Math 210B. Quadratic integer rings

1. Computing the integral closure of $\mathbf{Z}$

Let $d \in \mathbf{Z} - \{0,1\}$ be *squarefree*, and $K = \mathbf{Q}(\sqrt{d})$. In this handout, we aim to compute the integral closure $\mathscr{O}_K$ of $\mathbf{Z}$ in K (called the *ring of integers* of K). Clearly $\sqrt{d} \in \mathscr{O}_K$ (it is a root of $X^2 - d$), so $\mathbf{Z}[\sqrt{d}] \subset \mathscr{O}_K$. We'll see that in many cases this inclusion is an equality, and that otherwise it is an index-2 inclusion.

The key to controlling the possibilities for $\alpha \in \mathscr{O}_K$ is to use the fact that (writing $z \mapsto \overline{z}$ to denote the non-trivial automorphism of the Galois extension $K/\mathbf{Q}$) both rational numbers

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = \alpha + \overline{\alpha},\ \ \mathrm{N}_{K/\mathbf{Q}}(\alpha) = \alpha\overline{\alpha}$$

are algebraic integers and thus belong to $\mathbf{Z}$ (as we know that any UFD, such as $\mathbf{Z}$, is integrally closed in its own fraction field, and so the only algebraic integers in $\mathbf{Q}$ are the elements of $\mathbf{Z}$). Writing $\alpha = a + b\sqrt{d}$ for unique $a, b \in \mathbf{Q}$, we have $\overline{\alpha} = a - b\sqrt{d}$, so $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = 2a$ and $\mathrm{N}_{K/\mathbf{Q}}(\alpha) = a^2 - db^2$. Thus, we arrive at the *necessary* conditions $2a, a^2 - db^2 \in \mathbf{Z}$. This already imposes a severe constraint on the denominator of a when written as a reduced-form fraction: it is either 1 or 2.

Theorem 1.1. *If $d \equiv 2, 3 \bmod 4$ then $\mathscr{O}_K = \mathbf{Z}[\sqrt{d}]$, and if $d \equiv 1 \bmod 4$ then $\mathscr{O}_K = \mathbf{Z}[(1+\sqrt{d})/2]$.*

Note that the case $d \equiv 0 \bmod 4$ cannot occur since d is square-free. Although $K = \mathbf{Q}(\sqrt{d})$ is not affected if we replace d with $n^2 d$ for $n \in \mathbf{Z}^+$ (since $n \in \mathbf{Q}^\times$), the rings $\mathbf{Z}[\sqrt{d}]$ and $\mathbf{Z}[\sqrt{n^2 d}] = \mathbf{Z}[n\sqrt{d}]$ are very different. Thus, the square-free hypothesis on d that is not so essential for describing K is absolutely critical for the correctness of the description of $\mathscr{O}_K$ in terms of d in the Theorem.

As illustrations, for $K = \mathbf{Q}(i), \mathbf{Q}(\sqrt{\pm 2}), \mathbf{Q}(\sqrt{3}), \mathbf{Q}(\sqrt{-5})$ we have $\mathscr{O}_K = \mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{\pm 2}]$, $\mathbf{Z}[\sqrt{3}]$, $\mathbf{Z}[\sqrt{-5}]$ respectively and for $K = \mathbf{Q}(\sqrt{-3}), \mathbf{Q}(\sqrt{5})$ we have $\mathscr{O}_K = \mathbf{Z}[\omega], \mathbf{Z}[(1+\sqrt{5})/2]$ (where $\omega = (-1+\sqrt{-3})/2$ is a nontrivial cube root of 1, which is to say a root of $(X^3-1)/(X-1) = X^2+X+1$).

Proof. We have already noted that if $a \notin \mathbf{Z}$ then as a reduced-form fraction the denominator of a has no other option than to be 2; i.e., in the latter case $a = n/2$ for an odd integer n.

Let's see how the two possibilities ($a \in \mathbf{Z}$, or $a = n/2$ for odd $n \in \mathbf{Z}$) arising from the necessity of integrality of the trace interact with the necessity of integrality of the norm. Since $a^2 - db^2 \in \mathbf{Z}$, in case $a \in \mathbf{Z}$ we see that $db^2 \in \mathbf{Z}$. But d is *square-free*, so integrality of db^2 rules out the possibility of any prime p occurring in the denominator of b as a reduced-form fraction (since d cannot fully cancel the denominator factor p^2 for b^2). Thus, when $a \in \mathbf{Z}$ we conclude that necessarily $b \in \mathbf{Z}$, so $\alpha = a + b\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$. Hence, the only way it could happen that $\mathscr{O}_K$ is larger than $\mathbf{Z}[\sqrt{d}]$ is from cases with $a \notin \mathbf{Z}$ (if these can somehow manage to occur for some $\alpha \in \mathscr{O}_K$).

So suppose $a = n/2$ with odd $n \in \mathbf{Z}$. Thus, $a^2 - db^2 = n^2/4 - db^2$ is an integer. This forces db^2 to have a denominator of 4 when written in reduced form, so necessarily $b = m/2$ for some odd integer m and also d is odd (since if d is even then $db^2 = dm^2/4$ would have denominator at worst 2). This already settles the case of even d, which is to say $d \equiv 2 \bmod 4$. We can write

$$\alpha = a + b\sqrt{d} = \frac{1+\sqrt{d}}{2} + \left(\frac{n-1}{2} + \frac{m-1}{2} \cdot \sqrt{d}\right)$$

with $(n-1)/2, (m-1)/2 \in \mathbf{Z}$. Hence, integrality of α is equivalent to that of $(1+\sqrt{d})/2$!

The trace and norm of $(1+\sqrt{d})/2$ down to $\mathbf{Q}$ are 1 and $(1-d)/4$ respectively, so a necessary condition for $(1+\sqrt{d})/2$ to be integral over $\mathbf{Z}$ is that $d \equiv 1 \bmod 4$. This is also sufficient, since its minimal polynomial over $\mathbf{Q}$ is $X^2 - X + (1-d)/4$. Thus, if $d \equiv 3 \bmod 4$ then $\mathscr{O}_K = \mathbf{Z}[\sqrt{d}]$ whereas if $d \equiv 1 \bmod 4$ then $\mathscr{O}_K$ is generated over $\mathbf{Z}[\sqrt{d}]$ by $\rho := (1+\sqrt{d})/2$. But in such cases we have $2\rho - 1 = \sqrt{d}$ and so $\mathbf{Z}[\sqrt{d}] \subset \mathbf{Z}[\rho]$. Thus, $\mathscr{O}_K = \mathbf{Z}[\rho]$ if $d \equiv 1 \bmod 4$. ■

Remark 1.2. In case $d \equiv 1 \bmod 4$, elements of $\mathbf{Z}[(1+\sqrt{d})/2]$ have the form

$$n + m(1+\sqrt{d})/2 = ((m+2n) + m\sqrt{d})/2$$

for $n, m \in \mathbf{Z}$. This is $(a_0 + a_1\sqrt{d})/2$ for $a_0, a_1 \in \mathbf{Z}$ having the same parity: either elements of $\mathbf{Z}[\sqrt{d}]$ (for a_0, a_1 even) or $q_0 + q_1\sqrt{2}$ where each q_j is half an odd integer (for a_0, a_1 odd).

2. Subtleties of integral closure

Already with quadratic integer rings one can begin to see some ring-theoretic subtleties emerge. As a basic example, one might wonder: for a finite extension K of $\mathbf{Q}$, is $\mathscr{O}_K$ a PID (as $\mathbf{Z}$ is)? No! Already in the quadratic case this breaks down, as the following examples show.

Example 2.1. Let $K = \mathbf{Q}(\sqrt{-5})$, so $\mathscr{O}_K = \mathbf{Z}[\sqrt{-5}]$. We claim that $\mathscr{O}_K$ is not a PID; we will show it is not even a UFD (so it cannot be a PID). First, we need to get a handle on the possible units in $\mathscr{O}_K$ (since the UFD condition involves unique factorization into irreducible elements up to unit-scaling).

We saw in class that if A is an integrally closed domain with fraction field F and F'/F is a finite separable extension in which the integral closure of A is denoted A' then $\mathrm{Tr}_{F'/F}$ carries A' into A. The exact same argument applies to norm in place of trace, so we have the norm map $\mathrm{N}_{F'/F} : A' \to A$ that is *multiplicative* and carries 1 to 1, so it carries $A'^{\times}$ into $A^{\times}$ (i.e., if $u', v' \in A'$ satisfy $u'v' = 1$ then $\mathrm{N}_{F'/F}(u'), \mathrm{N}_{F'/F}(v') \in A$ have product equal to $\mathrm{N}_{F'/F}(u'v') = \mathrm{N}_{F'/F}(1) = 1$, so $\mathrm{N}_{F'/F}(u') \in A^{\times}$). We conclude that for *any* quadratic extension $L/\mathbf{Q}$, $\mathrm{N}_{L/\mathbf{Q}}(\mathscr{O}_L^{\times}) \subset \mathbf{Z}^{\times} = \{\pm 1\}$. Conversely, if $\alpha \in \mathscr{O}_L$ satisfies $\mathrm{N}_{L/\mathbf{Q}}(\alpha) = \pm 1$ then α is a unit: if $z \mapsto \overline{z}$ denotes the nontrivial automorphism of L then $\mathrm{N}_{L/\mathbf{Q}}(\alpha) = \alpha\overline{\alpha}$, so if $\mathrm{N}_{L/\mathbf{Q}}(\alpha) = \pm 1$ then $1/\alpha = \pm\overline{\alpha} \in \mathscr{O}_L$, so $\alpha \in \mathscr{O}_L^{\times}$.

Coming back to $K = \mathbf{Q}(\sqrt{-5})$, an element of $\mathscr{O}_K$ has the form $\alpha = a + b\sqrt{-5}$ for $a, b \in \mathbf{Z}$, so its norm is $a^2 + 5b^2$. The only solutions to $a^2 + 5b^2 = \pm 1$ in $\mathbf{Z}$ are $(a, b) = (\pm 1, 0)$, so $\alpha = \pm 1$. Thus, $\mathscr{O}_K^{\times} = \{\pm 1\}$. (The situation is very different for "real quadratic fields"; e.g., $1 + \sqrt{2} \in \mathbf{Z}[\sqrt{2}]^{\times}$, with reciprocal $-1 + \sqrt{2}$; the general structure of unit groups of rings of integers of number fields is a key part of classical algebraic number theory, beyond the scope of this course.) Now consider the factorization

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

These two factorizations of 6 are genuinely different in the sense that they are not obtained from each other through unit-scaling (as $\mathscr{O}_K^{\times} = \{\pm 1\}$).

To show that this contradicts the UFD property, we first claim that $2, 3 \in \mathscr{O}_K$ are *irreducible*. Suppose $2 = xy$ with non-units $x, y \in \mathscr{O}_K$. Taking norm of both sides gives $4 = \mathrm{N}(x)\mathrm{N}(y)$ with $\mathrm{N}(x), \mathrm{N}(y) > 1$ (as x, y are non-units), so the only possibility is $\mathrm{N}(x) = 2$. But $a^2 + 5b^2 = 2$ has no solutions in $\mathbf{Z}$, so this is impossible and hence 2 is irreducible; the same argument works for 3. Since $1 \pm \sqrt{-5}$ are non-units in $\mathscr{O}_K$ (each has norm 6), and $\mathscr{O}_K^{\times} = \{\pm 1\}$, the two factorizations of 6 given above really are not related through unit scaling and so contradict the UFD property. Hence, $\mathscr{O}_K$ is not a UFD (and so is not a PID).

Example 2.2. A variant of the preceding calculations shows that the integral closure $\mathbf{Z}[\sqrt{-6}]$ of $\mathbf{Z}$ in $K = \mathbf{Q}(\sqrt{-6})$ is not a PID (nor even a UFD) due to the factorizations

$$2 \cdot 5 = 10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$$

of 10.

Later we will understand both of the preceding examples as instances of a common phenomenon related to non-principal prime ideals in Dedekind domains: the ideals $(2, 1+\sqrt{-5}) \subset \mathbf{Z}[\sqrt{-5}]$ and $(2, \sqrt{-6}) \subset \mathbf{Z}[\sqrt{-6}]$ are each non-principal prime ideals (but the non-principlaity of each is not obvious at this stage). We'll come back to these examples later, to understand the sense in which each expresses a relation among non-principal ideals analogous to elementary factorization identities such as $(ab)(cd) = (ac)(bd)$ in commutative rings.

Example 2.3. Consider a finite extension $L/\mathbf{Q}$ that is a compositum of two subfields $K, K' \subset L$ over $\mathbf{Q}$ with the property that the natural map $K \otimes_{\mathbf{Q}} K' \to L$ is an isomorphism (equivalently $[K : \mathbf{Q}][K' : \mathbf{Q}] = [L : \mathbf{Q}]$ by Exercise 4 on HW2; such K and K' are called *linearly disjoint* over $\mathbf{Q}$ inside L). One may wonder if the natural map

$$m : \mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_{K'} \to \mathscr{O}_L$$

is an isomorphism. Let's first express this in more concrete terms, and then bring up a counterexample. We know that $\mathscr{O}_K$ is a free $\mathbf{Z}$-module of finite rank inside K, and $\mathbf{Q} \otimes_{\mathbf{Z}} \mathscr{O}_K = K$ (by denominator-chasing: any $x \in K$ is the root of a monic over $\mathbf{Q}$, so Nx is the root of a monic over $\mathbf{Z}$ for sufficiently divisible non-zero $N \in \mathbf{Z}$, so $x = (Nx)/N$ comes from $(1/N) \otimes (Nx)$); we have likewise for K' in place of K. Since $\mathscr{O}_K$ is $\mathbf{Z}$-free and $\mathscr{O}_{K'}$ is $\mathbf{Z}$-free, their tensor product over $\mathbf{Z}$ is also $\mathbf{Z}$-free and hence the natural map

$$\mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_{K'} \to \mathbf{Q} \otimes_{\mathbf{Z}} (\mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_{K'}) = (\mathbf{Q} \otimes_{\mathbf{Z}} \mathscr{O}_K) \otimes_{\mathbf{Q}} (\mathbf{Q} \otimes_{\mathbf{Z}} \mathscr{O}_{K'}) = K \otimes_{\mathbf{Q}} K' = L$$

is injective. The image of this lands inside $\mathscr{O}_L$, so the question of whether or not m is an isomorphism is exactly the same as asking if $\mathscr{O}_L$ coincides with the $\mathbf{Z}$-subalgebra $\mathscr{O}_K \mathscr{O}_{K'}$ of L consisting of finite sums $\sum_i x_i x_i'$ for $x_i \in \mathscr{O}_K$ and $x_i' \in \mathscr{O}_{K'}$.

It may be tempting to think that such equality somehow follows from the given equality $KK' = L$, but it generally fails! Here is a possible obstruction: since $\mathscr{O}_{K'}$ is a free $\mathbf{Z}$-module of finite rank, likewise $\mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_{K'}$ is a free $\mathscr{O}_K$-module of finite rank. Thus, if $\mathscr{O}_L$ is *not* free as an $\mathscr{O}_K$-module then we have an obstruction to m being an isomorphism. Since $\mathscr{O}_L$ is certainly a finitely generated torsion-free $\mathscr{O}_K$-module (it is a domain containing $\mathscr{O}_K$ as a subring, and is even finitely generated as a $\mathbf{Z}$-module), the only way it could possibly happen that it is not $\mathscr{O}_K$-free is if $\mathscr{O}_K$ is not a PID. Hence, to realize this obstruction we need to at least use some K for which $\mathscr{O}_K$ is not a PID.

Consider $L = \mathbf{Q}(\sqrt{-6}, \sqrt{-3})$ with $K = \mathbf{Q}(\sqrt{-6})$, $K' = \mathbf{Q}(\sqrt{-3})$. In this case $\mathscr{O}_{K'} = \mathbf{Z}[\omega]$ turns out to be a PID (it is even Euclidean), but we saw above that $\mathscr{O}_K = \mathbf{Z}[\sqrt{-6}]$ is *not* a PID. Using techniques from algebraic number theory it can be shown that $\mathscr{O}_L$ is not a free module over $\mathscr{O}_K = \mathbf{Z}[\sqrt{-6}]$, so in this case $\mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_{K'} \subsetneq \mathscr{O}_L$. A deeper understanding of this failure of equality at the level of integral closures requires more concepts from commutative algebra that we will see later in the course.