MAXIMAL AND NON-MAXIMAL ORDERS

LUKE WOLCOTT

Abstract. In this paper we compare and contrast various properties of maximal and non-maximal orders in the ring of integers of a number field.

1. Introduction

Let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. An *order* in K is a subring $R \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/R$ is finite as a quotient of abelian groups. From this definition, it's clear that there is a unique maximal order, namely $\mathcal{O}_K$. There are many properties that all orders in K share, but there are also differences. The main difference between a non-maximal order and the maximal order is that $\mathcal{O}_K$ is integrally closed, but every non-maximal order is not. The result is that many of the nice properties of Dedekind domains do not hold in arbitrary orders. First we describe properties common to both maximal and non-maximal orders. In doing so, some useful results and constructions given in class for $\mathcal{O}_K$ are generalized to arbitrary orders. Then we describe a few important differences between maximal and non-maximal orders, and give proofs or counterexamples. Several proofs covered in lecture or the text will not be reproduced here. Throughout, all rings are commutative with unity.

2. Common Properties

Proposition 2.1. *The ring of integers $\mathcal{O}_K$ of a number field K is a Noetherian ring, a finitely generated $\mathbb{Z}$-algebra, and a free abelian group of rank $n = [K : \mathbb{Q}]$.*

Proof: In class we showed that $\mathcal{O}_K$ is a free abelian group of rank $n = [K : \mathbb{Q}]$, and is a ring. Since $\mathbb{Z}$ is Noetherian, any $\mathbb{Z}$-module is Noetherian if and only if it is finitely generated. Because $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module, it is a Noetherian $\mathbb{Z}$-module. Since

Date: December 6, 2007.
Final Project, Math 581F, Autumn 2007.

$1 \in \mathcal{O}_K$, we have $\mathbb{Z} \subseteq \mathcal{O}_K$, so $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-algebra. Since $\mathbb{Z}$ is a Noetherian ring, the Hilbert Basis Theorem implies that the polynomial ring in n indeterminants $\mathbb{Z}[x_1, ..., x_n]$ is a Noetherian ring. Because $\mathcal{O}_K$ is the image of the surjective ring homomorphism $\mathbb{Z}[x_1, ..., x_n] \twoheadrightarrow \mathcal{O}_K$ sending the x_i to the generators, it is a Noetherian ring. ♦

Proposition 2.2. *Every order $R \subseteq \mathcal{O}_K$ is a Noetherian ring, a finitely generated $\mathbb{Z}$-algebra, and a free abelian group of rank $n = [K : \mathbb{Q}]$.*

Proof: By definition R is a subring of $\mathcal{O}_K$. Since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module and $\mathbb{Z}$ is Noetherian, as a $\mathbb{Z}$-submodule R is finitely generated. Hence R is a Noetherian $\mathbb{Z}$-module, and since $\mathbb{Z} \subseteq R$ it is a finitely generated $\mathbb{Z}$-algebra. The Hilbert Basis Theorem implies that R is a Noetherian ring. Every subgroup of a free abelian group is free. Since $\mathcal{O}_K/R$ is finite, the ranks of $\mathcal{O}_K$ and R are the same. ♦

As finitely generated $\mathbb{Z}$-algebras, we can write every order in the form $\mathbb{Z}[b_1, ..., b_k]$. The following result is useful in finding all the orders in a field.

Proposition 2.3. *Let $R \subseteq \mathcal{O}_K$ be an arbitrary order. There exist generators $a_1, ..., a_k \in K$ and integers $n_1, ..., n_k \in \mathbb{Z}\setminus\{0\}$, satisfying the property $n_1|n_2|\cdots|n_k$, such that*

$$\mathcal{O}_K = \mathbb{Z}[a_1, ..., a_k], \text{ and } R = \mathbb{Z}[n_1a_1, ..., n_ka_k].$$

Proof: Suppose $\{1, \alpha_1, ..., \alpha_k\}$ and $\{1, \beta_1, ..., \beta_k\}$ are $\mathbb{Z}$-bases for $\mathcal{O}_K$ and R, respectively, with $k+1 = [K : \mathbb{Q}]$. The natural map $\phi : \mathcal{O}_K \to R$ given by $1 \mapsto 1$ and $\alpha_i \mapsto \beta_i$ can be represented by an $n \times n$ matrix in $\mathbb{Z}$. Using Smith Normal Form, by changing bases this matrix can be made diagonal, with entries n_i satisfying $n_1|n_2|\cdots|n_k$. All the n_i are nonzero, since $\mathcal{O}_K/R$ is finite. Thus there is a basis $\{1, a_1, ..., a_k\}$ for $\mathcal{O}_K$ such that R has a basis $\{1, n_1a_1, ..., n_ka_k\}$ for some such nonzero $n_i \in \mathbb{Z}$. ♦

Note, however, that not everything of the form $\mathbb{Z}[b_1, ..., b_k]$ is an order. For example, take $K = \mathbb{Q}(\sqrt[4]{-1})$ and consider $\mathbb{Z}[i]$. We know that $\mathcal{O}_K$ is free of rank four and $\mathbb{Z}[i]$ is free of rank two. Although $\mathbb{Z}[i]$ is a Noetherian subring and finitely generated $\mathbb{Z}$-algebra, $\mathcal{O}_K/R$ has a torsion-free part so $\mathbb{Z}[i]$ is not an order. However, for the field $L = \mathbb{Q}(i)$ it's not hard to show that $\mathbb{Z}[i]$ is the maximal order in L.

As another example, consider $\mathbb{Z}[\frac{i}{2}]$. Since the minimal polynomial for $\frac{i}{2}$ is $4x^2+1$, it is not an algebraic integer. Thus for every possible field K we have $\frac{i}{2} \notin \mathcal{O}_K = K \cap \overline{\mathbb{Z}}$.

In class we showed that $\mathcal{O}_K$ may require arbitrarily many generators as a $\mathbb{Z}$-algebra. The proof of this applies verbatim to arbitrary orders $R \subseteq \mathcal{O}_K$. For example, the following code from Sage gives an order that cannot be generated by fewer than four elements of the field.

```
sage: R.<x> = QQ[]
sage: f = x^5+x^4-60*x^3-12*x^2+784*x+128
sage: K.<a> = NumberField(f)
sage: OK = K.ring_of_integers()
sage: OK_gens = OK.gens()
sage: OK_gens
[1,
5/16*a^4 + 1/16*a^3 + 1/4*a,
1/32*a^4 + 3/32*a^3 + 1/16*a^2,
1/8*a^4 + 1/8*a^3, a^4]
sage: O = K.order(OK_gens[0], 2*(OK_gens[1]),
                  OK_gens[2], OK_gens[3])
sage: O.gens()
[1,
21/16*a^4 + 1/16*a^3 + 1/4*a,
1/32*a^4 + 3/32*a^3 + 1/16*a^2,
1/8*a^4 + 1/8*a^3, 2*a^4]
```

Proposition 2.4. *Let $R \subseteq \mathcal{O}_K$ be an arbitrary order. Then $\mathbb{Q}\mathcal{O}_K = \mathbb{Q}R = K$.*

Proof: In class we showed that $\mathbb{Q}\mathcal{O}_K = K$. Since $R \subseteq \mathcal{O}_K$, it's clear that $\mathbb{Q}R \subseteq \mathbb{Q}\mathcal{O}_K$. Using Proposition 2.3, write $\mathcal{O}_K = \mathbb{Z}[a_1, ..., a_k]$ and $R = \mathbb{Z}[n_1 a_1, ..., n_k a_k]$ for some $a_i \in K$ and $n_i \in \mathbb{Z} \setminus \{0\}$. Then $a_i = \frac{1}{n_i}(n_i a_i) \in \mathbb{Q}R$ for all i, so $\mathcal{O}_K \subseteq \mathbb{Q}R$. This implies $\mathbb{Q}\mathcal{O}_K \subseteq \mathbb{Q}R$, and $\mathbb{Q}R = \mathbb{Q}\mathcal{O}_K = K$. ♦

Corollary 2.5. *Every order is a lattice.*

As a result, there are many constructions that work equally well for maximal and non-maximal orders. For example, we have the discriminant of an arbitrary order, and the volume of its lattice. For an ideal of an arbitrary order, $I \subseteq R$, we can define the *norm of I in R* to be the lattice index $[R : I]$.

Proposition 2.6. *Let $R \subseteq \mathcal{O}_K$ be an arbitrary order. Then $Frac(R) = Frac(\mathcal{O}_K) = K$, where $Frac$ denotes the field of fractions of a ring.*

Proof: For any $x \in K = \mathbb{Q}R$, we have $x = qy$ for some $q \in \mathbb{Q}$ and $y \in R$. Write $q = \frac{a}{b}$, with $a, b \in \mathbb{Z}$ and $b \neq 0$. Then $a \in \mathbb{Z} \subseteq R$, so $ay \in R$. Since $b \in \mathbb{Z} \subseteq R$ and $b \neq 0$, we have $x = \frac{ay}{b} \in Frac(R)$, so $K \subseteq Frac(R)$.

Conversely, take $x \in Frac(R)$. Then $x = \frac{a}{b}$ for $a, b \in R \subseteq K$, with $b \neq 0$. Thus $x = \frac{a}{b} \in K$. This shows that $Frac(R) \subseteq K$, and $Frac(R) = K$. ♦

Recall that an integral domain D is called *integrally closed* if whenever $\alpha \in Frac(D)$ satisfies a monic polynomial in $D[x]$, then $\alpha \in D$. A *Dedekind domain* is an integral domain that is Noetherian and integrally closed, such that every nonzero prime ideal is maximal.

Proposition 2.7. *Let $R \subseteq \mathcal{O}_K$ be an arbitrary order. Then R is an integral domain that is Noetherian, such that every nonzero prime ideal is maximal.*

Proof: Since $R \subseteq K$, it is an integral domain. We showed in Proposition 2.2 that R is Noetherian. Suppose $\mathfrak{p} \subseteq R \subseteq \mathcal{O}_K$ is a nonzero prime ideal, and let $a \in \mathfrak{p}$ be a nonzero element. Let $f(x) \in \mathbb{Z}[x]$ be the monic minimal polynomial of a. Then for some $c_i \in \mathbb{Z}$ we can write $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, and $c_0 \neq 0$ since f is minimal. Thus we have

$$0 = f(a) = a^n + c_{n-1}a^{n-1} + \cdots + c_1a + c_0, \text{ and}$$
$$a^n + c_{n-1}a^{n-1} + \cdots + c_1a = -c_0.$$

This shows that $-c_0 \in \mathfrak{p}$. The quotient $\mathcal{O}_K/\mathfrak{p}$ is a finitely generated $\mathbb{Z}$-module such that $c_0(\mathcal{O}_K/\mathfrak{p}) = 0$, so $\mathcal{O}_K/\mathfrak{p}$ is a finite abelian group. Since $\mathfrak{p}$ is prime, $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Since every finite integral domain is a field, $\mathfrak{p}$ must be maximal. ♦

3. Differences

Proposition 3.1. *The maximal order $\mathcal{O}_K$ is integrally closed, and thus is a Dedekind domain.*

Proof: Take $\alpha \in Frac(\mathcal{O}_K) = K$ such that α satisfies a monic polynomial in $\mathcal{O}_K[x]$. For a fixed choice of algebraic closure, we can embed $K \hookrightarrow \overline{\mathbb{Q}}$ and $\mathcal{O}_K \hookrightarrow \overline{\mathbb{Z}}$. Thus $\alpha \in \overline{\mathbb{Q}} = Frac(\overline{\mathbb{Z}})$, and satisfies a monic polynomial $f(x) \in \overline{\mathbb{Z}}[x]$. Because $\overline{\mathbb{Z}}$ is integrally closed, this

implies that $\alpha \in \overline{\mathbb{Z}}$. Therefore $\alpha \in K \cap \overline{\mathbb{Z}} = \mathcal{O}_K$, proving that $\mathcal{O}_K$ is integrally closed. Combining this with Proposition 2.7, we get that $\mathcal{O}_K$ is a Dedekind domain. ♦

Proposition 3.2. *Let $R \subsetneq \mathcal{O}_K$ be a non-maximal order. Then R is not integrally closed, and therefore is not a Dedekind domain.*

Proof: Because $R \subsetneq \mathcal{O}_K$, there is some $\beta \in \mathcal{O}_K$, $\beta \notin R$. Note that $\beta \in \mathcal{O}_K \subseteq Frac(\mathcal{O}_K) = Frac(R)$. Since β is an algebraic integer, it satisfies a monic polynomial $g(x) \in \mathbb{Z}[x] \subseteq R[x]$. That $\beta \notin R$ shows that R is not integrally closed. ♦

Given a (Noetherian) ring R, the ideals of R are the (finitely generated) R-modules contained in R. We generalize this notion to that of a *fractional ideal*, a finitely generated nonzero R-module contained in $Frac(R)$. In class we defined fractional ideals only for Dedekind domains such as $\mathcal{O}_K$, but the definition can be applied to arbitrary orders. The reason we looked only at fractional ideals in Dedekind domains is in that case we could prove the following nice result.

Proposition 3.3. *The set of fractional ideals in a Dedekind domain (e.g the maximal order $\mathcal{O}_K$) form an abelian group under ideal multiplication.*

However, non-maximal orders are not Dedekind domains, so we have the following.

Proposition 3.4. *There exists a field K with a non-maximal order $R \subsetneq \mathcal{O}_K$ such that not every fractional ideal of R has an inverse, so the set of fractional ideals of R does not form a group.*

Proof: In fact, it can be shown ([2]), using Discrete Valuation Rings, that a ring is a Dedekind domain if and only if every nonzero fractional ideal is invertible. Thus every non-maximal order has a fractional ideal that is not invertible. Here we give one example.

Suppose I is a fractional ideal of an order R, and define

$$J = \{\alpha \in Frac(R) \ : \ \alpha I \subseteq R\}.$$

Then if I is invertible, we must have $I^{-1} = J$. To see this, suppose I is invertible, and $AI = R$ for some fractional ideal A. Then $A \subseteq J$ by definition of J. Therefore we have $R = AI \subseteq JI \subseteq R$, which implies $JI = R$.

Let $K = \mathbb{Q}(\sqrt{34})$, and note that $34 \equiv 2(\text{mod } 4)$ implies $\mathcal{O}_K = \mathbb{Z}[\sqrt{34}]$. Consider the order $R = \mathbb{Z}[3\sqrt{34}] \subsetneq \mathcal{O}_K$.

For $\alpha, \beta \in K$, let $[\alpha, \beta]$ denote the free abelian group $\alpha\mathbb{Z} \oplus \beta\mathbb{Z}$. It can be shown ([5]) that for an arbitrary order R in a quadratic field, with $a, b + c\sqrt{D} \in R$, the group $[a, b + c\sqrt{D}]$ is an ideal of R if and only if the following hold: $c|a, c|b$, and $ac|Norm(b + c\sqrt{D})$.

Therefore we have an ideal $I = [9, 15 + 3\sqrt{34}] \subseteq R$. A computation shows that $J = \{\alpha \in Frac(R) : \alpha I \subseteq R\} = \left(\frac{1}{9}\right)[9, 15 - 3\sqrt{34}]$. As noted above, if I is invertible then $I^{-1} = J$. But another computation shows that $IJ = [3, 3\sqrt{34}] \neq R$. Thus the ideal I is not invertible. ♦

It is the case that every nonzero principal fractional ideal is invertible. To see this, let $(a) = I$ be a nonzero principal fractional ideal of an arbitrary order $R = \mathbb{Z}[a_1, ..., a_k]$. Then $I = a\mathbb{Z}[a_1, ..., a_k]$, and it's clear that $J = \frac{1}{a}\mathbb{Z}[a_1, ..., a_k]$ is a finitely generated R-module contained in $Frac(R)$, with $IJ = R$.

For an order $R \subseteq \mathcal{O}_K$, let $\mathcal{I}(R)$ be the set of nonzero invertible fractional ideals. Then $\mathcal{I}(R)$ does form an abelian group under ideal multiplication. Because of this, we can generalize our definition of the class group to arbitrary orders. Let $\mathcal{P}(R)$ be the set of nonzero principal fractional ideals. Then $\mathcal{P}(R)$ is a subgroup of $\mathcal{I}(R)$, and we can define the *class group of* R to be the quotient group $\mathcal{I}(R)/\mathcal{P}(R)$.

In this way, much of the theory of the class group can be extended and generalized.

The following important result for maximal orders, proved in class, does not carry over to non-maximal orders.

Proposition 3.5. *In a Dedekind domain (e.g. the maximal order $\mathcal{O}_K$), every nonzero ideal factors uniquely into a product of prime ideals.*

Proposition 3.6. *Let $R \subsetneq \mathcal{O}_K$ be a non-maximal order. Then in general, unique factorization of nonzero ideals into prime ideals fails.*

Proof: We will use the fact, noted above and proved in [2], that R is a Dedekind domain if and only if every fractional ideal is invertible.

Suppose to the contrary that R is such that every fractional ideal factors uniquely into a product of prime ideals. If I is a fractional ideal, we can write $I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n$ for some prime ideals $\mathfrak{p}_i$.

Next we show that in this case every nonzero prime ideal is invertible. If $\mathfrak{p}$ is a prime ideal, let $a \in \mathfrak{p}$ be some nonzero element. By assumption, $(a) = \mathfrak{q}_1 \cdots \mathfrak{q}_k$ for some prime ideals $\mathfrak{q}_i$. Then $\mathfrak{q}_1(\frac{1}{a}\mathfrak{q}_2 \cdots \mathfrak{q}_k) = R$, so $\mathfrak{q}_1$

is invertible, and similarly each $\mathfrak{q}_i$ is invertible, with

$$\mathfrak{q}_i^{-1} = \frac{1}{a}\mathfrak{q}_1 \cdots \mathfrak{q}_{i-1}\mathfrak{q}_{i+1} \cdots \mathfrak{q}_k.$$

Now $\mathfrak{q}_1 \cdots \mathfrak{q}_k = (a) \subseteq \mathfrak{p}$. If for all i we have $\mathfrak{q}_i \nsubseteq \mathfrak{p}$, then there are elements $c_i \in \mathfrak{q}_i$, $c_i \notin \mathfrak{p}$, such that $c_1 c_2 \cdots c_k \in \mathfrak{p}$. But $\mathfrak{p}$ is a prime ideal, so this is not possible. Therefore, for some i we have $\mathfrak{q}_i \subseteq \mathfrak{p}$. Since every nonzero prime ideal is maximal, we must have $\mathfrak{q}_i = \mathfrak{p}$. Thus $\mathfrak{p}$ is invertible.

Since every prime ideal is invertible, we have $I^{-1} = \mathfrak{p}_n^{-1} \cdots \mathfrak{p}_2^{-1}\mathfrak{p}_1^{-1}$. This implies that every fractional ideal is invertible, so R is a Dedekind domain. This contradicts the fact that the non-maximal orders are not Dedekind domains. Therefore unique factorization must fail in non-maximal orders. ♦

Unique factorization of ideals in $\mathcal{O}_K$ allowed us to prove the following result on ideals in $\mathcal{O}_K$, which does not apply to arbitrary orders.

Proposition 3.7. *Any ideal $I \subseteq \mathcal{O}_K$ is generated as a ring by one or two elements.*

Proposition 3.8. *There exists a field K with a non-maximal order $R \subsetneq \mathcal{O}_K$, and an ideal $J \subset R$ such that J requires more than two generators.*

Proof: Let $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2})$, and consider the subring

$$R = \mathbb{Z}[\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}] \subseteq \mathcal{O}_K.$$

Note that $[K : \mathbb{Q}] = 30$, and write $\alpha = \sqrt{2}$, $\beta = \sqrt[3]{2}$, and $\gamma = \sqrt[5]{2}$. The set $\left\{\alpha^a\beta^b\gamma^c \ : \ a = 0, 1;\ b = 0, 1, 2;\ c = 0, 1, 2, 3, 4\right\}$ is a $\mathbb{Z}$-basis for R and has 30 distinct linearly independent elements, as can be verified by computing all the elements via

$$\alpha^a\beta^b\gamma^c = 2^{\frac{15a}{30}} 2^{\frac{10b}{30}} 2^{\frac{6c}{30}} = 2^{\frac{15a+10b+6c}{30}}.$$

Therefore R is free abelian of rank 30, so $\mathcal{O}_K/R$ is finite and R is in fact an order.

Now consider the ideal $I = (\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}) \subseteq R$. Suppose to the contrary that $I = (a, b)$ for some $a, b \in R$. Write $a = a_0 + a_1 2^{15/30} + a_2 2^{10/30} + a_3 2^{6/30}$ and $b = b_0 + b_1 2^{15/30} + b_2 2^{10/30} + b_3 2^{6/30}$, for some $a_i, b_i \in \mathbb{Z}$. Then $2^{6/30} \in I$ implies there exist $r_1, r_2 \in R$ such that $2^{6/30} = r_1 a + r_2 b$. A little thought shows that this is only possible if either a or b is $2^{6/30}$, since by multiplying and distributing fractional

powers of two all the exponents will only increase. Without loss of generality, we have $a = 2^{6/30}$.

Likewise, the fact that $2^{10/30} \in I$ implies there are $r_1, r_2 \in R$ such that $2^{10/30} = r_1 2^{6/30} + r_2 b$. But this is only possible if $b = 2^{10/30}$. Thus we have $I = (2^{6/30}, 2^{10/30})$. However, $2^{15/30} = r_1 2^{6/30} + r_2 2^{10/30}$ has no solutions $r_1, r_2 \in R$, so $2^{15/30} \notin I$, a contradiction. This shows that the ideal $I = (\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2})$ requires at least three ring generators. ♦

4. Conclusion and Questions

These are a few of the major differences between maximal and non-maximal orders. Clearly, most of the differences result from the fact that maximal orders are always Dedekind domains and non-maximal domains are never. However, many constructions originally given for rings of integers, such as the class group, can be extended to the case of arbitrary orders.

At first it seems every non-maximal order has a similar structure, but perhaps its possible to study them further. For example, what does the group of invertible fractional ideals $\mathcal{I}(R)$ tell us about a non-maximal order? How do the generalized class groups of arbitrary orders compare to each other, and what do they tell us about the class group $Cl(K)$?

We could look at orders of orders, and there may be interesting structure there, particularly as they relate geometrically to real lattices. Finally, each non-maximal order, while not integrally closed, does have an integral closure contained in the ring of integers. Perhaps it would be interesting to study the interplay between non-maximal orders, their integral closures, and the maximal order.

On a practical note, Sage currently doesn't have much computational functionality with non-maximal orders. Implementing this would do much towards elucidating the relationship between maximal and non-maximal orders.

References

[1] W. Stein, *Algebraic Number Theory, A Computational Approach*, http://wiki.wstein.org, 2007.
[2] D.S.Dummit, R.M.Foote, *Abstract Algebra*, Prentice Hall, 1999.
[3] P. Stevenhagen, *The Arithmetic of Number Rings*, *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, Cambridge University Press, 2006.
[4] I.N.Stewart, *Algebraic Number Theory*, Chapman and Hall, 1987.
[5] R. Mollin, *Quadratics*, CRC Press, 1996.