Natural Science Report, Ochanomizu University, Vol. 28, No. 1, 1977
お茶の水女子大学 自然科学報告 第28巻第1号

On Non-Maximal Orders of Algebraic Number Fields

Rumiko Ohta

Department of Mathematics, Faculty of Science,
Ochanomizu University, Tokyo

(Received April 5, 1977)

§ 0. Introduction

Let k be an algebraic number field, O_k the maximal order, R an order of k with the conductor f, j an ideal of R, $O(j)$ the set of elements $\xi \in k$ such that ξj is contained in j, namely the largest order of which j is an ideal. We call j R-proper if we have $O(j)=\mathrm{R}$ and R-regular if we have $\alpha j \subset \mathrm{R}$, $(\alpha j, f)=\mathrm{R}$ for some element $\alpha \in k^*$.(*) Now it is clear that j is R-proper if it is R-regular. In this paper, we are going to consider whether the converse is true. Our result is as follows: if k is a quadratic number field, j is R-proper if and only if j is R-regular (§ 2); if k is an algebraic number field of degree greater than 3, there is an example of R-proper ideals which are not R-regular (§ 3). In order to prove this, we shall give a local characterization of R-regularity (§ 1). Incidentally we can define R-invertibleness; we call R-ideal j R-invertible if there exists a fractional ideal j' of R such that $jj'=\mathrm{R}$. In reality, we have obtained an example of an ideal which is R-proper, but not R-invertible (Proposition 2). If $n=3$ and p satisfies certain conditions, R_p-invertibleness implies R_p-regularity. But in general case, we could not decide whether this is so or not (§ 4).

§ 1. Non-maximal orders of k_p

Let k be an algebraic number field, O_k the maximal order, R an order of k, j an ideal of R. For any prime number p, we consider $k_p=k\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$, $O_p=O_k\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$ where $\boldsymbol{Q}_p$ is the p-adic number field and $\boldsymbol{Z}_p$ is the maximal order. It is obvious that k_p is $\boldsymbol{Q}_p$-algebra, $\mathrm{R}_p=\mathrm{R}\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$ an order of k_p, $j_p=j\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$ an ideal of R_p. On the other hand, if $(p)=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$ is the decomposition of (p) into prime ideals in k where $\mathfrak{p}_i$ is a distinct prime ideal dividing (p) $(1\leqq i\leqq g)$, we have the following isomorphism Φ_p of k_p onto $k_{\mathfrak{p}_1}\oplus\cdots\oplus k_{\mathfrak{p}_g}$ where $k_{\mathfrak{p}_i}$ is

(*) Usually the definition of regularity is as follows: an ideal j of R is regular if $(j, f)=\mathrm{R}$. Our definition slightly generalizes the usual one.

the $\mathfrak{p}_i$-adic number field $(1 \leqq i \leqq g)$.

$$\Phi_p: k \otimes_Q \boldsymbol{Q}_p \longrightarrow k_{\mathfrak{p}_1} \oplus \cdots \oplus k_{\mathfrak{p}_g}$$
$$a \otimes \lambda \mapsto (C_1(a)\lambda, \cdots, C_g(a)\lambda)$$

where C_i is a fixed isomorphism from k into $k_{\mathfrak{p}_i}$ $(1 \leqq i \leqq g)$. At this time, we have $\Phi_p(O_p) = O_{\mathfrak{p}_1} \oplus \cdots \oplus O_{\mathfrak{p}_g}$, hence O_p is the maximal order of k_p, where $O_{\mathfrak{p}_i}$ is the maximal order of $k_{\mathfrak{p}_i}$ $(1 \leqq i \leqq g)$. For any ideal $\mathfrak{a}$ of O_k, $\Phi_p(\mathfrak{a} \otimes_Z \boldsymbol{Z}_p) = \mathfrak{a}_{\mathfrak{p}_1} \oplus \cdots \oplus \mathfrak{a}_{\mathfrak{p}_g}$ where $\mathfrak{a}_{\mathfrak{p}_i} = C_i(\mathfrak{a}) O_{\mathfrak{p}_i}$ $(1 \leqq s \leqq g)$. We shall use the following results.

(1) $\mathrm{R} = \bigcap_p (\mathrm{R} \otimes_Z \boldsymbol{Z}_p) \cap k$, $j = \bigcap_p (j \otimes_Z \boldsymbol{Z}_p) \cap k$ *where* p *is any prime number. Moreover* $\mathrm{R} \otimes_Z \boldsymbol{Z}_p$ (resp. $j \otimes_Z \boldsymbol{Z}_p$) *is* O_p (resp. $\mathrm{R} \otimes_Z \boldsymbol{Z}_p$) *except for finitely many prime numbers* p.

(2) *Conversely, take an order* R_p *of* k_p *for each* p *such that* $\mathrm{R}_p = O_p$ *except for finitely many prime numbers* p; *denote by* $\{\mathrm{R}_p\}_p$ *the collection of them. Then an order* $\mathrm{R} = \bigcap_p \mathrm{R}_p \cap k$ *of* k *is uniquely determined by* $\{\mathrm{R}_p\}_p$ *and* $\mathrm{R} \otimes_Z \boldsymbol{Z}_p$ *is equal to* R_p *for each* p.

(2′) *Take an ideal* j_p *of* $\mathrm{R}_p = \mathrm{R} \otimes_Z \boldsymbol{Z}_p$ *for each* p *such that* $j_p = \mathrm{R}_p$ *except for finitely many prime numbers* p; *denote by* $\{j_p\}_p$ *the collection of them. Then an ideal* $j = \bigcap_p j_p \cap k$ *of* R *is uniquely determined by* $\{j_p\}_p$ *and* $j \otimes_Z \boldsymbol{Z}_p$ *is equal to* j_p *for each* p.

DEFINITION. Let R_p be an order of k_p, j_p an ideal of R_p. We denote by f_p the set of elements $\xi_p \in k_p$ such that $\xi_p O_p \subset \mathrm{R}_p$ and call it the conductor of R_p. We call j_p R_p-proper if $O_p(j_p) = \{\xi_p \in k \mid \xi_p j_p \subset j_p\}$ is equal to R_p, R_p-regular if $\alpha_p j_p \subset \mathrm{R}_p$, $(\alpha_p j_p, f_p) = \mathrm{R}_p$ for some $\alpha_p \in k_p^*$ (k_p^* is the set of unity of k_p).

(3) *Let* f *be the conductor of* R, *namely* $f = \{\xi \in k \mid \xi O_k \subset \mathrm{R}\}$. *Then* $f \otimes_Z \boldsymbol{Z}_p$ *is the conductor of* $\mathrm{R}_p = \mathrm{R} \otimes_Z \boldsymbol{Z}_p$.

(4) $O(j) \otimes_Z \boldsymbol{Z}_p = O_p(j \otimes_Z \boldsymbol{Z}_p)$.

(5) j *is* R*-proper if and only if* $j \otimes_Z \boldsymbol{Z}_p$ *is* $\mathrm{R} \otimes_Z \boldsymbol{Z}_p$*-proper for any prime number* p.

(6) *Let* R_p *be an order of* k_p, f_p *the conductor of* R_p. *Then, for any ideal* j_p *of* R_p *such that* $(j_p, f_p) = \mathrm{R}_p$, $j_p O_p$ *is an ideal of* O_p *such that* $(j_p O_p, f_p) = O_p$ *and* $(j_p O_p) \cap \mathrm{R}_p = j_p$. *Conversely, for any ideal* $\mathfrak{a}_p$ *of* O_p *such that* $(\mathfrak{a}_p, f_p) = O_p$, $\mathfrak{a}_p \cap \mathrm{R}_p$ *is an ideal of* R_p *such that* $(\mathfrak{a}_p \cap \mathrm{R}_p, f_p) = \mathrm{R}_p$ *and* $(\mathfrak{a}_p \cap \mathrm{R}_p) O_p = \mathfrak{a}_p$.(*)

(7) *Let* R_p *be an order of* k_p *with the conductor* f_p, j_p *an ideal of* R_p. *Then, if* j_p *is prime to* f_p, *namely* $(j_p, f_p) = \mathrm{R}_p$, j_p *is principal in* R_p.

PROOF. By (6), we have an ideal $\mathfrak{a}_p$ of O_p such that it is prime

(*) j_p and $\mathfrak{a}_p$ here are regular in usual sense.

to f_p and $j_p=\mathfrak{a}_p\cap \mathrm{R}_p$. Therefore we have the following isomorphism via Φ_p, permutating indices if necessary;

$$f_p\cong \mathfrak{p}_1^{l_1}\oplus\cdots\oplus\mathfrak{p}_r^{l_r}\oplus O_{\mathfrak{p}_{r+1}}\oplus\cdots\oplus O_{\mathfrak{p}_g}$$
$$\mathfrak{a}_p\simeq O_{\mathfrak{p}_1}\oplus\cdots\oplus O_{\mathfrak{p}_r}\oplus\mathfrak{p}_{r+1}^{m_{r+1}}\oplus\cdots\oplus\mathfrak{p}_g^{m_g}$$

where $0<r\leqq g$ and l_i, m_j are non-negative integers ($1\leqq i\leqq r$, $r+1\leqq j\leqq g$). Let π_i be a prime element of $\mathfrak{p}_i$ ($1\leqq i\leqq g$). Then we have an element φ_p of f_p such that

$$\Phi_p(\varphi_p)=(\pi_1^{l_1},\ \cdots,\ \pi_r^{l_r},\ 1-\pi_{r+1}^{m_{r+1}},\ \cdots,\ 1-\pi_g^{m_g})$$

If we define a_p by $a_p=1-\varphi_p$, we have $a_p\in \mathrm{R}_p$, $\mathfrak{a}_p=a_pO_p$ and $(a_p\mathrm{R}_p,\ f_p)=\mathrm{R}_p$. Then, by (6) we have

$$j_p=(j_pO_p)\cap \mathrm{R}_p=(a_pO_p)\cap \mathrm{R}_p=(a_p\mathrm{R}_pO_p)\cap \mathrm{R}_p=a_p\mathrm{R}_p\ .$$

According to (7), we have obviously the following proposition.

PROPOSITION 1. *Let R_p be an order of k_p, j_p an ideal of R_p. Then, j_p is R_p-regular if and only if it is principal in R_p.*

(8) APPROXIMATION THEOREM. *Let $p_1,\ \cdots,\ p_r$ be finitely many distinct prime numbers, a_{p_i} a unit of k_{p_i} R_{p_i} an order of k_{p_i} ($1\leqq i\leqq r$). Then, there exists an element $\alpha\in k^*$ such that $(\alpha\otimes 1)a_{p_i}$ is a unit of R_{p_i} ($1\leqq i\leqq r$) and $\alpha\otimes 1\in O_p$ for p different from $p_1,\ \cdots,\ p_r$.*

PROPOSITION 2. *Let R be an order of k, j an ideal of R, $\mathrm{R}_p=\mathrm{R}\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$, $j_p=j\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$. Then, j is R-regular if and only if j_p is R_p-regular for all prime numbers p.*

PROOF. Clearly we have only to verify the sufficiency. We denote by P the set $\{p|p$ is a prime number such that $j_p\neq O_p$ or $f_p\neq O_p\}$. Then P is a finite set. By the assumption, for any prime number p, we have an element $a_p\in k_p^*$ such that $a_pj_p\subset \mathrm{R}_p$ and $(a_pj_p,\ f_p)=\mathrm{R}_p$, where f is the conductor of R and $f_p=f\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$. Then, by (8), we have an element $\alpha\in k^*$ such that $(\alpha\otimes 1)a_p^{-1}$ is a unit of R_p for $p\in P$ and $\alpha\otimes 1\in O_p$ for $p\notin P$. Namely,

$$(\alpha\otimes 1)j_p=\begin{cases}a_pj_p\subset \mathrm{R}_p\ , & \text{if}\quad p\in P\\ (\alpha\otimes 1)O_p\subset O_p=\mathrm{R}_p\ , & \text{if}\quad p\notin P\end{cases}$$

Therefore by (1), we have $\alpha j\subset \mathrm{R}$ and

$$(\alpha j,\ f)_p=((\alpha\otimes 1)j_p,\ f_p)=\begin{cases}(a_pj_p,\ f_p)=\mathrm{R}_p\ , & \text{if}\quad p\in P\\ ((\alpha\otimes 1)O_p,\ O_p)=O_p=\mathrm{R}_p\ , & \text{if}\quad p\in P\end{cases}$$

where $(\alpha j, f)_p=(\alpha j, f)\otimes_Z \boldsymbol{Z}_p$. Then by (2′) we have $(\alpha j, f)=\mathrm{R}$ and this proposition is proved.

From Proposition 1 and 2, we have clearly the following theorem.

THEOREM 1. *Let* R *be an order of* k, j *an ideal of* R, $\mathrm{R}_p=\mathrm{R}\otimes_Z \boldsymbol{Z}_p$ *and* $j_p=j\otimes_Z \boldsymbol{Z}_p$ *for any prime number* p. *Then the following conditions are equivalent.*

(1) j *is* R*-regular.*

(2) j_p *is* R_p*-regular for all* p.

(3) j_p *is principal in* R_p *for all* p.

§ 2. Case of a quadratic number field

Let j_p be a $\boldsymbol{Z}_p$-submodule of O_p such that $(O_p: j_p)<\infty$. Then $O_p(j_p)=\{\xi_p\in k_p \mid \xi_p j_p\subset j_p\}$ is an order of k_p and j_p is a fractional ideal of it. In this section, we assume that k is a quadratic number field, and we are going to consider whether j_p is principal in $O_p(j_p)$.

Let k be $Q(\sqrt{m})$ where m is a square free integer. Then $O_p=\boldsymbol{Z}_p\oplus\omega\boldsymbol{Z}_p$ where ω is $\sqrt{m}$ if $m\equiv 2, 3 \pmod 4$ or $p\neq 2$, $(1+\sqrt{m})/2$ if $m\equiv 1 \pmod 4$ and $p=2$. Then, for any prime number p, we have

$$k_p=\boldsymbol{Q}_p\oplus\omega\boldsymbol{Q}_p$$
$$O_p=\boldsymbol{Z}_p\oplus\omega\boldsymbol{Z}_p$$
$$j_p=p^{l_1}\boldsymbol{Z}_p\oplus(\lambda+p^{l_2}\omega)\boldsymbol{Z}_p$$

where l_i are non-negative integers $(i=1, 2)$ and $\lambda\in\boldsymbol{Z}_p$. Now, since $O_p(\xi_p j_p)=O_p(j_p)$ for any element $\xi_p\in k_p^*$, we can assume one of the following three conditions; (1) $l_1=0$, (2) $l_2=0$, (3) λ is a unit of $\boldsymbol{Z}_p$. Then it is easy to see the following proposition holds.

PROPOSITION 3. *Notations being as above,* j_p *is expressed as follows.*

(I) *If* $m\equiv 2, 3 \pmod 4$ *or* $p\neq 2$, we have

$$j_p=\begin{cases} O_p(j_p) & \text{if } l_1=0 \\ (p^{l_1}+\lambda+\omega)O_p(j_p) & \text{if } l_1>0,\ l_2=0,\ l_0\neq 1_1 \\ (\lambda+\omega)O_p(j_p) & \text{if } l_1>0,\ l_2=0,\ l_0=1_1 \\ (\lambda+p^{l_2}\omega)O_p(j_p) & \text{if } l_1>0,\ l_2>0,\ \lambda \text{ is a unit of } \boldsymbol{Z}_p \end{cases}$$

where p^{l_0} *is the highest power of* p *which divides* $m-\lambda^2$.

(II) *If* $m\equiv 1 \pmod 4$ *and* $p=2$, *we have*

$$j_2=\begin{cases} O_2(j_2) & \text{if } l_1=0 \\ (2^{l_1}+\lambda+\omega)O_2(j_2) & \text{if } l_1>0,\ l_2=0,\ l_0\neq l_1 \\ (\lambda+\omega)O_2(j_2) & \text{if } l_1>0,\ l_2=0,\ l_0=l_1 \\ (\lambda+2^{l_2}\omega)O_2(j_2) & \text{if } l_1>0,\ l_2>0,\ \lambda \text{ is a unit of } \boldsymbol{Z}_2 \end{cases}$$

where 2^{l_0} *is the highest power of* 2 *which divides* $(m-1)/4-\lambda(\lambda+1)$.

PROOF. This proposition is immediately proved, since $O_p(j_p)$ has the following form.

(I) If $m\equiv 2, 3 \pmod 4$ or $p\neq 2$,

$$O_p(j_p)=\begin{cases} j_p & \text{if } l_1=0 \\ \boldsymbol{Z}_p\oplus p^{l_1-l_0}\omega\boldsymbol{Z}_p & \text{if } l_1>0,\ l_2=0,\ l_0<l_1 \\ O_p & \text{if } l_1>0,\ l_2=0,\ l_0\geqq l_1 \\ \boldsymbol{Z}_p\oplus p^{l_1+l_2}\omega\boldsymbol{Z}_p & \text{if } l_1>0,\ l_2>0,\ \lambda \text{ is a unit of } \boldsymbol{Z}_p \end{cases}$$

(II) If $m\equiv 1 \pmod 4$ and $p=2$,

$$O_2(j_2)=\begin{cases} j_2 & \text{if } l_1=0 \\ \boldsymbol{Z}_2\oplus 2^{l_1-l_0}\omega\boldsymbol{Z}_2 & \text{if } l_1>0,\ l_2=0,\ l_0<l_1 \\ O_2 & \text{if } l_1>0,\ l_2=0,\ l_0\geqq l_1 \\ \boldsymbol{Z}_2\oplus 2^{l_1+l_2}\omega\boldsymbol{Z}_2 & \text{if } l_1>0,\ l_2>0,\ \lambda \text{ is a unit of } \boldsymbol{Z}_2 \end{cases}$$

Thus, from this proposition and Theorem 1, we have the following theorem.

THEOEM 2. *Let* k *be a quadratic number field,* R *an order of* k, j *an ideal of* R. *Then,* j *is* R*-proper if and only if it is* R*-regular.*

§ 3. Case of an algebraic number field of degree n greater than 3 over Q

In this section, we shall give an example of an ideal which is R-proper and not R-regular in case $n\geqq 3$.

Let $k=\boldsymbol{Q}(\theta)$ be an algebraic number field of degree n greater than 3 over $\boldsymbol{Q}$. We may assume that θ is an algebraic integer. Let $f(X)=X^n+a_1X^{n-1}+\cdots+a_n$ be the irreducible polynomial that has θ as a root, a_i being a rational integer $(1\leqq i\leqq n)$.

PROPOSITION 4. *Notations being as above, let* p *be a prime number relatively prime to the discriminant of* k *and let* p^l *be the highest power of* p *which divides* a_n. *We consider the following*

order R *of* k *and the ideal* j *of* R.

$$\mathrm{R}= \quad \boldsymbol{Z}\oplus p^m\theta\boldsymbol{Z}\oplus\cdots\oplus p^m\theta^{n-1}\boldsymbol{Z}$$
$$j=p^{l+2m}\boldsymbol{Z}\oplus p^m\theta\boldsymbol{Z}\oplus\cdots\oplus p^m\theta^{n-1}\boldsymbol{Z}$$

where m *is an integer greater than* 2. *Then* j *is* R*-proper, but not* R*-regular.*

PROOF. We can verify by calculation that j is R-proper. In order to prove the second assertion, put R′ an order of k defined by

$$\mathrm{R}'=\boldsymbol{Z}\oplus p^{m-1}\theta\boldsymbol{Z}\oplus p^m\theta^2\boldsymbol{Z}\oplus\cdots\oplus p^m\theta^{n-1}\boldsymbol{Z}\,.$$

Then we have $O_p(j_p\mathrm{R}'_p)\supsetneqq\mathrm{R}'_p$ where $j_p=j\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$ and $\mathrm{R}'_p=\mathrm{R}'\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$. On the other hand, it follows from Theorem 1; if j is R-regular, j_p is principal in R_p, hence $j_p\mathrm{R}'_p$ is principal in R'_p. This contradicts the fact $O_p(j_p\mathrm{R}'_p)\supsetneqq\mathrm{R}'_p$.

§ 4. Case of an algebraic number field of degree 3 over Q

For k of degree 3 over $\boldsymbol{Q}$, we can prove by straightforward calculation the following;

PROPOSITION 5. *Let* j_p *be a* $\boldsymbol{Z}_p$*-submodule of* O_p *of rank* 3. *If the decomposition of the ideal* (p) *into prime ideals in* k *is* $(p)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ *or* $(p)=\mathfrak{p}_1\mathfrak{p}_2$ *where* $\mathfrak{p}_i\neq\mathfrak{p}_j$ $(i\neq j)$, *either* (1) *or* (2) *occurs*;

(1) j_p *is principal in* $O_p(j_p)$,

(2) $O_p(j_p)\subsetneqq O_p(j_p^2)$.

This proposition means that in these cases j_p is invertible in $O_p(j_p)$ (i.e. there exists a $\boldsymbol{Z}_p$-module j'_p such that $j_pj'_p=O_p(j_p)$) if and only if j_p is principal in $O_p(j_p)$. However we could not prove that this holds in general. This is an open question left to us.

References

[1] T. Takagi, Daisūteki Seisūron, Iwanami, 1948.

[2] M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren, J. Reine Angew. Math., **195** (1955), 127-151.