ALGEBRA, LOGIC AND NUMBER THEORY
BANACH CENTER PUBLICATIONS, VOLUME 121
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2020

MAXIMALITY OF ORDERS IN NUMBER FIELDS

BEATA ROTHKEGEL

Institute of Mathematics, University of Silesia
Bankowa 14, 40-007 Katowice, Poland
ORCID: 0000-0002-9953-5667 E-mail: beata.rothkegel@us.edu.pl

Abstract. In the paper, we formulate equivalent conditions for an order in a number field to be maximal.

1. Introduction. Let K be a number field and let R_K be the ring of integers of K. An *order* in K is a subring $\mathcal{O}$ of R_K which contains an integral basis of length $[K:\mathbb{Q}]$. The ring R_K is an order in K and it is called the *maximal order* (cf. [N, Chapter I, (12.1) Definition]).

According to [N, Chapter I, (12.2) Proposition], every order in K is a one-dimensional Noetherian domain with the field of fractions K.

The following ideal of R_K is associated with an order $\mathcal{O}$:

$$\mathfrak{f} = \{a \in R_K : aR_K \subseteq \mathcal{O}\}.$$

This ideal is called the *conductor* of $\mathcal{O}$. It is nonzero and it is the greatest ideal of R_K lying in $\mathcal{O}$ (cf. [N, p. 79]).

Example 1.1. Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer. Then

$$R_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{when } d \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{when } d \equiv 1 \pmod 4. \end{cases}$$

Moreover,

$$\mathcal{O} = \begin{cases} \mathbb{Z}[f\sqrt{d}] & \text{when } d \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[f\,\frac{1+\sqrt{d}}{2}\right] & \text{when } d \equiv 1 \pmod 4 \end{cases}$$

2010 *Mathematics Subject Classification*: Primary 16H15; Secondary 11R99.

Key words and phrases: order, Picard group, divisor, Witt ring.

The paper is in final form and no version of it will be published elsewhere.

DOI: 10.4064/bc121-14

for some $f \in \mathbb{N}$ (cf. [BS, p. 151]). The conductor of $\mathcal{O}$ is a principal ideal generated by f; $\mathfrak{f} = fR_K$.

The question is as follows: when is $\mathcal{O}$ the maximal order? Obviously, if it is integrally closed. Indeed, $\mathcal{O} \subseteq R_K$. Take $a \in R_K$. Then a is integral over $\mathbb{Z}$, so it is integral over $\mathcal{O}$. But $\mathcal{O}$ is integrally closed, so $a \in \mathcal{O}$ and $R_K \subseteq \mathcal{O}$.

In the paper, we consider the maximality of $\mathcal{O}$ in another context. We formulate equivalent conditions for the maximality of $\mathcal{O}$ using some homomorphisms between objects related to orders. The paper contains natural conclusions from the results of [R2] for orders in number fields.

Let K be a number field and let $\mathcal{O}$ be an order in K. We write $\mathrm{Spec}(\mathcal{O})$, $\mathrm{Pic}(\mathcal{O})$ and $\mathsf{cl}\, I$ for the maximal spectrum of $\mathcal{O}$, the Picard group of $\mathcal{O}$ and the class of an invertible fractional ideal I of $\mathcal{O}$ in $\mathrm{Pic}(\mathcal{O})$, respectively.

The group $\mathrm{Pic}(\mathcal{O})$ is generated by all invertible ideals of $\mathcal{O}$ modulo the principal ideals $a\mathcal{O}$, $0 \neq a \in K$ (cf. [N, Chapter I, (12.5) Definition]). From [N, Chapter I, (12.12) Theorem and p. 75], it follows that it is finite and if $\mathcal{O} = R_K$ is the maximal order, then $\mathrm{Pic}(R_K)$ is the ideal class group Cl_K of K. We write h_K for the class number $\#\mathrm{Cl}_K$.

Throughout the paper, $U(P)$ and U_K denote the group of invertible elements of a commutative ring P and the group $U(R_K)$ of units of K, respectively.

2. Picard group and divisors of $\mathcal{O}$. Consider the natural homomorphism $\mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}_K$ defined by

$$\mathsf{cl}\, I \mapsto \mathsf{cl}(IR_K) \quad \text{for all } \mathsf{cl}\, I \in \mathrm{Pic}(\mathcal{O}).$$

We call it the *Picard group homomorphism* and by [R2, Lemma 2.4] it is surjective.

Since the group $\mathrm{Pic}(R_K)$ is finite, from [R2, Theorem 4.1], the following fact follows.

THEOREM 2.1. *Let K be a number field and let $\mathcal{O}$ be an order in K. The following conditions are equivalent.*

(1) *$\mathcal{O}$ is the maximal order.*
(2) *The Picard group homomorphism is an isomorphism and $U_K \subseteq \mathcal{O}$.*
(3) *The Picard group homomorphism is injective and $U_K \subseteq \mathcal{O}$.*

COROLLARY 2.2. *Let K be a number field and let $\mathcal{O}$ be an order in K. Then $\mathcal{O}$ is the maximal order if and only if*

(1) $\#\mathrm{Pic}(\mathcal{O}) = h_k$.
(2) $U_K \subseteq \mathcal{O}$.

EXAMPLE 2.3. Consider $K = \mathbb{Q}(\sqrt{d})$, where $d < 0$ is a square-free integer and $d \equiv 5 \pmod 8$. Moreover, let $\mathcal{O} = \mathbb{Z}\big[f\frac{1+\sqrt{d}}{2}\big]$ for some $f \in \mathbb{N}$.

Suppose $f \neq 1$. If $d = -3$, then $U_K = \{\pm 1, \pm\frac{1\pm\sqrt{-3}}{2}\} \nsubseteq \mathcal{O}$. Therefore we assume $d \neq -3$.

Now $U_K = \{\pm 1\} \subseteq \mathcal{O}$. From [N, Chapter I, (12.12) Theorem], it follows that

$$\#\mathrm{Pic}(\mathcal{O}) = h_K\, \frac{\#U(R_K/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}.$$

We show that $\#\mathrm{Pic}(\mathcal{O}) \neq h_K$.

Indeed, assume $f \neq 2$. Then $\sqrt{d} \notin \mathcal{O}$. If $\gcd(d, f) = 1$, then there exist $x, y \in \mathbb{Z}$ such that $dx + fy = 1$. Hence

$$(\sqrt{d} + \mathfrak{f})(\sqrt{d}\,x + \mathfrak{f}) = 1 + \mathfrak{f}$$

and $\sqrt{d} + \mathfrak{f} \in U(R_K/\mathfrak{f}) \setminus U(\mathcal{O}/\mathfrak{f})$.

Let p be a prime number such that $p|d$ and $p|f$. It is easy to observe that $1 + \frac{f}{p}\sqrt{d} \notin \mathcal{O}$ and $\gcd\bigl(1 - \frac{f^2}{p^2}d, f\bigr) = 1$. Then $\bigl(1 - \frac{f^2}{p^2}d\bigr)x + fy = 1$ for some $x, y \in \mathbb{Z}$ and

$$\left[\left(1 + \frac{f}{p}\sqrt{d}\right) + \mathfrak{f}\right]\left[\left(1 - \frac{f}{p}\sqrt{d}\right)x + \mathfrak{f}\right] = 1 + \mathfrak{f}.$$

Moreover, $\bigl(1 + \frac{f}{p}\sqrt{d}\bigr) + \mathfrak{f} \in U(R_K/\mathfrak{f}) \setminus U(\mathcal{O}/\mathfrak{f})$.

Assume $f = 2$. Since $d \equiv 5 \pmod 8$, the integer $\frac{1-d}{4}$ is odd and $\gcd\bigl(\frac{1-d}{4}, f\bigr) = 1$. Similarly as above, there exist $x, y \in \mathbb{Z}$ such that $\frac{1-d}{4}x + fy = 1$. Hence

$$\left(\frac{1 + \sqrt{d}}{2} + \mathfrak{f}\right)\left(\frac{1 - \sqrt{d}}{2}\,x + \mathfrak{f}\right) = 1 + \mathfrak{f}$$

and $\frac{1+\sqrt{d}}{2} + \mathfrak{f} \in U(R_K/\mathfrak{f}) \setminus U(\mathcal{O}/\mathfrak{f})$.

Finally, $\#U(R_K/\mathfrak{f}) \neq \#U(\mathcal{O}/\mathfrak{f})$, i.e. $\#\mathrm{Pic}(\mathcal{O}) \neq h_K$.

Some homomorphism between the Picard group and the Chow group is associated with the maximality of $\mathcal{O}$.

First, consider the group $C(\mathcal{O})$ of Cartier divisors and the group $\mathrm{Div}(\mathcal{O})$ of Weil divisors of $\mathcal{O}$. The first one is a multiplicative group generated by all invertible ideals of $\mathcal{O}$ (cf. [E, Corollary 11.7]) and the second one is a free abelian group generated by all maximal ideals of $\mathcal{O}$ (cf. [E, pp. 225, 259]).

Let $I \neq 0$ be an invertible ideal in $\mathcal{O}$, $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ be a maximal ideal and $I_{\mathfrak{p}}$ be the localization of I at $\mathfrak{p}$. Moreover, let $\mathsf{length}(\mathcal{O}_{\mathfrak{p}}/I_{\mathfrak{p}})$ denotes the length of the ring $\mathcal{O}_{\mathfrak{p}}/I_{\mathfrak{p}}$.

From [E, Theorem 11.10 and its proof], it follows that $\mathsf{length}(\mathcal{O}_{\mathfrak{p}}/I_{\mathfrak{p}}) < \infty$ and there is a group homomorphism $g\colon C(\mathcal{O}) \to \mathrm{Div}(\mathcal{O})$ defined by

$$g(I) = \sum_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})} \mathsf{length}(\mathcal{O}_{\mathfrak{p}}/I_{\mathfrak{p}}) \cdot \mathfrak{p}$$

for all invertible ideals I in $\mathcal{O}$. We call it the *length homomorphism.*

In the case when $\mathcal{O} = R_K$ is the maximal order, the length homomorphism is injective (cf. [E, Proposition 11.11]). Theorem 2.4 shows that the injectivity of g is an equivalent condition for $\mathcal{O}$ to be maximal.

THEOREM 2.4. *Let K be a number field and let $\mathcal{O}$ be an order in K. The following conditions are equivalent.*

(1) *$\mathcal{O}$ is the maximal order.*
(2) *The length homomorphism is an isomorphism.*
(3) *The length homomorphism is injective.*

Proof. See [R2, proof of Theorem 3.1]. ∎

EXAMPLE 2.5. Consider $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O} = \mathbb{Z}\big[f\frac{1+\sqrt{-3}}{2}\big]$ for some $1 \neq f \in \mathbb{N}$. Then $\pm\frac{1\pm\sqrt{-3}}{2} \notin \mathcal{O}$, so $\frac{1\pm\sqrt{-3}}{2}\mathcal{O} \neq \mathcal{O}$. Since $\frac{1\pm\sqrt{-3}}{2}R_K = R_K$, by [R2, Lemma 3.1], $\frac{1\pm\sqrt{-3}}{2}\mathcal{O} \in \ker g$. The length homomorphism is not injective.

Let $\mathrm{Chow}(\mathcal{O})$ be the Chow group of $\mathcal{O}$. It is the group of Weil divisors of $\mathcal{O}$ modulo the principal divisors $g(a\mathcal{O})$, $0 \neq a \in K$ (cf. [E, p. 260]). The length homomorphism g induces a homomorphism $\overline{g}\colon \mathrm{Pic}(\mathcal{O}) \to \mathrm{Chow}(\mathcal{O})$.

Similarly as the length homomorphism, the homomorphism $\overline{g}\colon \mathrm{Cl}_K \to \mathrm{Chow}(R_K)$ is injective (cf. [E, Proposition 11.11]).

THEOREM 2.6. *Let K be a number field and let $\mathcal{O}$ be an order in K. The following conditions are equivalent.*

(1) *$\mathcal{O}$ is the maximal order.*
(2) *The homomorphism $\overline{g}\colon \mathrm{Pic}(\mathcal{O}) \to \mathrm{Chow}(\mathcal{O})$ is an isomorphism and $U_K \subseteq \mathcal{O}$.*
(3) *The homomorphism $\overline{g}\colon \mathrm{Pic}(\mathcal{O}) \to \mathrm{Chow}(\mathcal{O})$ is injective and $U_K \subseteq \mathcal{O}$.*

Proof. See [R2, proof of Theorem 4.2]. ∎

It is easy to observe that the group of Cartier divisors of R_K is the group of all fractional ideals of K. We write C_K for it.

There is a natural homomorphism $C(\mathcal{O}) \to C_K$ defined by

$$I \mapsto IR_K \quad \text{for all } I \in C(\mathcal{O}).$$

We call it the *Cartier group homomorphism.*

THEOREM 2.7. *Let K be a number field and let $\mathcal{O}$ be an order in K. The following conditions are equivalent.*

(1) *$\mathcal{O}$ is the maximal order.*
(2) *The Cartier group homomorphism is an isomorphism.*
(3) *The Cartier group homomorphism is injective.*

Proof. See [R2, proof of Theorem 2.1]. ∎

EXAMPLE 2.8. Consider $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O} = \mathbb{Z}\big[f\frac{1+\sqrt{-3}}{2}\big]$ for some $f \in \mathbb{N}$. If $f \neq 1$, then $\frac{1\pm\sqrt{-3}}{2}\mathcal{O} \in \ker(C(\mathcal{O}) \to C_K)$. The Cartier group homomorphism is not injective.

From Theorem 2.7, the corollary follows (see [R2, Corollary 2.1]).

COROLLARY 2.9. *Let K be a number field and let $\mathcal{O}$ be an order in K. Then $\mathcal{O}$ is the maximal order if and only if*

(1) *$C(\mathcal{O})$ is a torsion-free group.*
(2) *$U_K \subseteq \mathcal{O}$.*

3. Witt ring. There is a natural homomorphism $W\mathcal{O} \to WK$ between the Witt rings of $\mathcal{O}$ and K defined in the following way. If M is a finitely generated projective $\mathcal{O}$-module, $\alpha\colon M \times M \to \mathcal{O}$ is a nonsingular bilinear form on M and $\langle (M,\alpha)\rangle \in W\mathcal{O}$ is the similarity class of the inner product space (M,α), then

$$\langle (M,\alpha)\rangle \mapsto \langle (N,\beta)\rangle,$$

where $N = K \otimes_{\mathcal{O}} M$ and $\beta\colon N \times N \to K$ is a nonsingular bilinear form on N defined by

$$\beta(a \otimes m, b \otimes n) = ab\alpha(m,n) \quad \text{for all } a, b \in K,\ m, n \in M.$$

In the case when $\mathcal{O} = R_K$ is the maximal order, the natural homomorphism $WR_K \to WK$ is injective (cf. [K, Satz 11.1.1]).

In [CS1, CS2], Ciemała and Szymiczek examined the kernel of $W\mathcal{O} \to WK$. They proved that if $\mathcal{O}$ is not maximal, then the kernel of $W\mathcal{O} \to WK$ is a nilideal. Moreover, they showed that for every order $\mathcal{O} = \mathbb{Z}[fi]$, $f \neq 1$, in the field $K = \mathbb{Q}(i)$ the natural homomorphism is not injective. They formulated the conjecture that for a number field K and an order $\mathcal{O}$ in K the homomorphism $W\mathcal{O} \to WK$ is injective if and only if $\mathcal{O}$ is maximal. We know that it is not true. If $K = \mathbb{Q}(\sqrt{d})$, $d \not\equiv 1 \pmod 4$, $\mathcal{O} = \mathbb{Z}[f\sqrt{d}]$ is an order such that $2 \nmid f$ and the radical of f divides d, then the natural homomorphism $W\mathcal{O} \to WK$ is injective (cf. [R1, Theorem 2.2]). Therefore the injectivity of the natural homomorphism is not a sufficient condition for an order to be maximal. In [R2], we find equivalent conditions for the maximality of $\mathcal{O}$.

THEOREM 3.1. *Let K be a number field and let $\mathcal{O}$ be an order in K. Then $\mathcal{O}$ is the maximal order if and only if*

(1) *The natural homomorphism $W\mathcal{O} \to WK$ is injective.*
(2) *The group $C(\mathcal{O})$ does not contain a nontrivial element of odd order.*
(3) *$U_K \subseteq \mathcal{O}$.*

Proof. See [R2, proof of Theorem 5.1]. ∎

Consider the subgroup $C^2(\mathcal{O})$ of squares of the group $C(\mathcal{O})$ and the restriction $g|_{C^2(\mathcal{O})}$ of the length homomorphism $g\colon C(\mathcal{O}) \to \mathrm{Div}(\mathcal{O})$ to $C^2(\mathcal{O})$.

COROLLARY 3.2. *Let K be a number field and let $\mathcal{O}$ be an order in K. Then $\mathcal{O}$ is the maximal order if and only if*

(1) *The natural homomorphism $W\mathcal{O} \to WK$ is injective.*
(2) *The homomorphism $g|_{C^2(\mathcal{O})}$ is injective.*
(3) *$U_K \subseteq \mathcal{O}$.*

Proof. See [R2, proof of Corollary 5.1]. ∎

References

[BS] Z. Borevich, I. Shafarevich, *Number Theory*, Nauka, Moscow, 1985 (in Russian).

[CS1] M. Ciemała, K. Szymiczek, *On natural homomorphisms of Witt rings*, Proc. Amer. Math. Soc. 133 (2005), 2519–2523.

[CS2] M. Ciemała, K. Szymiczek, *On injectivity of natural homomorphisms of Witt rings*, Ann. Math. Sil. 21 (2007), 15–30.

[E] D. Eisenbud, *Commutative Algebra. With a View Toward Algebraic Geometry*, Grad. Texts in Math. 150, Springer, New York, 1999.

[K] M. Knebusch, *Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen*, S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl. 1969/1970, 93–157.

[N] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, Berlin, 1999.

[R1] B. Rothkegel, *Witt functor of a quadratic order*, Math. Slovaca 68 (2018), 1339–1342.

[R2] B. Rothkegel, *Maximality of orders in Dedekind domains*, J. Algebra Appl. 19 (2020), 2050125.