Math 361 lecture for Wednesday, Week 9

Generators for ideals in a number ring

Let K be a number field with ring of integers $\mathfrak{O}_K$. We have seen that every ideal in $\mathfrak{O}_K$ may be uniquely factored into a product of prime ideals. Given nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathfrak{O}_K$, define their *greatest common divisor* to be the ideal $\mathfrak{c}$ such that (1) $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$ and (2) if $\mathfrak{d}$ is any ideal dividing $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{d}|\mathfrak{c}$. Since division of ideals in $\mathfrak{O}_K$ is the same as containment, the condition for $\mathfrak{c}$ is that (1) $\mathfrak{c} \supseteq \mathfrak{a}$ and $\mathfrak{c} \supseteq \mathfrak{b}$ and (2) if $\mathfrak{d} \supseteq \mathfrak{a}$ and $\mathfrak{d} \supseteq \mathfrak{b}$, then $\mathfrak{d} \supseteq \mathfrak{c}$. Note that $\mathfrak{c} \supseteq \mathfrak{a}$ and $\mathfrak{c} \supseteq \mathfrak{b}$ if and only if

$$\mathfrak{c} \supseteq \mathfrak{a} + \mathfrak{b}.$$

It follows that

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}.$$

Similarly, we define the *least common multiple* to be ideal $\mathfrak{c}$ such that $\mathfrak{c}$ is the multiple of $\mathfrak{a}$ and of $\mathfrak{b}$ such that if $\mathfrak{d}$ is any other common multiple, then $\mathfrak{c}$ divides $\mathfrak{d}$. So $\mathfrak{c} \subseteq \mathfrak{a}$ and $\mathfrak{c} \subseteq \mathfrak{b}$ and if the same containments hold for $\mathfrak{d}$, then $\mathfrak{d} \subseteq \mathfrak{c}$. It follows that

$$\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}.$$

If we have factorizations into primes

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \quad \text{and} \quad \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i},$$

(taking some $e_i = 0$ or $\ell_i = 0$, if necessary), then

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{k} \mathfrak{p}_i^{\min\{e_i, \ell_i\}} \quad \text{and} \quad \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{k} \mathfrak{p}_i^{\max\{e_i, \ell_i\}}.$$

In particular, if $\mathfrak{a}$ and $\mathfrak{b}$ relatively prime, then $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}) = (1) = \mathfrak{O}_K$.

We know that not every number ring is a PID. However, our main result shows that $\mathfrak{O}_K$ is not far from being a PID: every ideal can be generated by two elements.

Theorem 1. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$, and let $0 \neq \beta \in \mathfrak{a}$. Then there exists $\alpha \in \mathfrak{O}_K$ such that

$$\mathfrak{a} = (\alpha, \beta).$$

To prove this theorem, we use the following:

Lemma 2. If $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals of $\mathfrak{O}_K$, then there exists $\alpha \in \mathfrak{a}$ such that

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{O}_K.$$

Proof. (We are following the proof of Lemma 5.19 in the text.) First note that if $\alpha \in \mathfrak{a}$, then we can multiply $(\alpha) \subseteq \mathfrak{a}$ through by $\mathfrak{a}^{-1}$ to get $\alpha\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$. Hence, $\alpha\mathfrak{a}^{-1}$ will be an ideal not just a fractional ideal.

Suppose that $\mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ is the factorization of $\mathfrak{b}$ into prime ideals, and suppose that we can find $\alpha \in \mathfrak{a}$ such that $\alpha\mathfrak{a}^{-1}$ is relatively prime to $\mathfrak{p}_i$ for $i = 1, \ldots, k$. Then $\alpha\mathfrak{a}^{-1}$ will be relatively prime to $\mathfrak{b}$, and the result will follow: $\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{O}_K$.

Now

$$\mathfrak{p}_i | (\alpha\mathfrak{a}^{-1}) \Leftrightarrow \alpha\mathfrak{a}^{-1} \subseteq \mathfrak{p}_i \Leftrightarrow (\alpha) \subseteq \mathfrak{a}\mathfrak{p}_i \Leftrightarrow \alpha \in \mathfrak{a}\mathfrak{p}_i.$$

So it suffices to find $\alpha \in \mathfrak{a}$ such that $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}_i$ for all i. If $k = 1$, there is no problem. So suppose that $k > 1$.

For each $i = 1, \ldots, k$, define

$$\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_1 \cdots \widehat{\mathfrak{p}_i} \cdots \mathfrak{p}_k$$

where the hat over $\mathfrak{p}_i$ means to omit that factor. Since $\mathfrak{p}_i \subsetneq \mathfrak{O}_K$ it follows that $\mathfrak{a}_i\mathfrak{p}_i \subsetneq \mathfrak{a}_i$. Let $\alpha_i \in \mathfrak{a}_i \setminus (\mathfrak{a}_i\mathfrak{p}_i)$. Then define

$$\alpha = \alpha_1 + \cdots + \alpha_k.$$

Since $\alpha_i = \mathfrak{a}_i \subseteq \mathfrak{a}$ for all i, it follows that $\alpha \in \mathfrak{a}$.

It remains to be shown that for each i, we have $\alpha \notin \mathfrak{a}\mathfrak{p}_i$. For sake of contradiction, suppose that $\alpha \in \mathfrak{a}\mathfrak{p}_i$ for some i. For each $j \neq i$, from the definition of $\mathfrak{a}_j$, it follows that $\mathfrak{a}\mathfrak{p}_i$ divides $\mathfrak{a}_j$. Hence,

$$\alpha_j \in \mathfrak{a}_j \subseteq \mathfrak{a}\mathfrak{p}_i.$$

It follows that

$$\alpha_i = \alpha - \alpha_1 - \cdots - \widehat{\alpha_i} - \cdots - \alpha_k \in \mathfrak{a}\mathfrak{p}_i.$$

Therefore, we have $\mathfrak{a}_i | (\alpha_i)$ and $(\mathfrak{a}\mathfrak{p}_i) | (\alpha_i)$. So $\operatorname{lcm}(\mathfrak{a}_i, \mathfrak{a}\mathfrak{p}_i) | (\alpha_i)$. However,

$$\operatorname{lcm}(\mathfrak{a}_i, \mathfrak{a}\mathfrak{p}_i) = \operatorname{lcm}(\mathfrak{a}\mathfrak{p}_1 \cdots \widehat{\mathfrak{p}_i} \cdots \mathfrak{p}_k, \mathfrak{a}\mathfrak{p}_i) = \mathfrak{a} \operatorname{lcm}(\mathfrak{p}_1 \cdots \widehat{\mathfrak{p}_i} \cdots \mathfrak{p}_k, \mathfrak{p}_i) = \mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_i \cdots \mathfrak{p}_k = \mathfrak{a}_i\mathfrak{p}_i.$$

So $(\mathfrak{a}_i\mathfrak{p}_i) | (\alpha_i)$, from which we get the contradiciton $\alpha_i \in \mathfrak{a}_i\mathfrak{p}_i$. □

Proof of Theorem 1. Define $\mathfrak{b} = \beta\mathfrak{a}^{-1}$. By Lemma 2, there exists $\alpha \in \mathfrak{a}$ such that

$$\alpha\mathfrak{a}^{-1} + \beta\mathfrak{a}^{-1} = \mathfrak{O}_K.$$

Multiplying through by $\mathfrak{a}$, we get

$$(\alpha, \beta) = (\alpha) + (\beta) = \mathfrak{a}.$$

□

Factorization of rational integers in number rings. Give $a \in \mathbb{Z}$, how does the principal ideal $a\mathfrak{O}_K = (a) \subseteq \mathfrak{O}_K$ factor into primes? By factoring a into primes in $\mathbb{Z}$, we see that it suffices determine, for each rational prime p, how the principal ideal $p\mathfrak{O}_K = (p)$ factors in $\mathfrak{O}_K$.

Definition 3. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Last time, we saw that there exists a unique rational prime p such that $N(\mathfrak{p}) = p^f$ where $1 \leq f \leq n$. The integer f is called the *inertial degree* of $\mathfrak{p}$.

Theorem 4. (The e_i-f_i theorem.) Let p be a rational prime, and say $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ is the prime factorization of the ideal (p) in $\mathfrak{O}_K$. Then

$$\sum_{i=1}^{k} e_i f_i = n.$$

were f_i is the inertial degree of $\mathfrak{p}_i$ for each i and $n = [K : \mathbb{Q}]$.

Proof. For each $\mathfrak{p}_i$, we know $N(\mathfrak{p}_i) = p_i^{f_i}$ for some rational prime p_i. We have seen that the norm of an ideal is element of the ideal. Hence, $p_i^{f_i} \in \mathfrak{p}_i$. Since $\mathfrak{p}_i$ is prime, we have $p_i \in \mathfrak{p}_i$. However, we also know that $p \in \mathfrak{p}_i$. So $p_i = p$. (If p_i and p were distinct primes both in $\mathfrak{p}_i$, then we get that $1 \in \mathfrak{p}_i$. However, then $\mathfrak{p}_i = \mathfrak{O}_K$, contradicting the fact that $\mathfrak{p}_i$ is prime.) Take norms

$$p^n = N((p)) = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{k} p^{f_i e_i} = p^{\sum_{i=1}^{k} e_i f_i}.$$

The result follows from equating exponents. □

The next result allows us to factor rational integers in number fields with a *power basis*, i.e., whose ring of integers has the form $\mathbb{Z}[\theta]$ for some algebraic integer θ.

Theorem 5. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n such that $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Suppose that p is a rational prime, and let f be the minimal polynomial for θ over $\mathbb{Q}$. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field with p elements. If $g \in \mathbb{Z}[x]$, we let $\overline{g}$ denote the image of g in $\mathbb{F}_p[x]$ under the quotient mapping $\mathbb{Z}[x] \to \mathbb{Z}[x]/(p) = \mathbb{F}_p[x]$.

Suppose that

$$\overline{f} = \prod_{i=1}^{k} \overline{f}_i^{e_i}$$

is the factorization of f as an element of $\mathbb{F}_p[x]$ into monic irreducibles $\overline{f}_i$. Let $\mathfrak{p}_i = (p, f_i(\theta))$ for $i = 1, \ldots, k$. Then each $\mathfrak{p}_i$ is prime and

$$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}$$

is the prime factorization of (p) in $\mathfrak{O}_K$.

Example 6. Let $K = \mathbb{Q}(\sqrt{-6})$. Since $-6 \neq 1 \bmod 4$, we know that $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-6}] = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{-6}\}$. One of the homework problems gives a method for factoring the principal ideal (6) in $\mathfrak{O}_K$. Alternatively, we may use Theorem 4.

The minimal polynomial for $\sqrt{-6}$ over $\mathbb{Q}$ is $f = x^2 + 6$. Modulo 2, we have $f = x^2 \bmod 2$. Hence, $(2) = (2, \sqrt{-6})^2 \subset \mathfrak{O}_K$. Similarly, $(3) = (3, \sqrt{-6}) \subset \mathfrak{O}_K$. So the factorization of (2) into primes in $\mathfrak{O}_K$ is

$$(2) = (2, \sqrt{-6})^2 (3, \sqrt{-6})^2.$$

On the other hand, we have

$$f = x^2 + 1 = (x - 1)(x + 1) \bmod 5.$$

Hence, the prime factorization of (5) in $\mathfrak{O}_K$ is

$$(5) = (5, -1 + \sqrt{-6})(5, 1 + \sqrt{-6}).$$

Exercise: what about (7)?

Proof of Theorem 4. **Step 1.** First, we show that sending x to θ induces an isomorphism

$$\overline{\phi} \colon \mathbb{Z}[x]/(f) \xrightarrow{\sim} \mathbb{Z}[\theta].$$

To see this consider the mapping of rings $\phi \colon \mathbb{Z}[x] \to \mathbb{Z}[\theta]$ determined $\phi(x) = \theta$. It is clearly surjective, and since $f(\theta) = 0$, we have $f \in \ker(\phi)$. Hence, $\overline{\phi}$ is well-defined. Suppose that $g \in \ker \overline{\phi}$, i.e., $g(\theta) = 0$. Since f is the minimal polynomial of θ, we have $g = fh$ for some $h \in \mathbb{Q}[x]$. It is easy to check that since f is monic, we must have $h \in \mathbb{Z}[x]$ (or one may use Gauss's lemma and the fact that f is monic). Hence, $g = 0 \in \mathbb{Z}[x]/(f)$.

Step 2. For each i, we have a natural sequence of surjections

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f_i) = \mathbb{Z}[x]/(p, f_i)$$

Since $f_i | f$, we see f is in the kernel. So we get a surjection

$$\phi_i \colon \mathbb{Z}[\theta] \simeq \mathbb{Z}[x]/(f) \to \mathbb{Z}[x]/(p, f_i).$$

where

$$\phi_i(g(\theta)) = \overline{g(x)} \in \mathbb{Z}[x]/(p, f_i)$$

for all $g \in \mathbb{Z}[x]$.

Step 3. We claim $(p, f_i(\theta))$ is a prime ideal in $\mathbb{Z}[\theta]$. We have the isomorphism

$$\mathbb{Z}[\theta]/\ker(\phi_i) \xrightarrow{\sim} \mathbb{F}_p[x]/(f_i).$$

Since $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field, $\mathbb{F}_p[x]$ is a PID. Then, since f_i is irreducible, (f_i) is a maximal ideal (if $(f_i) \subset (g)$, then $f = gh$ for some h. So either g is a unit and $(g) = \mathbb{F}_p[x]$ or h is

a unit and $(f) = (g)$. Therefore, $\mathbb{F}_p[x]/(f_i)$ is a field, which implies $\ker(\phi_i)$ is a maximal, hence, prime ideal. So to show $(p, f_i(\theta))$ is prime, it suffices to show that

$$\ker(\phi_i) = (p, f_i(\theta)).$$

It is clear that $(p, f_i(\theta)) \subseteq \ker(\phi_i)$. For the opposite inclusion, let $g(\theta) \in \ker(\phi_i)$. Then $g(x) = p\ell(x) + h(x)f_i(x)$. Then,

$$g(\theta) = p\ell(\theta) + h(\theta)f_i(\theta) \in (p, f_i(\theta)).$$

Step 4. We claim that if $i \neq j$, then $(p, f_i(\theta)) \neq (p, f_j(\theta))$. To see this, suppose that these ideals are equal. Then,

$$(p, f_i(\theta)) = (p, f_j(\theta)) \Rightarrow f_j(\theta) \in (p, f_i(\theta)) \in \ker(\phi_i) \Rightarrow \phi_i(f_j) = 0 \Rightarrow f_j(x) \in (p, f_i).$$

Therefore, $f_j = hf_i \bmod p$, i.e., $f_j = hf_i$ in $\mathbb{F}_p[x]$. However, f_j is irreducible in $\mathbb{F}_p[x]$. Hence, h is a unit, i.e., $h \in \{1, 2, \ldots, p-1\}$ in $\mathbb{F}_p$. Since f_i and f_j are both monic, it follows that $f_i = f_j$.

Step 5. We now show that

$$(p) = \prod_{i=1}^{k} (p, f_i(\theta))^{e_i}.$$

We use the fact that for ideals in $\mathfrak{O}_K$,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{bc}.$$

We have

$$\begin{aligned}
\prod_{i=1}^{k} (p, f_i(\theta))^{e_i} &= \prod_{i=1}^{k} ((p) + (f_i(\theta)))^{e_i} \\
&\subseteq \prod_{i=1}^{k} ((p) + (f_i(\theta)^{e_i})) \\
&\subseteq (p) + \left(\prod_{i=1}^{k} f_i(\theta)^{e_i} \right) \\
&= (p) + (f(\theta)) \\
&= (p).
\end{aligned}$$

since $f(\theta) = 0$. Thus, (p) divides $\prod_{i=1}^{k} (p, f_i(\theta))^{e_i} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$. It follows that

$$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$$

for some $0 \leq \ell_i \leq e_i$.

Take norms:

$$\mathfrak{p}^n = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}.$$

Now,

$$N(\mathfrak{p}_i) = |\mathbb{Z}[\theta]/\mathfrak{p}_i|$$

and

$$\mathbb{Z}[\theta]/\mathfrak{p}_i = \mathbb{Z}[\theta]/\ker(\phi_i) \simeq \mathbb{F}_p[x]/(f_i).$$

The elements of $\mathbb{F}_p[x]/(f_i)$ are exactly $a_0 + a_1 x + \cdots + a_{d_i-1}x^{d_i-1}$ where the a_i are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $d_i = \deg(f_i)$. Therefore

$$|\mathbb{F}_p[x]/(f_i)| = p^{\deg(f_i)}.$$

It follows that

$$p^n = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{\ell_i} = \prod_{i=1}^{k} p^{\deg(f_i)\ell_i} = p^{\sum_{i=1}^{k} \deg(f_i)\ell_i},$$

and hence

$$n = \sum_{i=1}^{k} \deg(f_i)\ell_i.$$

On the other hand, $f = \prod_{i=1}^{k} f_i^{e_i}$ implies

$$n = \deg(f) = \sum_{i=1}^{k} \deg(f_i)e_i.$$

Since $0 \leq \ell_i \leq e_i$, we must have $\ell_i = e_i$ for all i. □

Remark 7. It would be nice to have criteria for deciding when a number field has a power basis.