ACTA ARITHMETICA
120.3 (2005)

Decomposition of primes in non-maximal orders

by

Ilaria Del Corso (Pisa), Roberto Dvornicich (Pisa)
and Denis Simon (Caen)

1. Introduction. Let $F(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial, α be a root of F and $L = \mathbb{Q}(\alpha)$. Then the ring $\mathbb{Z}[\alpha]$ is a subgroup of finite index

$$\mathrm{Ind}(F) = [\mathcal{O}_L : \mathbb{Z}[\alpha]]$$

of the ring of integers $\mathcal{O}_L$ of L, given by the formula

$$\mathrm{Disc}(L) \cdot \mathrm{Ind}(F)^2 = \mathrm{Disc}(F).$$

Decomposing $p\mathbb{Z}[\alpha]$ into primary ideals is an easy task, and a theorem of Kummer says that, if p is a prime not dividing $\mathrm{Ind}(F)$, then the factorization of $p\mathcal{O}_L$ can be derived directly from the decomposition of $p\mathbb{Z}[\alpha]$. Also, Dedekind's criterion allows us to test whether or not p divides $\mathrm{Ind}(F)$ and to enlarge $\mathbb{Z}[\alpha]$ when it does. Of course, the best possible situation occurs when $\mathcal{O}_L$ is *monogenic* (i.e., there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathbb{Z}[\alpha]$) or, at least, when the *index* of the field K (i.e., the greatest common divisor of $\mathrm{Ind}(F)$ when F runs over all minimal polynomials of integral generators of L) is equal to 1. Unfortunately, this is not always the case, but one can decide whether p divides the index of L in terms of the factorization type of $p\mathcal{O}_L$ (see for instance [5, Ch. 4, Theorem 4.13]).

In this paper we deal with problems of similar type in the more general case of an irreducible polynomial F which is primitive without being necessarily monic, and replacing $\mathbb{Z}$ and $\mathbb{Q}$ by any Dedekind ring R and its quotient field K. In this situation D. Simon [6] constructed an order R_F of $\mathcal{O}_L$ which generalizes the order $R[\alpha]$ when F is monic (it turns out that

$$R_F = R[\alpha] \cap R[\alpha^{-1}],$$

as shown in Proposition 2 below), and that continues to satisfy the index rule

$$\mathrm{Disc}(L) \cdot [\mathcal{O}_L : R_F]^2 = \mathrm{Disc}(F).$$

2000 *Mathematics Subject Classification*: Primary 11R04.

We show that, even in the case when F is not monic, the classical invariants of R_F can be derived from the polynomial F, precisely as in the case of monogenic orders.

More specifically, in Section 3 we give the explicit primary decomposition of the ideals pR_F, where p is a prime ideal of R (Theorem 1). In Section 4 we generalize the Dedekind criterion for p-maximality to the ring R_F (Theorem 2). In Section 5 we generalize Kummer's theorem to the case when p does not divide the index of R_F in $\mathcal{O}_L$ (Theorem 3).

As an application, we introduce a generalized index for L, namely the greatest common divisors of the indexes $[\mathcal{O}_L : R_F]$ where F runs over all primitive irreducible polynomials such that L is generated over K by a root of F, and we show how to decide whether a prime p divides this generalized index in terms of the factorization type of $p\mathcal{O}_L$ (Proposition 10). On the one hand, it turns out that this generalized index does not give theoretical advantages over the classical index, except for one particular case (see Remark 3). On the other hand, our results show that the same kind of information that one obtains from an integral generator can also be obtained from a non-integral one, thereby giving some computational advantage.

2. Notation and basic properties. Let R be a Dedekind ring and K be its field of fractions. Let $F(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ be a primitive irreducible polynomial with coefficients in R such that $a_0 \neq 0$. We also denote by F the homogenized polynomial $F(x, y) = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n$. Define

$$\begin{aligned} T_0 &= a_0, \\ T_1 &= a_0x + a_1, \\ &\cdots \\ T_{n-1} &= a_0x^{n-1} + \cdots + a_{n-1}. \end{aligned}$$

Let L be the field $K[x]/(F(x))$. We denote by α the image of x under this projection (α is a root of F). We consider

$$R_F = R \oplus T_1(\alpha)R \oplus \cdots \oplus T_{n-1}(\alpha)R.$$

This R-module is an order in L (see [6]). In particular, it is contained in the maximal order $\mathcal{O}_L$ of L.

Let $\mathfrak{B} = T_0R_F + T_1(\alpha)R_F + \cdots + T_{n-1}(\alpha)R_F$. This is an invertible ideal of R_F (see [7]), in fact $\mathfrak{B} = T_0R \oplus T_1(\alpha)R \oplus \cdots \oplus T_{n-1}(\alpha)R$. Similarly, let $\mathfrak{A} = \alpha\mathfrak{B} = \alpha T_0R_F + \alpha T_1(\alpha)R_F + \cdots + \alpha T_{n-1}(\alpha)R_F$. We have $\mathfrak{A} = \alpha T_0R \oplus \alpha T_1(\alpha)R \oplus \cdots \oplus \alpha T_{n-1}(\alpha)R$. In [7] it was proved that $\mathfrak{A} + \mathfrak{B} = R_F$. From this we get $(\alpha) = \mathfrak{A}\mathfrak{B}^{-1}$ and therefore $\mathfrak{A}$ and $\mathfrak{B}$ are the numerator and the denominator of α.

Since R is a Dedekind domain and F is primitive, the following proposition holds (see for instance [4, Cor. 28.4]):

PROPOSITION 1. *F divides a polynomial $U \in R[x]$ in $K[x]$ if and only if F divides U in $R[x]$.*

It follows, in particular, that $R[x]/(F(x)) \cong R[\alpha]$. Moreover, we have the following characterization of R_F:

PROPOSITION 2. *$R_F = R[\alpha] \cap R[\alpha^{-1}]$.*

Proof. We have $T_i(\alpha) = a_0\alpha^i + \cdots + a_i = -(a_{i+1}\alpha^{-1} + \cdots + a_n\alpha^{i-n})$, so the inclusion $\subseteq$ is clear. To prove the converse inclusion, let $P, Q \in R[x]$ be such that $P(\alpha) = Q(\alpha^{-1})$, and let $m = \deg P$.

Let $P = c_0x^m + \cdots + c_m$. We first prove that, if $m > 0$, then $a_0 \mid c_0$. In fact, letting $Q^*(x) = x^{\deg Q}Q(1/x)$, we see that the integer polynomial $U = x^{\deg Q}P - Q^*$ vanishes at α, and therefore F divides U in $K[x]$; by Proposition 1, F divides U also in $R[x]$, whence $a_0 \mid c_0$.

We prove that $P \in R_F$ by induction on m. If $m = 0$, the inclusion is trivial. For $m > 0$, let $c_0 = a_0b_0$. If $m \le n-1$, then $P(\alpha) - b_0T_m(\alpha) \in R[\alpha] \cap R[\alpha^{-1}]$ and $P - b_0T_m$ has degree $< m$, so the inclusion follows by the induction hypothesis. Similarly, if $m \ge n$, then $P(\alpha) = P(\alpha) - b_0\alpha^{m-n}F(\alpha)$ and $P - b_0x^{m-n}F$ has degree $< m$, so the inclusion follows again. ∎

PROPOSITION 3. *For $d \ge 0$, let $R_d[x, y]$ denote the R-module of homogeneous polynomials of degree d with coefficients in R. Then*

$$\mathfrak{B}^d\{b(\alpha, 1) \mid b \in R_d[x, y]\} = R_F.$$

Proof. The inclusion $\subseteq$ is clear since $\mathfrak{B}\alpha = \mathfrak{A} \subset R_F$. For the converse it is enough to observe that choosing $b = x^d$ and $b = y^d$ we find that $\mathfrak{A}^d$ and $\mathfrak{B}^d$ are in this product. Since $\mathfrak{A}$ and $\mathfrak{B}$ are coprime, we have the conclusion. ∎

REMARK 1. Given an algebraic number α over K of degree n, it is not always possible to find an irreducible primitive polynomial of degree n and with coefficients in R which has α as a root. However, if R is a principal ideal domain, it is straightforward to see that such a polynomial exists, and one can always reduce to this case by localizing R at a prime ideal. When R is not principal, and no irreducible primitive polynomial of degree n exists, one can also use the generalized definitions of R_F, $\mathfrak{A}$ and $\mathfrak{B}$ given by D. Simon in [7], and we suspect that, with these definitions, almost all the results of the present paper remain valid.

EXAMPLE 1. Let $R = \mathbb{Q}[\sqrt{10}]$ and let α be a root of $x^2 + \sqrt{10}/2$. The factorizations in R of the ideals (2) and $(\sqrt{10})$ are $(2) = \mathfrak{p}^2$ and $(\sqrt{10}) = \mathfrak{pq}$, where $\mathfrak{p} = (2, \sqrt{10})$ and $\mathfrak{q} = (5, \sqrt{10})$ are not principal. Any quadratic polynomial $F \in R[x]$ vanishing at α has the form $F = cx^2 + c\sqrt{10}/2$,

with $(c) = \mathfrak{p}I$ where I is a proper ideal such that $\mathfrak{p}I$ is principal. The ideal generated by the coefficients of F must therefore be exactly $(\mathfrak{p}I, \mathfrak{q}I) = I \neq 1$.

PROPOSITION 4. $\operatorname{disc} R_F = \operatorname{disc} F$.

Proof. We have

$$\begin{pmatrix} 1 \\ T_1(\alpha) \\ \cdots \\ T_{n-1}(\alpha) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ * & a_0 & 0 & 0 \\ * & * & \cdots & 0 \\ * & * & * & a_0 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \cdots \\ \alpha^{n-1} \end{pmatrix},$$

hence, letting $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in some algebraic closure $\overline{K}$ of K,

$$\begin{aligned} \operatorname{disc} R_F &= \operatorname{disc}\{1, T_1(\alpha), \ldots, T_{n-1}(\alpha)\} = a_0^{2n-2} \operatorname{disc}\{1, \alpha, \ldots, \alpha^{n-1}\} \\ &= a_0^{2n-2} \prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha)) = \operatorname{disc} F. \ \blacksquare \end{aligned}$$

3. The primary decomposition of prime ideals. Let p be a prime ideal of R (the interesting case is when p divides a_0). We use the notation $x \mapsto \overline{x}$ for the reduction modulo p. Let

$$\overline{F}(x, y) = \prod_i \overline{F}_i(x, y)^{e_i}$$

be the factorization into irreducible factors of $F(x, y)$ modulo p. Let f_i be the degree of $\overline{F}_i$. Fix a choice $F_i(x, y)$ for a lift of $\overline{F}_i(x, y)$ in $R[x, y]$, homogeneous of degree f_i. Define

$$\mathfrak{p}_i = pR_F + \mathfrak{B}^{f_i} F_i(\alpha, 1).$$

It is easily seen that $\mathfrak{p}_i$ does not change if we multiply $\overline{F}_i$ by a unit in R/p, and is independent of the choice of the lift F_i. By Proposition 3, $\mathfrak{p}_i$ is an integral ideal of R_F. We now define

$$\mathfrak{q}_i = pR_F + \mathfrak{B}^{e_i f_i} F_i^{e_i}(\alpha, 1).$$

LEMMA 1. • *If* $\overline{F}_i \neq uy$ (*with* $u \in (R/p)^*$) *then* $\mathfrak{p}_i + \mathfrak{B} = R_F = \mathfrak{q}_i + \mathfrak{B}$.
• *If* $\overline{F}_i = uy$ *then* $\mathfrak{B} \subset \mathfrak{p}_i$.
• *If* $\overline{F}_i \neq ux$ *then* $\mathfrak{p}_i + \mathfrak{A} = R_F = \mathfrak{q}_i + \mathfrak{A}$.
• *If* $\overline{F}_i = ux$ *then* $\mathfrak{A} \subset \mathfrak{p}_i$.

Proof. Assume first that $\overline{F}_i \neq uy$ (with $u \in (R/p)^*$). Let c be the coefficient of F_i corresponding to x^{f_i}. We can assume without loss of generality that $c = 1$. We have

$$\mathfrak{p}_i + \mathfrak{B} = pR_F + \mathfrak{B}^{f_i} F_i(\alpha, 1) + \mathfrak{B} = pR_F + \mathfrak{A}^{f_i} + \mathfrak{B} = pR_F + R_F = R_F.$$

Assume now that $\overline{F}_i = uy$ (with $u \in (R/p)^*$). We can still assume that $F_i = y$. Hence $\mathfrak{p}_i = pR_F + \mathfrak{B} \supset \mathfrak{B}$. The proof for the remaining cases is similar. ∎

PROPOSITION 5. *Let $I = pR_F + \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha, 1)$ with $1 \le b_i \le e_i$. The quotient ring R_F/I is isomorphic to $(R/p)[x]/\overline{F}_i^{b_i}(x, 1)$ when $\overline{F}_i \ne uy$ with u a unit in R/p, and is isomorphic to $(R/p)[y]/y^{b_i}$ otherwise. The norm of the ideal I is $\mathcal{N}_{R_F/R}(I) = p^{b_i f_i}$. In particular, the $\mathfrak{p}_i$ are prime ideals, the $\mathfrak{q}_i$ are $\mathfrak{p}_i$-primary and their norms are given by $\mathcal{N}_{R_F/R}(\mathfrak{p}_i) = p^{f_i}$, $\mathcal{N}_{R_F/R}(\mathfrak{q}_i) = p^{e_i f_i}$.*

Proof. We consider first the case $\overline{F}_i \ne uy$. We have $I \supset \mathfrak{q}_i$. But, by Lemma 1, $\mathfrak{q}_i + \mathfrak{B} = R_F$, hence $I + \mathfrak{B} = R_F$. Consider the ring homomorphism

$$\phi : R_F \to (R/p)[x]/(\overline{F}_i^{b_i}(x, 1))$$

defined by $\phi(g(\alpha)) = \overline{g}(x)$. Since $R_F \subset R[\alpha] \cong R[x]/(F(x))$ and $\overline{F}_i^{b_i}$ divides $\overline{F}$, this map is well defined. As for its kernel, it is clear that $I \subset \ker \phi$. Conversely, let $g \in R[x]$ be such that $g(\alpha) \in \ker \phi$. We thus have $g(x) = F_i^{b_i}(x, 1)q(x) + r(x)$ in $R[x]$ with $q(x) \in R[x]$ and $r(x) \in p[x]$. Multiplying by $\mathfrak{B}^{\deg g}$ and evaluating at α, we get

$$\mathfrak{B}^{\deg g} g(\alpha) = \mathfrak{B}^{f_i b_i} F_i^{b_i}(\alpha, 1) \cdot \mathfrak{B}^{\deg g - f_i b_i} q(\alpha) + \mathfrak{B}^{\deg g} r(\alpha),$$

which is a relation between ideals of R_F. It follows that $\mathfrak{B}^{\deg g} g(\alpha) \subset I$ and, since obviously $I g(\alpha) \subset I$ and $\mathfrak{B}^{\deg g} + I = R_F$, we obtain $g(\alpha) \in I$. We have therefore proved that $\ker \phi = I$. To prove surjectivity, let $\gamma \in I$ and $\beta \in \mathfrak{B}$ be such that $\gamma + \beta = 1$. We have $\phi(\beta) = 1$ and $\phi(\alpha\beta) = \overline{x}$, which implies that ϕ is onto. The other claims for the case $\overline{F}_i \ne uy$ are now immediate.

Consider now the case $\overline{F}_i = uy$, where u is a unit in R/p. We can assume that $u = 1$. Let G be the reciprocal polynomial of F. We know from Proposition 2 that $R_F = R_G$. It is then possible to work with G instead of F. The factor $F_i = y$ of F modulo p corresponds to the factor $G_i = x$ of G. We can apply the results of the first case to G, and the proposition is proved in all cases. ∎

THEOREM 1. *The decomposition of pR_F into primary ideals is given by*

$$pR_F = \bigcap_i \mathfrak{q}_i = \prod_i \mathfrak{q}_i$$

where $\mathfrak{q}_i = pR_F + \mathfrak{B}^{e_i f_i} F_i^{e_i}(\alpha, 1)$.

Proof. By Proposition 5 we know that the ideals $\mathfrak{q}_i$ are $\mathfrak{p}_i$-primary and therefore pairwise coprime, hence $\bigcap \mathfrak{q}_i = \prod \mathfrak{q}_i = \prod (pR_F + \mathfrak{B}^{e_i f_i} F_i^{e_i}(\alpha, 1))$

$\subset pR_F + \mathfrak{B}^{\sum e_i f_i} \prod F_i^{e_i}(\alpha,1)$. Since $\sum e_i f_i = n$, we have $pR_F \subset pR_F + \mathfrak{B}^n \prod F_i^{e_i}(\alpha,1)$. From the definition of the F_i we deduce that $\prod F_i^{e_i}(x,y) - F(x,y) \in pR[x,y]$. Since $F(\alpha,1)=0$, by Proposition 3 we get $\mathfrak{B}^n \prod F_i^{e_i}(\alpha,1) \subset pR_F$, and hence $pR_F = \prod \mathfrak{q}_i$. ∎

COROLLARY 1. *The ideals $\mathfrak{q}_i$ are invertible. For each i, the ideal $\mathfrak{p}_i$ is invertible if and only if $\mathfrak{p}_i^{e_i} = \mathfrak{q}_i$.*

Proof. Since p is invertible, Theorem 1 says immediately that the $\mathfrak{q}_i$ are invertible.

The identity $\mathfrak{p}_i^{e_i} = \mathfrak{q}_i$ implies that $\mathfrak{p}_i$ is also invertible. Assume now that $\mathfrak{p}_i$ is invertible. In this case $\mathcal{N}_{R_F/R}(\mathfrak{p}_i^{e_i}) = \mathcal{N}_{R_F/R}(\mathfrak{p}_i)^{e_i}$ and, by Proposition 5, $\mathcal{N}_{R_F/R}(\mathfrak{p}_i)^{e_i} = p^{e_i f_i} = \mathcal{N}_{R_F/R}(\mathfrak{q}_i)$. But $\mathfrak{p}_i^{e_i} \subset \mathfrak{q}_i$, hence $\mathfrak{p}_i^{e_i} = \mathfrak{q}_i$. ∎

We can now classify the ideals containing pR_F and their inclusion relations.

PROPOSITION 6. *The ideals of R_F containing pR_F are in one-to-one correspondence with the divisors of $\overline{F}$, where, if $\overline{P} \mid \overline{F}$, the corresponding ideal is $pR_F + \mathfrak{B}^{\deg P} P(\alpha,1)$ for any homogeneous lift P of $\overline{P}$.*

If $I_1 = pR_F + \mathfrak{B}^{d_1} P_1(\alpha,1)$ and $I_2 = pR_F + \mathfrak{B}^{d_2} P_2(\alpha,1)$ where $\overline{P}_1 \mid \overline{F}$ and $\overline{P}_2 \mid \overline{F}$, then:

(i) $I_1 \subset I_2 \Leftrightarrow \overline{P}_2 \mid \overline{P}_1$;

(ii) $I_1 + I_2 = pR_F + \mathfrak{B}^{\deg D} D(\alpha,1)$, *where D is any homogeneous lift of the greatest common divisor $\overline{D}$ of $\overline{P}_1$ and $\overline{P}_2$*;

(iii) $I_1 \cap I_2 = pR_F + \mathfrak{B}^{\deg M} M(\alpha,1)$, *where M is any homogeneous lift of the least common multiple $\overline{M}$ of $\overline{P}_1$ and $\overline{P}_2$.*

Proof. Via projection, the ideals of R_F containing pR_F are in one-to-one correspondence with the ideals of $R_F/pR_F \cong \prod_i R_F/\mathfrak{q}_i$. The ideals of the last ring are products of ideals of $R_F/\mathfrak{q}_i$ and, since projection preserves products of ideals, each ideal I containing pR_F must be of the form $\prod_i \mathfrak{q}_i'$, where $\mathfrak{q}_i' \supset \mathfrak{q}_i$ for all i.

By Proposition 5, the ideals $\mathfrak{q}_i'$ containing $\mathfrak{q}_i$ are of the form $\mathfrak{q}_i' = pR_F + \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha,1)$ with $0 \le b_i \le e_i$. Now, we clearly have $\prod_i (pR_F + \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha,1)) \subset pR_F + \prod_i \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha,1)$. On the other hand,

$$\prod_i \mathfrak{q}_i' = \prod_i (pR_F + \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha,1))$$
$$\supset pR_F\Big(\sum_i \prod_{j\neq i} \mathfrak{q}_j'\Big) + \prod_i \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha,1) = pR_F + \prod_i \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha,1).$$

Hence the ideals I containing pR_F are exactly those of the form $I = pR_F + \prod_i \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha,1)$ and, since the products $\prod_i \overline{F}_i^{b_i}$ represent all divisors of $\overline{F}$, the first statement of the proposition follows.

(i) Let $I_1 = \prod_i \mathfrak{q}'_{i,1} = \prod_i (pR_F + \mathfrak{B}^{b_{i,1}f_i} F_i^{b_{i,1}}(\alpha,1))$ and $I_2 = \prod_i \mathfrak{q}'_{i,2} = \prod_i (pR_F + \mathfrak{B}^{b_{i,2}f_i} F_i^{b_{i,2}}(\alpha,1))$. We have $I_1 \subset I_2$ if and only if $\mathfrak{q}'_{i,1} \subset \mathfrak{q}'_{i,2}$ for all i, as can be seen by localizing at $\mathfrak{q}_i$; by Proposition 5, this is true if and only if $b_{i,2} \le b_{i,1}$ for all i.

(ii) and (iii) are easy consequences of (i), since $I_1 + I_2$ is the smallest ideal containing I_1 and I_2 and $I_1 \cap I_2$ is the greatest ideal contained in I_1 and I_2. ∎

The following elementary proposition appears to be quite useful when we deal with ideals dividing pR_F in the next section.

PROPOSITION 7. *Let $P \in R[x,y]$ be any homogeneous polynomial and let $I = pR_F + \mathfrak{B}^{\deg P} P(\alpha,1)$.*

(i) *The ideal I can be written canonically as $I = pR_F + \mathfrak{B}^{\deg P_0} P_0(\alpha,1)$, where P_0 is any homogeneous polynomial satisfying $(\overline{P},\overline{F}) = \overline{P}_0$.*

(ii) *Let $0 \le b_i \le e_i$. We have $pR_F + \mathfrak{B}^{b_i f_i} F_i^{b_i}(\alpha,1) \mid pR_F + \mathfrak{B}^{\deg P} P(\alpha,1)$ if and only if $\overline{F}_i^{b_i} \mid \overline{P}$.*

Proof. (i) Let $I = \prod_i \mathfrak{q}'_i$, where $\mathfrak{q}'_i \supset \mathfrak{q}_i$. Consider the projection $R_F \to R_F/\mathfrak{q}_i$. Since $R_F/\mathfrak{q}_i \cong (R/p)[x]/(\overline{F}_i^{e_i}(x,1))$ or $R_F/\mathfrak{q}_i \cong (R/p)[y]/(y^{e_i})$ (see Proposition 5), the ideal I corresponds to $(\overline{P}(x,1))/(\overline{F}_i^{e_i}(x,1))$ or to $(\overline{P}(1,y))/(y^{e_i})$. Now, $(\overline{P}(x,1))/(\overline{F}_i^{e_i}(x,1)) = (\overline{P}(x,1),\overline{F}_i^{e_i}(x,1))/(\overline{F}_i^{e_i}(x,1))$ and $(\overline{P}(1,y))/(y^{e_i}) = (\overline{P}(1,y),y^{e_i})/(y^{e_i})$, whence the result follows.

(ii) is an immediate consequence of (i) and Proposition 6. ∎

Now, we give a proposition and its corollary which will not be needed in the rest of this paper, but which give a very practical way to find generators for the ideals containing pR_F.

PROPOSITION 8. *Let $\mathfrak{D}, I$ be integral ideals of R_F, with $\mathfrak{D}$ invertible. Then there exists an integral ideal $\mathfrak{C}$ of R_F in the same ideal class of $\mathfrak{D}$ such that $\mathfrak{C} + I = 1$. In particular, there exists an integral ideal $\mathfrak{C}$ of R_F such that $\mathfrak{C}\mathfrak{B} = (\beta)$ is principal and $\mathfrak{C} + pR_F = 1$.*

Proof. We have $\mathfrak{C} + I = 1$ if and only if $\mathfrak{C} + \sqrt{I} = 1$. Write $\sqrt{I} = \bigcap_i \mathfrak{r}_i = \prod_i \mathfrak{r}_i$, where $\mathfrak{r}_i$ are distinct prime ideals of R_F. It follows that $\mathfrak{C}$ is coprime to I if and only if it is coprime to each of the $\mathfrak{r}_i$. Since $\mathfrak{D}\mathfrak{D}^{-1} = 1$, we can find, for each i, an element $x_i \in \mathfrak{D}^{-1}$ such that $x_i\mathfrak{D} \not\subset \mathfrak{r}_i$. Now, since the $\mathfrak{r}_i$ are prime, $\mathfrak{r}_i \not\supset \bigcap_{j\ne i} \mathfrak{r}_j$, and hence there exist elements $y_i \notin \mathfrak{r}_i$, $y_i \in \bigcap_{j\ne i} \mathfrak{r}_j$. Letting $z_i = x_i y_i$, we have $z_i\mathfrak{D} \not\subset \mathfrak{r}_i$ and $z_i\mathfrak{D} \subset \bigcap_{j\ne i} \mathfrak{r}_j$. Finally, $z = \sum z_i$ is an element of $\mathfrak{D}^{-1}$ such that $z\mathfrak{D}$ is coprime to $\mathfrak{r}_i$ for all i. ∎

COROLLARY 2. *Let $\beta \in \mathfrak{B}$ be such that $(\beta) = \mathfrak{C}\mathfrak{B}$ where $\mathfrak{C}$ is an ideal of R_F with $\mathfrak{C} + pR_F = 1$. Then β and $\alpha\beta$ are in R_F and $pR_F + \mathfrak{B}^{\deg P} P(\alpha,1) = (p, P(\alpha\beta,\beta))$.*

Proof. By definition of $\mathfrak{B}$, β and $\alpha\beta$ are in R_F. For each ideal I and each non-negative integer m, we have $pR_F + I = pR_F + (p + \mathfrak{C}^m)I \subset pR_F + \mathfrak{C}^m I \subset pR_F + I$, and therefore $pR_F + I = pR_F + \mathfrak{C}^m I$. It follows that $pR_F + \mathfrak{B}^{\deg P} P(\alpha, 1) = pR_F + \mathfrak{C}^{\deg P}\mathfrak{B}^{\deg P} P(\alpha, 1) = (p, P(\alpha\beta, \beta))$. ∎

4. The Dedekind criterion. Now we generalize [3, Ch. 2.4], to be able to decide whether the order R_F is p-maximal or not, and to enlarge it when it is not. The main result is the generalization of the Dedekind criterion. For this, we need some definitions.

Let $\mathcal{O} \subset \mathcal{O}_L$ be an order in L. Then $\mathcal{O}_L/\mathcal{O}$ is a finitely generated torsion R-module. By [3, Thm 1.2.30], there exist unique integral ideals $\mathfrak{d}_1, \dots, \mathfrak{d}_r$, with $0 \neq \mathfrak{d}_1 \subset \mathfrak{d}_2 \subset \cdots \subset \mathfrak{d}_r \neq R$, such that

$$\mathcal{O}_L/\mathcal{O} \cong (R/\mathfrak{d}_1) \oplus \cdots \oplus (R/\mathfrak{d}_r).$$

The *index-ideal* $[\mathcal{O}_L : \mathcal{O}]$ is by definition the product of the ideals $\mathfrak{d}_i$. When the base ring R is $\mathbb{Z}$, this definition coincides with the usual index if we identify an ideal of $\mathbb{Z}$ with its positive generator.

We say that an order $\mathcal{O}$ in L is *p-maximal* if the index-ideal $[\mathcal{O}_L : \mathcal{O}]$ is not divisible by p.

The *p-radical* I_p of $\mathcal{O}$ at p is defined as the radical of the ideal p, that is,

$$I_p = \sqrt{p\mathcal{O}} = \{x \in \mathcal{O} \mid \exists m \geq 1 \text{ such that } x^m \in p\mathcal{O}\}.$$

The p-radical is a useful tool for enlarging an order $\mathcal{O}$ when it is not p-maximal, as we can see in Zassenhaus's theorem (see [3, Prop. 2.4.4]):

PROPOSITION 9 (Zassenhaus's theorem). *Set* $\mathcal{O}' = \{x \in L \mid xI_p \subset I_p\}$. *Then*

(i) $\mathcal{O}'$ *is an order in* L *containing* $\mathcal{O}$,
(ii) $\mathcal{O}' = \mathcal{O}$ *if and only if* $\mathcal{O}$ *is* p*-maximal*,
(iii) *if* $\mathcal{O}' \neq \mathcal{O}$, *then* $[\mathcal{O}' : \mathcal{O}] = p^k$ *with* $1 \leq k \leq n$.

THEOREM 2 (Dedekind criterion). *Let* $h = \sum_i f_i$ *be the degree of* $H_1 = \prod_i F_i$.

(i) *The* p*-radical of* R_F *at* p *is given by*

$$I_p = pR_F + \mathfrak{B}^h H_1(\alpha, 1).$$

(ii) *Let* $\xi \in p^{-1} \setminus R$ (*i.e. a uniformizer of* p^{-1}), H_2 *be a lift of* $\overline{F}/\overline{H}_1$ *and* $H_3 = \xi(H_1H_2 - F) \in R[x, y]$. *Let also* $\overline{G}$ *be the gcd of* $\overline{H}_1$, $\overline{H}_2$ *and* $\overline{H}_3$ *in* $R/p[x, y]$, *and* $g = \deg \overline{G}$. *Finally, let* U *be a lift of* $\overline{F}/\overline{G}$ *in* $R[x, y]$ *of degree* $n - g$. *Then the order given by Zassenhaus's theorem starting with* $\mathcal{O} = R_F$ *is equal to*

$$\mathcal{O}' = R_F + p^{-1}\mathfrak{B}^{n-g}U(\alpha, 1).$$

We have $[\mathcal{O}' : R_F] = p^g$. *In particular*, R_F *is p-maximal if and only if* $(\overline{H}_1, \overline{H}_2, \overline{H}_3) = 1$.

Proof. (i) This statement is a consequence of Proposition 6 and of the equality $I_p = \sqrt{pR_F} = \sqrt{\bigcap_i \mathfrak{q}_i} = \bigcap_i \sqrt{\mathfrak{q}_i} = \bigcap_i \mathfrak{p}_i$.

(ii) Clearly $p\mathcal{O}'$ is an ideal of R_F containing pR_F, and by Proposition 6 we may write $p\mathcal{O}' = pR_F + \mathfrak{B}^{\deg P}P(\alpha, 1)$ for some homogeneous polynomial P such that $\overline{P}$ is a divisor of $\overline{F}$. Since pR_F is invertible, we have to prove that we can choose P such that $\overline{P} = \overline{U}$.

From now on we shall follow closely the lines of the proof of [2, Theorem 6.1.4]. The ideal $p\mathcal{O}'$ is characterized as the set of elements γ such that $\gamma \in I_p$ and $\gamma\mathfrak{B}^h H_1(\alpha, 1) \subset pI_p$. We first remark that Proposition 6 and part (i) of this theorem give immediately $pR_F + \mathfrak{B}^{\deg P}P(\alpha, 1) \subset I_p$ if and only if $\overline{H}_1 \mid \overline{P}$. Hence, the polynomial $\overline{P}$ is characterized as the smallest one such that $\overline{H}_1 \mid \overline{P} \mid \overline{F}$ and

$$\mathfrak{B}^h H_1(\alpha, 1)(pR_F + \mathfrak{B}^{\deg P}P(\alpha, 1)) \subset pI_p. \tag{1}$$

But $\mathfrak{B}^h H_1(\alpha, 1)pR_F \subset p^2R_F + \mathfrak{B}^h H_1(\alpha, 1)pR_F = pI_p$, hence (1) is equivalent to

$$\mathfrak{B}^{h+\deg P}H_1(\alpha, 1)P(\alpha, 1) \subset pI_p. \tag{2}$$

We note that (2) implies that

$$\mathfrak{B}^{h+\deg P}H_1(\alpha, 1)P(\alpha, 1) \subset pR_F,$$

and by Proposition 7 we get $\overline{F} \mid \overline{H}_1\overline{P}$, that is, $\overline{H}_2 \mid \overline{P}$. Let $P = A_3H_2 + B_1$, where A_3 and B_1 are homogeneous polynomials respectively in $R[x, y]$ and $p[x, y]$. Now, we have $H_1P = H_1H_2A_3 + H_1B_1 = (H_1H_2 - F)A_3 + H_1B_1 + FA_3$, and (2) is equivalent to

$$\mathfrak{B}^{h+\deg P}((H_1H_2 - F)A_3 + H_1B_1)(\alpha, 1) \subset pI_p,$$

or after multiplication by ξ to

$$\mathfrak{B}^{h+\deg P}(H_3A_3 + H_1\xi B_1)(\alpha, 1) \subset I_p. \tag{3}$$

We use again the fact that $I_p = pR_F + \mathfrak{B}^h H_1(\alpha, 1)$, which implies that $\mathfrak{B}^{h+\deg P}(H_1\xi B_1)(\alpha, 1) \subset \mathfrak{B}^h H_1(\alpha, 1) \subset I_p$, and (3) is now equivalent to

$$\mathfrak{B}^{h+\deg P}(H_3A_3)(\alpha, 1) \subset pR_F + \mathfrak{B}^h H_1(\alpha, 1). \tag{4}$$

By Proposition 7, this is equivalent to $\overline{H}_1 \mid \overline{H}_3\overline{A}_3$, or simply to $\overline{H}_4 \mid \overline{A}_3$ where $\overline{H}_4 = \overline{H}_1/(\overline{H}_1, \overline{H}_3)$. Putting together the different conditions, we see that (1) is equivalent to $\overline{H}_4\overline{H}_2 \mid \overline{P}$.

Summarizing, the two conditions on $\overline{P}$ mean that $\overline{P}$ is the least common multiple of $\overline{H}_1$ and $\overline{H}_4\overline{H}_2$. Now,

$$\begin{aligned}\operatorname{lcm}(\overline{H}_1, \overline{H}_4\overline{H}_2) &= \overline{H}_4 \operatorname{lcm}((\overline{H}_1, \overline{H}_3), \overline{H}_2) \\ &= \frac{\overline{H}_1}{(\overline{H}_1, \overline{H}_3)} \frac{(\overline{H}_1, \overline{H}_3)\overline{H}_2}{(\overline{H}_1, \overline{H}_2, \overline{H}_3)} = \frac{\overline{F}}{(\overline{H}_1, \overline{H}_2, \overline{H}_3)} = \overline{U}. \ \blacksquare\end{aligned}$$

5. The case when p is coprime to the index. Let $\operatorname{Ind}(R_F) = [\mathcal{O}_L : R_F]$ be the index-ideal of R_F in $\mathcal{O}_L$ as described in Section 4.

THEOREM 3. *If p is coprime to* $\operatorname{Ind}(R_F)$, *the factorization of pR_F into prime ideals is given by*

$$pR_F = \prod_i \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_i = pR_F + \mathfrak{B}^{f_i} F_i(\alpha, 1)$. *Moreover*,

$$p\mathcal{O}_L = \prod_i (\mathfrak{p}_i \mathcal{O}_L)^{e_i}$$

and $\mathcal{N}_{\mathcal{O}_L/R}(\mathfrak{p}_i) = p^{f_i}$.

Proof. Setting $S = R \setminus p$ we have $(S^{-1}R)_F = S^{-1}R_F = S^{-1}\mathcal{O}_L$, and therefore $S^{-1}R_F$ is a Dedekind domain. The decomposition of $S^{-1}p$ in $S^{-1}R_F$ is $S^{-1}p = \bigcap S^{-1}\mathfrak{q}_i$, where the prime ideals $S^{-1}\mathfrak{p}_i$ are invertible and the $S^{-1}\mathfrak{q}_i$ are $S^{-1}\mathfrak{p}_i$-primary. By Corollary 1 we see that $S^{-1}\mathfrak{q}_i = S^{-1}\mathfrak{p}_i^{e_i}$ and, contracting these ideals to R_F and to $\mathcal{O}_L$, we obtain $\mathfrak{q}_i = \mathfrak{p}_i^{e_i}$ and $\mathfrak{q}_i\mathcal{O}_L = (\mathfrak{p}_i\mathcal{O}_L)^{e_i}$ (see for instance [1, Proposition 4.8]). The factorizations of pR_F and $p\mathcal{O}_L$ now follow from Theorem 1.

Finally, $R_F/\mathfrak{p}_i \cong \mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L$ and the last statement follows from Proposition 5. ∎

6. Applications. In this section, we consider the standard case $K = \mathbb{Q}$ and $R = \mathbb{Z}$, and we write $\mathbb{Z}_F$ for the ring R_F.

DEFINITION 1. The *generalized index* of a number field L is the greatest common divisor of the indices $[\mathcal{O}_L : \mathbb{Z}_F]$ where F is the primitive irreducible minimal polynomial of α, and α runs over all generators of L over $\mathbb{Q}$.

The usual definition of the index of L is the same, except that α is restricted to algebraic integers. It is not difficult to see that the generalized index of L is a divisor of the index of L. The following proposition is the analogue of [5, Ch. 4, Theorem 4.13].

PROPOSITION 10. *Let L be a number field, p be a rational prime and let*

$$p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$$

be the factorization of $p\mathcal{O}_L$ into prime ideals. Let also f_i be the inertial degree of $\mathfrak{p}_i$ for $i = 1, \dots, t$. Then p does not divide the generalized index of L if and only if there exist distinct irreducible homogeneous polynomials $\overline{F}_1, \dots, \overline{F}_t \in \mathbb{F}_p[x, y]$ with degrees $f_1, \dots, f_t$, respectively.

REMARK 2. To say that the polynomials $\overline{F}_i$ and $\overline{F}_j$ are distinct means in this context that there is no unit $u \in \mathbb{F}_p^*$ such that $\overline{F}_i = u\overline{F}_j$.

Proof of Proposition 10. If p does not divide the generalized index of L, then there exists a generator $\alpha \in L$ such that $p \nmid [\mathcal{O}_L : \mathbb{Z}_{F_\alpha}]$ (where $F_\alpha \in \mathbb{Z}[x]$ is a primitive irreducible polynomial having α as a root). Denote again by F_α the homogenized polynomial of F_α with the same degree; by Theorem 3, the factors of F_α modulo p are homogeneous polynomials with the required properties.

To prove the converse, let $F_1, \dots, F_t$ be homogeneous lifts of $\overline{F}_1, \dots, \overline{F}_t$ to $\mathbb{Z}[x, y]$.

If none of the $\overline{F}_i$ is equal to y (up to some invertible element modulo p), then we can apply to $\overline{F}_i(x, 1)$ the standard result, for example [5, Ch. 4, Theorem 4.13]. In this case, we find that p does not divide the index of L, and therefore it cannot divide the generalized index of L either.

Assume now that $\overline{F}_{i_0} = y$ for some index i_0. Let β be an element of $\mathcal{O}_L$ such that $\beta \in \mathfrak{p}_{i_0}$, $\beta \notin \mathfrak{p}_{i_0}^2$ and $\beta \equiv 1 \pmod{\mathfrak{p}_i^2}$ for $i \neq i_0$. For $i = 1, \dots, t$, $i \neq i_0$, let γ_i be an element of $\mathcal{O}_L$ such that $\gamma_i \notin \mathfrak{p}_{i_0}$ and

$$F_i(\gamma_i, 1) \equiv 0 \pmod{\mathfrak{p}_i}.$$

Such a root of $\overline{F}_i$ does exist since the degree of $\overline{F}_i$ is equal to the inertial degree of $\mathfrak{p}_i$. Furthermore, the polynomial $\overline{F}_i$ is irreducible modulo p, and its discriminant is coprime to p, hence to $\mathfrak{p}_i$, so $\overline{F}_i'(\gamma_i, 1) \notin \mathfrak{p}_i$, and by Hensel's Lemma we can also assume that

$$F_i(\gamma_i, 1) \not\equiv 0 \pmod{\mathfrak{p}_i^2}.$$

Since $\beta \equiv 1 \pmod{\mathfrak{p}_i^2}$, we have moreover

$$F_i(\gamma_i, \beta) \equiv 0 \pmod{\mathfrak{p}_i}, \qquad F_i(\gamma_i, \beta) \not\equiv 0 \pmod{\mathfrak{p}_i^2}.$$

Finally, let $\gamma \in \mathcal{O}_L$ with $\gamma \equiv \gamma_i \pmod{\mathfrak{p}_i^2}$ and $\gamma \equiv 1 \pmod{\mathfrak{p}_{i_0}}$.

Let $\mathfrak{q}_i = (p, F_i(\gamma, \beta))$ (for $i = i_0$, this gives $\mathfrak{q}_{i_0} = (p, \beta)$). Clearly, $\mathfrak{p}_i \mid \mathfrak{q}_i$, $\mathfrak{p}_i^2 \nmid \mathfrak{q}_i$. Moreover, if $i \neq j$, $i, j \neq i_0$, then $\mathfrak{p}_i \nmid \mathfrak{q}_j$, since otherwise $F_i(\gamma, 1) \equiv 0 \pmod{\mathfrak{p}_i}$ and $F_j(\gamma, 1) \equiv 0 \pmod{\mathfrak{p}_i}$, whence $\overline{F}_i(x, 1)$ and $\overline{F}_j(x, 1)$ would have a common root, but they are coprime. Similarly, for $i \neq i_0$, $\mathfrak{p}_{i_0} \nmid \mathfrak{q}_i$ (since otherwise $F_i(\gamma, \beta) \in \mathfrak{p}_{i_0}$, which would imply that $\gamma \in \mathfrak{p}_{i_0}$) and $\mathfrak{p}_i \nmid \mathfrak{q}_{i_0}$ (since otherwise $\beta \in \mathfrak{p}_i$). It follows that $\mathfrak{q}_i = \mathfrak{p}_i$ for all i.

Let $F = F_1^{e_1} \cdots F_t^{e_t}$. It is plain that $F(\gamma, \beta) \equiv 0 \pmod{p\mathcal{O}_L}$. On the other hand, let $\alpha = \gamma/\beta$ and let $W(x)$ be a primitive irreducible polynomial with integer coefficients such that $W(\alpha) = 0$. In particular, denoting by

W again the homogenized polynomial of W with the same degree, we have $W(\gamma,\beta)=0$, whence $W(\gamma,\beta)\in\mathfrak{p}_i^{e_i}$ for all i. Arguing as above, we see that $\mathfrak{p}_i$ and $G(\gamma,\beta)$ are coprime for all G such that $(\overline{F}_i,\overline{G})=1$, and we get the inequality

$$e_i \le v_{\mathfrak{p}_i}(W(\gamma,\beta)) = v_{\mathfrak{p}_i}(F_i(\gamma,\beta))v_{\overline{F}_i}(\overline{W}).$$

In any case, we see that $v_{\overline{F}_i}(\overline{W})\ge 1$, and if $e_i\ge 2$, we have $v_{\mathfrak{p}_i}(F_i(\gamma,\beta))=1$ from the previous discussion, which gives $e_i \le v_{\overline{F}_i}(\overline{W})$. It follows that $\overline{F}_i^{e_i} \mid \overline{W}$ for all i, whence $\overline{F} \mid \overline{W}$. Taking into account the degrees, we infer in fact that $\overline{F}=\overline{W}$ up to a non-zero constant.

Consider now the order $\mathbb{Z}_W$. We want to show that

$$\mathbb{Z}_W \cap p\mathcal{O}_L = pZ_W.$$

One inclusion is obvious, so let $\varrho\in\mathbb{Z}_W\cap p\mathcal{O}_L$, and write $\varrho=T(\alpha)$ for some $T(x)\in\mathbb{Z}[x]$. Homogenizing T we obtain $T(\gamma,\beta)\equiv 0 \pmod{\mathfrak{p}_i^{e_i}}$ and therefore $\overline{T}$ is divisible by $\overline{F}_i^{e_i}$ in view of what we have just proved. By the proof of Proposition 5, $\varrho\in p\mathbb{Z}_W+\mathfrak{B}^{e_if_i}F_i^{e_i}(\alpha,1)$ for $i\ne i_0$ where $\mathfrak{B}$ is the denominator of α in $\mathbb{Z}_W$; similarly, interchanging the roles of α and α^{-1}, we obtain $\varrho\in p\mathbb{Z}_W+\mathfrak{B}^{e_{i_0}}y^{e_{i_0}}$ as well. Hence $\varrho\in p\mathbb{Z}_W$ by Theorem 1, as wanted.

Finally, the equality $\mathbb{Z}_W\cap p\mathcal{O}_L = pZ_W$ means that the inclusion $\mathbb{Z}_W\to\mathcal{O}_L$ induces an isomorphism $\mathbb{Z}_W/p\mathbb{Z}_W \xrightarrow{\sim} \mathcal{O}_L/p\mathcal{O}_L$, showing that $p\nmid[\mathcal{O}_L:\mathbb{Z}_W]$. ∎

Corollary 3. *If p divides the generalized index of a number field L with $[L:\mathbb{Q}]=n$, then $p<n-1$.*

Proof. It is immediate to check that for $p+1\ge n$ and for every $d\ge 1$ there are at least $[n/d]$ distinct homogeneous irreducible polynomials in $\mathbb{F}_p[x,y]$ of degree d. ∎

Remark 3. For $d>1$, the number of irreducible homogeneous polynomials of degree d in $\mathbb{F}_p[x,y]$ is the same as the number of irreducible polynomials of degree d in $\mathbb{F}_p[x]$, whereas for $d=1$ there are $p+1$ irreducible linear forms and p linear polynomials. It follows that a prime p does not divide the generalized index of L if and only if: either (i) p does not divide the index of L (with the usual definition given in [5]), or (ii) there are exactly $p+1$ primes with inertial degree 1 above p.

Example 2. Consider the cubic field $L=\mathbb{Q}(\alpha)$ where α is a root of $F=2x^3+x^2+3x+2=0$. The discriminant of this cubic field is $\mathrm{Disc}(F)=\mathrm{Disc}(L)=-431$. We have $F(x,y)=x(x-y)y \pmod 2$, and this implies that the generalized index of L is 1, whereas the usual index of L is divisible by 2 (it is exactly 2 because of the polynomial $4F(x/2)$).

We also derive a necessary condition for an element α of a number field to have index 1.

PROPOSITION 11. *Let $L = \mathbb{Q}(\alpha)$ be a number field and p a prime number. Let F be the minimal polynomial of α, and $\mathfrak{A}$ the numerator of α (an ideal in $\mathcal{O}_L$). If one of the following conditions is satisfied, then p divides the index $[\mathcal{O}_L : \mathbb{Z}_F]$:*

(i) *there is a prime ideal $\mathfrak{p}$ above p with inertial degree $f_\mathfrak{p} \geq 2$ such that $\mathfrak{p} \mid \mathfrak{A}$,*

(ii) *there are two different prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ above p with inertial degree 1 such that $\mathfrak{p}_1\mathfrak{p}_2 \mid \mathfrak{A}$,*

(iii) *there is a prime ideal $\mathfrak{p}$ above p with ramification index $e_\mathfrak{p} \geq 2$ such that $\mathfrak{p}^2 \mid \mathfrak{A}$.*

Proof. Let p be a prime, and assume that p does not divide the index of α. Then from Theorem 3 all prime ideals above are of the form $\mathfrak{p} = p\mathcal{O}_L + \mathfrak{B}^{f_i} F_i(\alpha, 1)$. But Lemma 1 shows that $\mathfrak{p}$ is coprime to $\mathfrak{A}$, unless $F_i = ux$. This proves that at most one prime ideal above p can divide $\mathfrak{A}$. In this case, we have $f_i = \deg(ux) = 1$. This prime ideal $\mathfrak{p}$ is such that $\mathfrak{p} = p\mathcal{O}_L + \alpha\mathfrak{B} = p\mathcal{O}_L + \mathfrak{A}$. By inspecting valuations, we see that if $e_\mathfrak{p} > 1$, we must have $v_\mathfrak{p}(\mathfrak{A}) = 1$. ∎

REMARK 4. Since the index of α does not change under the transformations of $\mathrm{GL}_2(\mathbb{Z})$, we can apply this proposition to all the elements of the form $(a\alpha + b)/(c\alpha + d)$ with $ad - bc = \pm 1$. In particular, we can apply it to $1/\alpha$ or to $\alpha + q$. This shows, for example, that for any integer q and any prime p, the numerator and the denominator of $\alpha + q$ can only be divisible by primes $\mathfrak{p}$ with inertial degree $f_\mathfrak{p} = 1$, and by at most one such prime above each prime p.

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, 3rd corrected printing, Springer, 1996.

[3] —, *Advanced Topics in Computational Number Theory*, Grad. Texts in Math. 193, Springer, 2000.

[4] R. W. Gilmer, *Multiplicative Ideal Theory*, Queen's Papers in Pure and Appl. Math. 12, Queen's Univ., Kingston, ON, 1968.

[5] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., PWN and Springer, 1990.

[6] D. Simon, *The index of nonmonic polynomials*, Indag. Math. (N.S.) 12 (2001), 505–517.

[7] D. Simon, *La classe invariante d'une forme binaire*, C. R. Acad. Sci. Paris Math. 336 (2003), 7–10.

Dipartimento di Matematica
Università di Pisa
Largo B. Pontecorvo, 5
56127 Pisa, Italy
E-mail: delcorso@dm.unipi.it
dvornic@dm.unipi.it

LMNO–UMR 6139
Université de Caen
Campus II-Bd Marechal Juin
BP 5186
14032 Caen Cedex, France
E-mail: simon@math.unicaen.fr

Received on 5.10.2004 (4860)