is an easy exercise to prove the following proposition:

**PROPOSITION 3.4.** *Let  $\{M_\lambda\}_{\lambda \in \Lambda}$  be the set of maximal ideals of  $A$ . Then  $T_{A[\underline{u}]} = A[\underline{u}] - \cup_{\lambda \in \Lambda} M_\lambda[\underline{u}]$ .*

**DEFINITION 3.2.** We denote by  $A(\underline{u})$  the localization  $(A[\underline{u}])_{T_{A[\underline{u}]}}$ .

Let  $I \subseteq A$  be an ideal, then  $I[\underline{u}]$  and  $I(\underline{u})$  will denote the extension of  $I$  to  $A[\underline{u}]$  and  $A(\underline{u})$  respectively.

**PROPOSITION 3.5.** *There is a one to one correspondence, induced by inclusion, between the maximal ideals of  $A$  and those of  $A(\underline{u})$ .*

*Moreover if the ring  $A$  is noetherian, then  $A$  and  $A(\underline{u})$  have the same Krull dimension. In particular, if  $A$  is an integral domain of dimension 1, there is a one to one correspondence between the prime ideals of  $A$  and those of  $A(\underline{u})$ .*

*Proof.* The maximal ideals of  $A(\underline{u})$  are exactly the extensions of those ideals of  $A[\underline{u}]$  which are maximal among the ideals which do not meet  $T_{A[\underline{u}]}$  (see [2], prop. 3.11), hence, by Proposition 3.4,  $\{M_\lambda(\underline{u})\}_{\lambda \in \Lambda}$  is the set of maximal ideals of  $A(\underline{u})$ .

If the ring  $A$  is noetherian, then

$$\dim A[u_1, \dots, u_t] = \dim A + t$$

(see, for example, [2], p.183). Let  $M$  be a maximal ideal of  $A$ , then  $M[\underline{u}] \subset (M, u_1) \subset \dots \subset (M, u_1, \dots, u_t)$  hence  $\text{ht } M[\underline{u}] \leq \dim A[\underline{u}] - t = \dim A$ . Since  $\text{ht } M(\underline{u}) = \text{ht } M[\underline{u}]$  it follows that  $A$  and  $A(\underline{u})$  have the same dimension. Finally, if  $A$  is an integral domain of dimension 1, the same is true for  $A(\underline{u})$ , hence their prime ideals are only the maximal ones (which are in one to one correspondence) and the 0 ideal. ■

**COROLLARY 3.6.** *Let  $S$  be a Dedekind domain, then  $S(\underline{u})$  is a Dedekind domain. Moreover the extension of ideals is an isomorphism between the group of fractional ideals of  $S$  and those of  $S(\underline{u})$ .*

*Proof.* By Proposition 3.5 the ring  $S(\underline{u})$  is an integral domain of Krull dimension 1. Moreover  $S(\underline{u})$  is noetherian and integrally closed, since  $S$  is such and these properties are inherited by the ring of polynomials and are preserved by localization, whence  $S(\underline{u})$  is a Dedekind domain.

Finally, we recall that prime ideals in Dedekind domains are free generators for the group of fractional ideals, hence the one to one correspondence between the primes of  $S$  and  $S(\underline{u})$  can be extended to an isomorphism between the whole groups of ideals of  $S$  and  $S(\underline{u})$ . ■

**THEOREM 3.7.** *Let  $S$  be a Dedekind domain. Then  $S(\underline{u})$  is a PID.*

*Proof.* Corollary 3.6 ensures that all ideals of  $S(\underline{u})$  are extended ideals, hence they can be generated by elements of  $S$ . Let  $J = (r_1, \dots, r_v)$  be an ideal of  $S$  and let  $f(\underline{u}) \in S[\underline{u}]$  be a polynomial with  $C(f) = \{r_1, \dots, r_v\}$ . The ideal  $(f(\underline{u}))$  is of the form  $I(\underline{u})$  for a suitable ideal  $I$  of  $S$ . Since  $f(\underline{u}) \in I(\underline{u})$ , then there exist  $\xi(\underline{u}) \in I[\underline{u}]$  and  $s(\underline{u}) \in S(\underline{u})$  primitive such that  $f(\underline{u}) = \xi(\underline{u})/s(\underline{u})$ , hence  $f(\underline{u})s(\underline{u}) = \xi(\underline{u})$ . Taking contents and using Lemma 3.1, we get  $J = (C(f(\underline{u}))) = (C(f(\underline{u}))(C(s(\underline{u}))) = (C(\xi(\underline{u}))) \subseteq I$ . Clearly  $I(\underline{u}) \subseteq J(\underline{u})$ , hence they are equal, i.e.  $J(\underline{u})$  is principal. ■

**REMARK 3.1.** From the proofs just given it is clear that for  $h_i = f_i/g_i \in S(\underline{u})$  ( $i = 1, \dots, m$  and  $f_i, g_i \in S[\underline{u}]$  with  $C(g_i) = S$ ) we have the following equalities in  $S(\underline{u})$ :

$$\begin{aligned} (f_1(\underline{u})/g_1(\underline{u}), \dots, f_m(\underline{u})/g_m(\underline{u})) &= (f_1(\underline{u}), \dots, f_m(\underline{u})) \\ &= \left( \sum_{i=1}^m \underline{u}^{J_i} f_i(\underline{u}) \right) = (C(f_1), \dots, C(f_m)) \end{aligned}$$

where the  $\underline{u}^{J_i}$ 's are suitably chosen monomials of  $\langle \underline{u} \rangle$ .

**REMARK 3.2.** From the definition of Kronecker's divisors given in the introduction it follows that each integral divisor is represented by an element of  $S(\underline{u})$ , and that two elements of  $S(\underline{u})$  represent the same divisor if and only if they generate the same ideal in  $S(\underline{u})$ . In other words, since  $S(\underline{u})$  is a principal ideal domain, the divisors of  $S$  are precisely the ideals of  $S(\underline{u})$ .

On the other hand, we have just proved that the ideals of  $S(\underline{u})$  are in one-to-one correspondence with those of  $S$ , hence the ideals of  $S$  correspond to the divisor of  $S$ . More precisely each divisor of  $S$  corresponds to the ideal generated by the coefficients of any of its polynomial representatives, hence in Kronecker's language it represents their greatest common divisor.

**PROPOSITION 3.8.** *Let  $A$  be an integral extension of the Dedekind domain  $R$ , then  $A(\underline{u}) = (A[\underline{u}])_{T_{R[\underline{u}]}} \cong A \otimes_R R(\underline{u})$  and it is integral over  $R(\underline{u})$ . In particular,  $S(\underline{u})$  is the integral closure of  $R(\underline{u})$  in  $F(\underline{u})$ .*

*Proof.* Clearly  $(A[\underline{u}])_{T_{R[\underline{u}]}} \subseteq A(\underline{u})$ ; to prove equality we have to show that if  $a(\underline{u}) \in A[\underline{u}]$  is primitive then  $1/a(\underline{u}) \in (A[\underline{u}])_{T_{R[\underline{u}]}}$ . Let  $L$  be the finite extension of  $K$  generated by the coefficients of  $a(\underline{u})$  and denote by  $N_{L/K}$  the usual norm from  $L$  over  $K$ . Then  $N_{L/K}(a(\underline{u}))$  is a primitive polynomial of  $R[\underline{u}]$ . From Corollary 3.3, it follows that  $\tilde{N}_{L/K}(a(\underline{u})) = N_{L/K}(a(\underline{u}))/a(\underline{u})$  belongs to  $A[\underline{u}]$ . We have  $1/a(\underline{u}) = \tilde{N}_{L/K}(a(\underline{u}))/N_{L/K}(a(\underline{u}))$  hence it belongs to  $(A[\underline{u}])_{T_{R[\underline{u}]}}$ .

Moreover, it is trivial to verify that the map  $a \otimes r_1(\underline{u})/r_2(\underline{u}) \mapsto ar_1(\underline{u})/r_2(\underline{u})$  induces an isomorphism between the rings  $A \otimes_R R(\underline{u})$  and  $(A[\underline{u}])_{T_{R[\underline{u}]}}$ .

Since the ring  $S$  is the integral closure of  $R$  in  $F$ , the polynomial ring  $S[\underline{u}]$  is the integral closure of  $R[\underline{u}]$  in  $F[\underline{u}]$  (see [2], p.105) and hence in  $F(\underline{u})$  since  $F[\underline{u}]$  is integrally closed. Localizing at  $T_{R[\underline{u}]}$  we obtain that  $S(\underline{u}) = (S[\underline{u}])_{T_{R[\underline{u}]}}$  is the integral closure of  $R(\underline{u})$  in  $F(\underline{u})$ ; this ensures also that  $A(\underline{u})$ , which is included in  $S(\underline{u})$ , is integral over  $R(\underline{u})$ . ■

**PROPOSITION 3.9.** *Let  $A$  be a finitely generated integral extension of  $R$ , then the discriminant of  $A(\underline{u})$  over  $K(\underline{u})$  is the extension to  $R(\underline{u})$  of the discriminant of  $A$  over  $K$ .*

*Proof.* We can reduce to the case when  $A$  is a free  $R$ -module (otherwise we can localize and use the well known properties of the discriminant). A basis  $\{\alpha_i\}$  for  $A$  over  $R$  is also a  $R(\underline{u})$ -basis of  $A(\underline{u})$ . On the other hand, the embeddings of  $F(\underline{u})$  over  $K(\underline{u})$  are the obvious extensions of the embeddings  $\sigma_j$  of  $F/K$ , hence  $\text{disc}_{F/K} A$  and  $\text{disc}_{F(\underline{u})/K(\underline{u})} A(\underline{u})$  are both equal to  $|\sigma_j(\alpha_i)|^2$ . ■

Let  $S = R[\alpha_1, \dots, \alpha_k]$  and let  $\alpha(\underline{u}) = \sum_{i=1}^k m_i \alpha_i$  and the  $m_i \in \langle \underline{u} \rangle$  are distinct. Let  $T(X) \in R(\underline{u})[X]$  be the minimal polynomial of  $\alpha(\underline{u})$  over  $R(\underline{u})$ .

We know that in general a Dedekind domain  $S$  is not monogenic over  $R$ . The following theorem ensures that  $S(\underline{u})$  is always monogenic over  $R(\underline{u})$ .

**THEOREM 3.10.**  $S(\underline{u}) = R(\underline{u})[\alpha(\underline{u})]$ .

*Proof.* Clearly  $R(\underline{u})[\alpha(\underline{u})] \subseteq S(\underline{u})$ , hence

$$(3.3) \quad \text{disc}_{F(\underline{u})/K(\underline{u})} R(\underline{u})[\alpha(\underline{u})] \subseteq \text{disc}_{F(\underline{u})/K(\underline{u})} S(\underline{u})$$

and the rings are equal if and only if inclusion in equation (3.3) is an equality.

The discriminant of  $S(\underline{u})$  is the norm of its different, and the discriminant of  $R(\underline{u})[\alpha(\underline{u})]$  is the norm of the different of  $\alpha(\underline{u})$  (see [17] pp.155-162): denoting the different

by  $\mathcal{D}_{F(\underline{u})/K(\underline{u})}$  it is enough to prove that

$$\mathcal{D}_{F(\underline{u})/K(\underline{u})}(S(\underline{u})) \subseteq \mathcal{D}_{F(\underline{u})/K(\underline{u})}(\alpha(\underline{u})).$$

Now  $\mathcal{D}_{F(\underline{u})/K(\underline{u})}(S(\underline{u}))$  is the ideal generated by the differentials of all elements of  $S(\underline{u})$  (see [17] Thm 4.6), or, equivalently (see Proposition 3.9), of all elements of  $S$ , i.e.  $\mathcal{D}_{F(\underline{u})/K(\underline{u})}(S(\underline{u})) = (\{T'_\xi(\xi)\}_{\xi \in S})$ , where  $T_\xi$  denote the minimal polynomial of  $\xi$  over  $R$ .

On the other hand  $\mathcal{D}_{F(\underline{u})/K(\underline{u})}(\alpha(\underline{u})) = (T'_{\alpha(\underline{u})}(\alpha(\underline{u}))) = (\prod_j (\alpha(\underline{u}) - \tilde{\sigma}_j(\alpha(\underline{u}))))$  where  $2 \leq j \leq [F : K]$  and we suppose  $\sigma_1 = \text{identity}$ .

Let  $L$  denote the normal closure of  $F$  over  $K$ , and let  $V$  be the integral closure of  $R$  in  $L$ . Being  $V$  a Dedekind domain, each ideal of  $V(\underline{u})$  is the extension of an ideal of  $V$ , hence

$$\begin{aligned} \mathcal{D}_{F(\underline{u})/K(\underline{u})}(\alpha(\underline{u}))V(\underline{u}) &= \prod_j (\alpha(\underline{u}) - \tilde{\sigma}_j(\alpha(\underline{u}))) = \prod_j C(\alpha(\underline{u}) - \tilde{\sigma}_j(\alpha(\underline{u}))) \\ &= \prod_j (\alpha_1 - \sigma_j(\alpha_1), \dots, \alpha_k - \sigma_j(\alpha_k)) \end{aligned}$$

We claim that

$$(3.4) \quad \mathcal{D}_{F(\underline{u})/K(\underline{u})}(\alpha(\underline{u}))V(\underline{u}) = \prod_j (\{\xi - \sigma_j(\xi)\}_{\xi \in S})$$

Since one inclusion is trivial, proving (3.4) reduces to show that  $\xi - \sigma_j(\xi)$  belongs to the ideal  $(\alpha_1 - \sigma_j(\alpha_1), \dots, \alpha_k - \sigma_j(\alpha_k))$  for each  $\xi \in S$  and for each index  $j$ . It is easy to see that what claimed will follow once proved that, if  $\xi = \alpha_1^{l_1} \dots \alpha_k^{l_k}$  ( $l_i \geq 0$ ) is a monomial, then  $(\xi - \sigma(\xi)) \in (\alpha_1 - \sigma(\alpha_1), \dots, \alpha_k - \sigma(\alpha_k))$  for each  $\sigma \in \{\sigma_2, \dots, \sigma_n\}$ . This is clear if  $l = \sum_{i=1}^k l_i = 1$ . For  $l > 1$ , we can suppose  $l_1 \geq 1$ ; then  $\xi - \sigma\xi = (\alpha_1 - \sigma(\alpha_1))\alpha_1^{l_1-1} \dots \alpha_k^{l_k} + \sigma(\alpha_1)(\alpha_1^{l_1-1} \dots \alpha_k^{l_k} - \sigma(\alpha_1^{l_1-1} \dots \alpha_k^{l_k}))$ , and the claim follows by induction on  $l$ .

Finally, it is trivial to see that  $\mathcal{D}_{F(\underline{u})/K(\underline{u})}(S(\underline{u}))V(\underline{u}) \subseteq \mathcal{D}_{F(\underline{u})/K(\underline{u})}(\alpha(\underline{u}))V(\underline{u})$ . This together with equation (3.3) gives

$$\mathcal{D}_{F(\underline{u})/K(\underline{u})}(S(\underline{u})) = \mathcal{D}_{F(\underline{u})/K(\underline{u})}(\alpha(\underline{u}))$$

hence  $S(\underline{u}) = R(\underline{u})[\alpha(\underline{u})]$ . ■

COROLLARY 3.11.

$$\text{disc}_{F/K} S = C(N_{F(\underline{u})/K(\underline{u})}(T'(\alpha(\underline{u}))))$$

*Proof.* The last theorem ensures that

$$\text{disc}_{F(\underline{u})/K(\underline{u})} S(\underline{u}) = \text{disc}_{F(\underline{u})/K(\underline{u})} R(\underline{u})[\alpha(\underline{u})] = N_{F(\underline{u})/K(\underline{u})}(T'(\alpha(\underline{u}))).$$

The thesis follows from Proposition 3.9. ■

**THEOREM 3.12.** *Let  $P \subset R$  be a prime ideal and let*

$$T \equiv T_1^{e_1}(x) \cdots T_r^{e_r}(x) \pmod{P}$$

*be the factorization of  $T$  modulo  $P$ . Then*

$$PS = Q_1^{e_1} \cdots Q_r^{e_r}$$

*where, for each  $i = 1, \dots, r$ , the inertial degree of  $Q_i$  over  $P$  is equal to the degree of  $T_i$  and  $Q_i = (P, C(T_i(\alpha(\underline{u}))))$ .*

*Proof.* Let

$$PS = Q_1^{a_1} \cdots Q_s^{a_s}$$

be the factorization of  $PS$ . Then Corollary 3.6 ensures that

$$PS(\underline{u}) = Q_1(\underline{u})^{a_1} \cdots Q_s(\underline{u})^{a_s}$$

is the factorization of  $PS(\underline{u})$ . On the other hand, being  $S(\underline{u}) = R(\underline{u})[\alpha(\underline{u})]$ , Kummer's theorem yields

$$PS(\underline{u}) = (P, T_1(\alpha(\underline{u})))^{e_1} \cdots (P, T_r(\alpha(\underline{u})))^{e_r}.$$

From the uniqueness of the factorization we get  $r = s$ ,  $e_i = a_i$  and  $Q_i(\underline{u}) = (P, T_i(\alpha(\underline{u})))$ , hence  $Q_i = (P, C(T_i(\alpha(\underline{u}))))$ . Finally it is easily seen that  $a_i = [(S/Q_i) : (R/P)] = e_i = \text{deg } T_i$ . ■

#### 4. Non-maximal orders

In the previous section we have shown that some information on the ring  $S$  can be derived from the analogous information on  $S(\underline{u})$ : this turns out to be convenient since the ring  $S(\underline{u})$  is monogenic, hence some of its properties can be easily obtained from the minimal polynomial of a generator of  $S(\underline{u})$  over  $R(\underline{u})$ .

Trying to do the same with a generic  $R$ -order  $A$  of  $F$  we soon realize that this is not so easy as in the case of the maximal order: in fact, in general the ring  $A(\underline{u})$  is not monogenic, hence, a priori, it is not easier to study than the ring  $A$  itself. On the other hand for  $A = R[\alpha_1, \dots, \alpha_k]$  we can try to study the ring  $A$  via the monogenic ring  $\mathcal{M} = R(\underline{u})[\alpha(\underline{u})]$  where  $\alpha(\underline{u}) = \sum_{i=1}^k m_i \alpha_i$  and the  $m_i \in \langle \underline{u} \rangle$  are distinct. But, while it is easy to relate properties of  $A$  to properties of  $A(\underline{u})$ , it is not so straightforward to do this with the ring  $\mathcal{M}$ . For example  $A$  and  $A(\underline{u})$  have the "same" discriminant (see Proposition 3.9) that in general is different from the discriminant of  $\mathcal{M}$ .

EXAMPLE 1. Let  $\mathbb{Z}_p$  denote the ring of  $p$ -adic integers, and let  $\pi$  be a root of the polynomial  $f(x) = x^5 - p$  in any algebraic closure of  $\mathbb{Q}_p$ . Let  $A = \mathbb{Z}_p[\pi^2, \pi^3]$ , then  $A(\underline{u}) = \mathbb{Z}_p(\underline{u})[\pi^2, \pi^3]$ . Let  $\mathcal{M} = \mathbb{Z}_p(\underline{u})[\pi^2 + u\pi^3]$ . It can be shown that  $\mathcal{M}$  is generated, as  $\mathbb{Z}_p(\underline{u})$ -module, by the set  $\{1, \pi^2 + u\pi^3, \pi^4, \pi^6, \pi^7\}$ . It is apparent that  $\mathcal{M}$  is strictly contained in  $A(\underline{u})$ .

Nevertheless, the following theorem ensures that the ring  $\mathcal{M}$  and the ring  $A(\underline{u})$  are very similar to each other.

For the proof of the results of this section see [10].

THEOREM 4.1. *Notation being as above,*

- (1)  $A(\underline{u})$  and  $\mathcal{M}$  have the same quotient field.
- (2) There is a one to one correspondence between the set of prime ideals of  $A(\underline{u})$  and  $\mathcal{M}$ . Moreover,  $A(\underline{u})$  and  $\mathcal{M}$  have isomorphic residue fields at corresponding primes.
- (3) Let  $I \subseteq \mathcal{M}$  be an ideal and let

$$I = P_1 \cdots P_r$$

be its primary decomposition. Denote by  $*$  the extension to  $A(\underline{u})$  of ideals of  $\mathcal{M}$ . Then

$$I^* = P_1^* \cdots P_r^*$$

is the primary decomposition of  $I^*$ .

In the following we give results on the  $R$ -order  $A$ : roughly speaking we can say that these results are obtained by relating the properties of  $A$  to those of  $A(\underline{u})$  and getting the last from the analogous properties of  $\mathcal{M}$ , using Theorem 4.1.

Let  $T(x) \in R(\underline{u})[x]$  be the minimal polynomial of  $\alpha(\underline{u})$  over  $R(\underline{u})$ . Let  $P \subseteq R$  be a prime ideal; denote by  $\bar{\phantom{x}}$  the projection on  $(R/P)(\underline{u})[x]$ . Let

$$\bar{T} = \bar{T}_1^{e_1}(x) \cdots \bar{T}_r^{e_r}(x)$$

be the factorization of  $\bar{T}$ .

THEOREM 4.2. *Let  $m_1 = u_1, \dots, m_k = u_k$  be distinct indeterminates. Then the prime ideals of  $A$  lying over  $P$  are exactly  $Q_1, \dots, Q_r$ , where  $Q_j = (P, \mathcal{C}(T_j(\alpha(\underline{u}))))$ .*

*Moreover, for each index  $j$ , the residue field  $A/Q_j$  has degree  $f_j = \deg_x T_j(x)$  over  $R/P$ .*

REMARK 4.1. In the case  $A(\underline{u}) = R(\underline{u})[\alpha(\underline{u})]$  Theorem 4.2 is trivial and holds even when the  $m_i$  are any distinct monic monomials. In fact, in this case the primes of  $A(\underline{u})$  lying over  $P$  are exactly  $(P, T_j(\alpha(\underline{u})))$  for  $j = 1, \dots, r$ . Since the primes of  $A(\underline{u})$  are the extensions of the primes of  $A$ , we get that  $(P, \mathcal{C}(T_j(\alpha(\underline{u}))))$  is prime for each  $j$ .

In the general case, to prove Theorem 4.2 we need to assume that the  $m_i$  are distinct variables instead of distinct monic monomials as it would be natural in this context. I doubt whether, in the general case, this hypothesis is really necessary. This is not the case for example when  $\text{char}(R/P) = 0$  or is large enough.

**THEOREM 4.3.** *Let everything be as in Theorem 4.2 and let  $G(x) = T_1(x) \cdots T_r(x)$ . Then the  $P$ -radical of  $A$  is*

$$J_P = (P, C(G(\alpha(\underline{u}))))$$

**THEOREM 4.4.** *Let notation be as above, but  $m_1, \dots, m_k \in \langle \underline{u} \rangle$  be any monomials. Then*

$$PA = (P, C(T_1^{e_1}(\alpha(\underline{u})))) \cdots (P, C(T_r^{e_r}(\alpha(\underline{u}))))$$

*is the primary decomposition of the ideal  $PA$ .*

**COROLLARY 4.5 (ANALOGUE OF DEDEKIND CRITERION).** *Let  $P = (\pi(\underline{u}))$ , let  $\bar{T}(x) = \prod_{i=1}^r \bar{T}_i(x)^{e_i}$  and set  $G(x) = \prod_{i=1}^r T_i(x)$  where the  $T_i \in R(\underline{u})[x]$  are arbitrary monic lifts of  $\bar{T}_i$ . Let  $H(x) \in R(\underline{u})[x]$  be a monic lift of  $\bar{T}(x)/\bar{G}(x)$  and set*

$$J(x) = (G(x)H(x) - T(x))/\pi(\underline{u}) \in R(\underline{u})[x].$$

*Then  $A = R[\alpha_1, \dots, \alpha_k]$  is  $P$ -maximal if and only if*

$$(\bar{G}, \bar{H}, \bar{J}) = 1.$$

**REMARK 4.2.** Unfortunately, part (2) of Theorem 2.4 does not have a straightforward generalization to non-monogenic orders. In fact, if  $\mathcal{M}$  is not maximal, using the notation of Theorem 2.4, one gets that  $U(\alpha(\underline{u}))/\pi(\underline{u}) \notin \mathcal{M}$ . Corollary 4.5 ensures that also  $A$  is not maximal, but it may happen that all the coefficients of  $U(\alpha(\underline{u}))/\pi(\underline{u})$  belong to  $A$ .

In fact, consider example 1 again: the minimal polynomial of  $\pi^2 + u\pi^3$  over  $\mathbb{Z}_p(\underline{u})$  is  $T(x) = x^5 - 5pu^2x^3 + 5pu^2x - p^3u^5 - p^2$ , and it is easy to see that  $(\bar{G}, \bar{H}, \bar{J}) = x$ ; it follows that  $\mathcal{M}$  and  $\mathbb{Z}_p[\pi^2, \pi^3]$  are not maximal. Moreover  $(\pi^2 + u\pi^3)^4/p$  is not in  $\mathcal{M}$ , but all its coefficients belong to  $\mathbb{Z}_p[\pi^2, \pi^3]$ .

## REFERENCES

- [1] ARNOLD J.I., *On the Ideal Theory of the Kronecker Function Ring and the Domain  $D(X)$* , *Canad. J. Math.* **21** (1969), 558–563.
- [2] ATIYAH M.F., MACDONALD I.G., *Introduction to Commutative Algebra*, Addison-Wesley, (1969).
- [3] BOREVICH Z.I., SHAFAREVICH I.R., *Number Theory*, Academic Press, London (1966).
- [4] CASSELS J.W.S., FRÖHLICH A., *Algebraic Number Theory*, Academic Press, London (1967).
- [5] COHEN H., *A Course in Computational Algebraic Number Theory*, Springer-Verlag, New York (1993).
- [6] COHN H., *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag, New York (1978).
- [7] DEDEKIND R., *Über die Theorie der ganzen algebraischen Zahlen*, XI Suppl. to Dirichlet's "Vorlesungen über Zahlentheorie", (1871).
- [8] DEL CORSO I., *Factorization of Prime Ideal Extensions in Number Rings*, *Math.Comp.* **58** (1992), 849-853.
- [9] DEL CORSO I., *Factorization of Prime Ideal Extensions in Dedekind Domains*, *JSC* **19** (1995), 435–439.
- [10] DEL CORSO I., *Kronecker's Method of Indeterminate Coefficients*, (to appear).
- [11] EDWARDS H.M., *Divisor Theory*, Birkhäuser (1990).
- [12] GILMER R.W., *Multiplicative Ideal Theory*, Queen's Papers in Pure and Appl. Math., no.90, Queen's University (1992).
- [13] KAPLANSKY I., *Commutative Rings*, University of Chicago Press, Chicago (1974).
- [14] KRONECKER L., *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, *J. Reine Angew. Math.* **92** (1882), 1-122. Werke 2, 237-387.
- [15] LANG S., *Algebraic Number Theory*, Springer-Verlag, New York (1986).
- [16] NAGATA M., *Local Rings*, Interscience Publishers, New York (1962).
- [17] NARKIEWICZ W., *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag & PWN-Polish Scientific Publishers, Warszawa (1990).
- [18] PARSHIN A.N., SHAFAREVICH I.R. (EDS.), *Number Theory II*, Springer-Verlag (1992).
- [19] POHST M., ZASSENHAUS H., *Algorithmic Algebraic Number Theory*, Cambridge University Press (1989).

Ilaria DEL CORSO  
Dipartimento di Matematica  
Università di Pisa  
via Buonarroti, 2  
56127 Pisa, Italy.

