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 $\mathcal{O}$:

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

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,

$$\mathcal{O} = \begin{cases} \mathbb{Z}[f\sqrt{d}] & \text{when } d \not\equiv 1 \pmod{4}, \\ \mathbb{Z}\left[f\frac{1+\sqrt{d}}{2}\right] & \text{when } d \equiv 1 \pmod{4}. \end{cases}$$
for some \( f \in \mathbb{N} \) (cf. [BS, p. 151]). The conductor of \( \mathcal{O} \) is a principal ideal generated by \( f \); \( f = fR_K \).

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 \( \text{Spec}(\mathcal{O}), \text{Pic}(\mathcal{O}) \) and \( \text{cl} \, I \) 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 \( \text{Pic}(\mathcal{O}) \), respectively.

The group \( \text{Pic}(\mathcal{O}) \) 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 \( \text{Pic}(R_K) \) is the ideal class group \( \text{Cl}_K \) of \( K \). We write \( h_K \) for the class number \( \#\text{Cl}_K \).

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 \( \text{Pic}(\mathcal{O}) \to \text{Cl}_K \) defined by

\[
\text{cl} \, I \mapsto \text{cl}(IR_K) \quad \text{for all } \text{cl} \, I \in \text{Pic}(\mathcal{O}).
\]

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

Since the group \( \text{Pic}(R_K) \) 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) \( \#\text{Pic}(\mathcal{O}) = h_K \).
(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 \( \mathcal{O} = \mathbb{Z}\left[f + \frac{1 + \sqrt{-d}}{2}\right] \) for some \( f \in \mathbb{N} \).

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

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

\#
\text{Pic}(\mathcal{O}) = h_K \frac{\#U(R_K/f)}{\#U(\mathcal{O}/f)}.
\]

We show that \( \#\text{Pic}(\mathcal{O}) \neq h_K \).
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
\[(\sqrt{d} + f)(\sqrt{d}x + f) = 1 + f\]
and $\sqrt{d} + f \in U(R_K/f) \setminus U(\mathcal{O}/f)$.

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 $\gcd\left(1 - \frac{f^2}{p^2}d, f\right) = 1$. Then $\left(1 - \frac{f^2}{p^2}d\right)x + fy = 1$ for some $x, y \in \mathbb{Z}$ and
\[\left[\left(1 + \frac{f}{p}\sqrt{d}\right) + f\right]\left[\left(1 - \frac{f}{p}\sqrt{d}\right)x + f\right] = 1 + f.\]
Moreover, $(1 + \frac{f}{p}\sqrt{d}) + f \in U(R_K/f) \setminus U(\mathcal{O}/f)$.

Assume $f = 2$. Since $d \equiv 5 \pmod{8}$, the integer $\frac{1 - d}{4}$ is odd and $\gcd\left(\frac{1 - d}{4}, f\right) = 1$. Similarly as above, there exist $x, y \in \mathbb{Z}$ such that $\frac{1 - d}{4}x + fy = 1$. Hence
\[\left(1 + \frac{\sqrt{d}}{2} + f\right)\left(1 - \frac{\sqrt{d}}{2}x + f\right) = 1 + f\]
and $\frac{1 + \sqrt{d}}{2} + f \in U(R_K/f) \setminus U(\mathcal{O}/f)$.

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

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 $\text{Div}(\mathcal{O})$ 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 $\mathcal{O}$, $p \in \text{Spec}(\mathcal{O})$ be a maximal ideal and $I_p$ be the localization of $I$ at $p$. Moreover, let $\text{length}(\mathcal{O}_p/I_p)$ denotes the length of the ring $\mathcal{O}_p/I_p$.

From [E, Theorem 11.10 and its proof], it follows that $\text{length}(\mathcal{O}_p/I_p) < \infty$ and there is a group homomorphism $g: C(\mathcal{O}) \to \text{Div}(\mathcal{O})$ defined by
\[g(I) = \sum_{p \in \text{Spec}(\mathcal{O})} \text{length}(\mathcal{O}_p/I_p) \cdot p\]
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 $\mathcal{O} = \mathbb{Z}[f \frac{1 + \sqrt{-3}}{2}]$ for some $1 \neq f \in \mathbb{N}$. Then $\pm \frac{1 + \sqrt{-3}}{2} \notin \mathcal{O}$, so $\frac{1 + \sqrt{-3}}{2} \mathcal{O} \neq \mathcal{O}$. Since $\frac{1 + \sqrt{-3}}{2} R_K = R_K$, by [R2, Lemma 3.1], $\frac{1 + \sqrt{-3}}{2} \mathcal{O} \in \ker g$. The length homomorphism is not injective.

Let 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 $\overline{g}: \text{Pic}(\mathcal{O}) \to \text{Chow}(\mathcal{O})$.

Similarly as the length homomorphism, the homomorphism $\overline{g}: \text{Cl}_K \to \text{Chow}(R_K)$ 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 $\overline{g}: \text{Pic}(\mathcal{O}) \to \text{Chow}(\mathcal{O})$ is an isomorphism and $U_K \subseteq \mathcal{O}$.
(3) The homomorphism $\overline{g}: \text{Pic}(\mathcal{O}) \to \text{Chow}(\mathcal{O})$ 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 $I \mapsto IR_K$ 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 $\mathcal{O} = \mathbb{Z}[f \frac{1 + \sqrt{-3}}{2}]$ for some $f \in \mathbb{N}$. If $f \neq 1$, then $\frac{1 + \sqrt{-3}}{2} \mathcal{O} \in \ker(C(\mathcal{O}) \to C_K)$. 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 $\text{W} \mathcal{O} \to \text{W} K$ between the Witt rings of $\mathcal{O}$ and $K$ defined in the following way. If $M$ is a finitely generated projective $\mathcal{O}$-module, $\alpha: M \times M \to \mathcal{O}$ is a nonsingular bilinear form on $M$ and $\langle (M, \alpha) \rangle \in \text{W} \mathcal{O}$ is the similarity class of the inner product space $(M, \alpha)$, then

$\langle (M, \alpha) \rangle \mapsto \langle (N, \beta) \rangle,$
where $N = K \otimes O M$ and $\beta: N \times N \to K$ 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 $O = R_K$ 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 $W O \to WK$. They proved that if $O$ is not maximal, then the kernel of $W O \to WK$ is a nilideal. Moreover, they showed that for every order $O = \mathbb{Z}[f i], f \neq 1$, 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 $O$ in $K$ the homomorphism $W O \to WK$ is injective if and only if $O$ is maximal. We know that it is not true. If $K = \mathbb{Q}(\sqrt{d}), d \not\equiv 1 \pmod{4}, O = \mathbb{Z}[f \sqrt{d}]$ is an order such that $2 \nmid f$ and the radical of $f$ divides $d$, then the natural homomorphism $W O \to WK$ 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 $O$.

**Theorem 3.1.** Let $K$ be a number field and let $O$ be an order in $K$. Then $O$ is the maximal order if and only if

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

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

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

**Corollary 3.2.** Let $K$ be a number field and let $O$ be an order in $K$. Then $O$ is the maximal order if and only if

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

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

**References**


