Math 361 lecture for Monday, Week 9

The norm of an ideal

Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Recall the proof that if $\mathfrak{a}$ is a nonzero ideal of $\mathfrak{O}_K$, then $\mathfrak{O}_K/\mathfrak{a}$ is finite. Pick $0 \neq \alpha \in \mathfrak{a}$. Then we saw that $N(\alpha) \in \mathfrak{a}$, and hence the usual quotient map $\mathfrak{O}_K \to \mathfrak{O}_K/\mathfrak{a}$ induces a surjection

$$\mathfrak{O}_K/(N(\alpha)) \to \mathfrak{O}_K/\mathfrak{a}.$$

We then appeal to the structure theorem of finite abelian groups and use the fact that no element of $\mathfrak{O}_K/(N(\alpha))$ has infinite order to conclude that $\mathfrak{O}_K/(N(\alpha))$ is a finite product of finite cyclic groups, hence, finite. The surjection above then implies that $\mathfrak{O}_K/\alpha$ is also finite.

Definition 1. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. Then the *norm* of $\mathfrak{a}$ is

$$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|.$$

Example 2. Let $K = \mathbb{Q}(\sqrt{-14})$, and consider the ideal $\mathfrak{a} = (6, 1+\sqrt{-14}) \subset \mathfrak{O}_K$. Since $-14 \not\equiv 1 \bmod 4$, each element of $\mathfrak{O}_K$ has the form $a + b\sqrt{-14}$ for some $a, b \in \mathbb{Z}$. Working modulo $\mathfrak{a}$, we have

$$a + b\sqrt{-14} = (a + b\sqrt{-14}) - b(1 + \sqrt{-14l}) = (a - b) \bmod \mathfrak{a}. \tag{1}$$

Since $6 \in \mathfrak{a}$, one might be tempted to jump to the conclusion that $\mathfrak{O}_K/\mathfrak{a}$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. However, that reasoning assumes that $0, 1, 2, 3, 4, 5$ are distinct modulo $\mathfrak{a}$. The above reasoning actually says that we get a well-defined surjection

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} &\to \mathfrak{O}_K/\mathfrak{a} \\ x &\mapsto x. \end{aligned}$$

It is well-defined since $6 \in \mathfrak{a}$, and it is surjective by equation (1). The kernel of this mapping is one of the following: (0), (1), (2), or (3), since these are the only ideals of $\mathbb{Z}/6\mathbb{Z}$. If the kernel is (0), the mapping is an isomorphism. Otherwise, we will have $1, 2$ or 3 in $\mathfrak{a}$. So our problem is solved by finding the smallest positive integer in $\mathfrak{a}$.

An arbitrary element of $\mathfrak{a}$ has the form

$$\alpha = (a + b\sqrt{-14})6 + (c + d\sqrt{-14})(1 + \sqrt{-14}) = (6a + c - 14d) + (6b + c + d)\sqrt{-14}.$$

Then α is a rational integer if and only if $d = -6b - c$. In that case,

$$\alpha = 6a + c - 14d = 6a + c - 14(-6b - c) = 6a + 84b + 15c = 3(2a + 28b + 5c).$$

The possible values for $2a + 28b + 5c$ are the elements in the ideal $(2, 28, 5) = (1) = \mathbb{Z}$. So the smallest positive integer in $\mathfrak{a}$ is 3. We can get this by letting $a = -2, b = 0, c = 1$, and $d = -6b - c = -1$:

$$(-2)6 + (1 - \sqrt{-14})(1 + \sqrt{-14}) = -12 + 1 + 14 = 3.$$

Therefore,

$$\mathbb{Z}/3\mathbb{Z} \simeq \mathfrak{O}_K/\mathfrak{a},$$

and

$$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}| = 3.$$

Proposition 3. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$ and pick a $\mathbb{Z}$-module basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathfrak{a}$.[1] Then

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{1/2}$$

where Δ is the discriminant of K (i.e., the discriminant of any $\mathbb{Z}$-basis for $\mathfrak{O}_K$).

Proof. Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}$-basis for $\mathfrak{O}_K$. Each α_i is a $\mathbb{Z}$-linear combination of the ω_is. Hence, there is an integer matrix C such that

$$(\alpha_1, \ldots, \alpha_n)^t = C\,(\omega_1, \ldots, \omega_n)^t.$$

By the change of basis formula for the discriminant, we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\omega_1, \ldots, \omega_n] = \det(C)^2 \Delta.$$

On the other hand, we have the commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{a} \arrow[r] \arrow[d, "\wr"] & \mathfrak{O}_K \arrow[r] \arrow[d, "\wr"] & \mathfrak{O}_K/\mathfrak{a} \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & \mathbb{Z}^n \arrow[r, "C"] & \mathbb{Z}^n \arrow[r] & \operatorname{cok} C \arrow[r] & 0,
\end{tikzcd}$$

and we have seen that $|\operatorname{cok}(C)| = |\det(C)|$. (Recall that by an integer change of coordinates, i.e., by applying integer row and column operations to C, we can replace C be a diagonal matrix D. It is then easy to see that $|\det(C)| = |\det(D)| = |\operatorname{cok}(D)| = |\operatorname{cok}(C)|$.) It follows that $|\det(C)| = |\mathfrak{O}_K/\mathfrak{a}| = N(\mathfrak{a})$.

We then have

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta = N(\mathfrak{a})^2 \Delta,$$

and the result follows by taking square roots. $\square$

[1] We have seen that $\mathfrak{a}$ if a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

Corollary 4. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Proof. Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}$-basis for $\mathfrak{O}_K$. Then $\{\alpha\omega_1, \ldots, \alpha\omega_n\}$ is a $\mathbb{Z}$-basis for the principal ideal (α). Say $\sigma_1, \ldots, \sigma_n$ are the embeddings of K in $\mathbb{C}$. By definition of the discriminant,

$$\Delta[\alpha\omega_1, \ldots, \alpha\omega_n] = \prod_{i=1}^{n} \sigma_i(\alpha\omega_j)^2 = \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^2 \left(\prod_{i=1}^{n} \sigma_i(\omega_j)^2\right) = N(\alpha)^2\Delta.$$

The result now follows from Proposition 3. □

Example 5. Let d be a square-free integer not equal to 0 or 1. Let $a, b \in \mathbb{Z}$ and consider the principal ideal $\mathfrak{a} = (a + b\sqrt{d})$ in $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$. Then

$$\left|\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{a}\right| = N(\mathfrak{a}) = |N(a + b\sqrt{d})| = |(a + b\sqrt{d})(a - b\sqrt{d})| = |a^2 - db^2|.$$

Just like the norm we defined for algebraic numbers, the norm for ideals is multiplicative:

Proposition 6. Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals of $\mathfrak{O}_K$. Then

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Proof. See Theorem 5.12 in our text. □

Proposition 7. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. Then

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.
2. $N(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1) = \mathfrak{O}_K$.
3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.
4. $N(\mathfrak{a}) \in \mathfrak{a}$.
5. If $\mathfrak{a}$ is prime, then $\mathfrak{a}$ contains a unique rational prime p and $N(\mathfrak{a}) = p^m$ for some $1 \leq m \leq n := [K : \mathbb{Q}]$.

Proof.

1. If $\alpha \in \mathfrak{a}$, then the principal ideal (α) is contained in $\mathfrak{a}$. Therefore $\mathfrak{a}|(\alpha)$, i.e., there exists an ideal $\mathfrak{b}$ such that $(\alpha) = \mathfrak{a}\mathfrak{b}$. Taking norms yiels

   $$N((\alpha)) = |N(\alpha)| = N(\mathfrak{a})N(\mathfrak{b}).$$

   The result follows.

2. This part is immediate from the definition of the norm.
3. Factor $\mathfrak{a}$ into primes:

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}.$$

Taking norms:

$$N(\mathfrak{a}) = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i}. \tag{2}$$

If $\mathfrak{p}$ is prime, then $\mathfrak{p} \neq \mathfrak{O}_K$, and hence $N(\mathfrak{p}) > 1$. Therefore, $N(\mathfrak{a})$ is prime if and only if $\mathfrak{a}$ is prime.

4. Since $N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$, it follows that for any $\alpha \in \mathfrak{O}_K$, we have $N(\mathfrak{a})\alpha = 0 \in \mathfrak{O}_K/\mathfrak{a}$, i.e., $N(\mathfrak{a})\alpha \in \mathfrak{a}$. Letting $\alpha = 1$ gives the result.
5. Suppose that $\mathfrak{p}$ is prime. Let $N(\mathfrak{a}) = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of $N(\mathfrak{a})$. Since $N(\mathfrak{a}) \in \mathfrak{a}$, on the level of ideals, we have

$$\prod_{i=1}^{k} (p_i)^{e_i} \subseteq \mathfrak{a},$$

and, hence,

$$\mathfrak{a} | \prod_{i=1}^{k} (p_i)^{e_i}.$$

Since $\mathfrak{a}$ is prime, there exists i such that $\mathfrak{a}|(p_i)$, which means $(p_i) \subseteq \mathfrak{a}$ or, equivalently, $p_i \in \mathfrak{a}$. If there exists an rational prime $q \neq p_i$ in $\mathfrak{a}$, we would have

$$1 \in (p_i, q) = (p_i) + (q) \subseteq \mathfrak{a}$$

However, since $\mathfrak{a}$ is prime, it does not contain 1. So there exists a unique prime $p = p_i \in \mathfrak{a}$. From the first part of this problem, we have $N(\mathfrak{a})|N(p)$. Since $N(p) = p^n$, the result follows.

$\square$

Proposition 8.

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Proof.

1. This is an immediate consequence of prime factorization of ideals.
2. We have $a \in \mathfrak{a}$ if and only if $\mathfrak{a}|(a)$. So this result follows from the previous applied to the principal ideal (a).
3. Fix $a \in \mathbb{Z}_{>0}$. If $\mathfrak{a}$ is an ideal with $N(\mathfrak{a}) = a$, then from the previous proposition, we have $a \in \mathfrak{a}$. The result then follows from part 2.

$\square$

Proposition 9. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. We already know that a PID is a UFD and that $\mathfrak{O}_K$ is a factorization domain, i.e., every element of $\mathfrak{O}_K$ has a factorization into irreducibles. Suppose that $\mathfrak{O}_K$ is a UFD. Since every ideal is a product of prime ideals, to show $\mathfrak{O}_K$ is a PID, it suffices to show that every prime ideal is principal.

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. We have

$$\mathfrak{p} \ni N(\mathfrak{p}) = \pi_1 \cdots \pi_k$$

where the π_i are irreducibles in $\mathfrak{O}_K$. Since $\mathfrak{p}$ is prime and divides $\prod_{i=1}^{k}(\pi)$, it follows that $\mathfrak{p}|(\pi_i)$ for some i. Thus, $(\pi_i) \subseteq \mathfrak{p}$. In a UFD, irreducibles are prime. Therefore, (π_i) is prime. Since $\mathfrak{O}_K$ is Dedekind, nonzero primes are maximal. Therefore $\mathfrak{p} = (\pi_i)$. $\square$

Proposition 10. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π). Then no $\mathfrak{p}_i$ is principal.

Proof. For the sake of contradiction, suppose $\mathfrak{p}_i = (\alpha)$ from some i and some $\alpha \in \mathfrak{O}_K$. Then since $\mathfrak{p}_i|(\pi)$, it follows that $(\pi) \subseteq \mathfrak{p}_i = (\alpha)$. Hence, $\pi = \alpha\beta$ from some $\beta \in \mathfrak{O}_K$. Since $\mathfrak{p}$ is prime, so is α. Since π is irreducible, β is a unit. Hence, π is prime—a contradiction. $\square$