Math 361 lecture for Friday, Week 2

Quadratic fields

Lemma 1. (Gauss's lemma.) Let $f \in \mathbb{Z}[x]$, and suppose that $f = gh$ for $g, h \in \mathbb{Q}[x]$. Then there exists a nonzero $\lambda \in \mathbb{Q}$ such that λg and $\frac{1}{\lambda}h$ are in $\mathbb{Z}[x]$. (Thus, a polynomial in a single variable with integer coefficients factors over $\mathbb{Q}$ if and only if it factors over $\mathbb{Z}$.)

Proof. See our text, Lemma 1.7. $\square$

Last time, we defined the *algebraic integers* to be the set of complex numbers that are integral over $\mathbb{Z}$:

$$\mathfrak{O} := \{\alpha \in \mathbb{C} : f(\alpha) = 0 \text{ for some monic polynomial } f \in \mathbb{Z}[x]\}.$$

Corollary 2. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. If the minimal polynomial of α has integer coefficients, then it follows immediately that α is an algebraic integer. So we now consider the converse.

Recall that if L/K is a field extension, then $\alpha \in L$, is *algebraic* over K if there exists a polynomial $f \in K[x]$ such that $f(\alpha) = 0$. If α is algebraic, then $[K(\alpha) : K] < \infty$ and, in fact, $K(\alpha) = K[\alpha]$.

Let $\alpha \in \mathfrak{O} \subset \mathbb{C}$ be an algebraic integer, and let $f \in \mathbb{Z}[x]$ be a monic polynomial such that $f(\alpha) = 0$. It follows that α is algebraic over $\mathbb{Q}$. Thus, it makes sense to talk about its minimal polynomial $p \in \mathbb{Q}[x]$. We need to show the coefficients of p are integers. Since $f(\alpha) = 0$, it must be that $f = qp$ for some $q \in \mathbb{Q}[x]$. (Reminder: apply the division algorithm to write $f = qp + r$ where $q, r \in \mathbb{Q}[x]$ and $\deg(r) < \deg(p)$. Evaluating at α yields $r(\alpha) = 0$. The minimality condition in the definition of p then forces $\deg(r) = 0$, i.e., r is a constant polynomial. Then $r(\alpha) = 0$ says that $r = 0$. Thus, $f = qp$.)

By Gauss's lemma, there exists a nonzero $\lambda \in \mathbb{Q}$ such that λq and $\frac{1}{\lambda}p \in \mathbb{Z}[x]$ have integer coefficients. Next, compare leading coefficients. Since the leading coefficients of f and p are both 1 and $f = qp$, it follows that the leading coefficient of q is 1 also. Since q is monic and $\lambda q \in \mathbb{Z}[x]$, it follows that $\lambda \in \mathbb{Z}$. Since p is monic, and $\frac{1}{\lambda}p \in \mathbb{Z}[x]$, it follows that $\frac{1}{\lambda} \in \mathbb{Z}$. Therefore, $\lambda = \pm 1$, Then, since $\frac{1}{\lambda}p \in \mathbb{Z}[x]$, it follows that $p \in \mathbb{Z}[x]$, too, as required. $\square$

In the previous lecture, we gave an ad hoc argument that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$. We now obtain that result as a corollary of the result we just proved.

Corollary 3. $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$.

Proof. Certainly, $\mathbb{Z} \subseteq \mathfrak{O} \cap \mathbb{Q}$. For the reverse inclusion, suppose that $a \in \mathfrak{O} \cap \mathbb{Q}$. The minimal polynomial for a over $\mathbb{Q}$ is $x - a$. By Corollary 2, it follows that $x - a \in \mathbb{Z}[x]$. In particular, this means that $a \in \mathbb{Z}$. $\square$

Ring of integers in a number field. Let K be a number field. In other words, K is a finite field extension of $\mathbb{Q}$ inside of $\mathbb{C}$. Define the *ring of integers in* K to be the set of all algebraic integers in K:

$$\mathfrak{O}_K := \mathfrak{O} \cap K.$$

We picture the situation like this:

$$\begin{array}{ccc} K & \text{———} & \mathfrak{O}_K \\ | & & | \\ \mathbb{Q} & \text{———} & \mathbb{Z}. \end{array}$$

Lemma 4. With notation as above. If $\alpha \in K$, then there exists an integer c such that $c\alpha \in \mathfrak{O}_K$.

Proof. Homework. $\square$

Theorem 5. (Primitive element theorem (generalized).) Let K be a number field. Then there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$.

Proof. Our text proves there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ (cf. Theorem 2.2). By the lemma, there exists $c \in \mathbb{Z}$ such that $c\alpha \in \mathfrak{O}_K$. Let $\theta := c\alpha$. Then it is clear that $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$. However, since θ is algebraic over $\mathbb{Q}$, it follows from previous work that $\mathbb{Q}(\theta) = \mathbb{Q}[\theta]$. $\square$

Quadratic fields. Suppose that K is a extension of $\mathbb{Q}$ of degree 2, i.e., $[K : \mathbb{Q}] = 2$. By the primitive element theorem, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$. Since $[K : \mathbb{Q}] = 2$, it follows that the minimal polynomial for θ has the form $p = x^2 + mx + n$ for some $m, n \in \mathbb{Z}$. Therefore,

$$\theta = \frac{-m \pm \sqrt{m^2 - 4n}}{2}.$$

Write

$$m^2 - 4n = r^2 d$$

where $r, d \in \mathbb{Z}$ and d is square-free. Since $\theta \notin \mathbb{Q}$, we have $d \neq 0, 1$. Then

$$\theta = \frac{-m \pm r\sqrt{d}}{2}$$

and

$$K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}] = \mathrm{Span}_{\mathbb{Q}}\{1, \sqrt{d}\}.$$

Our goal is to find $\mathfrak{O}_K$. Let $\alpha \in \mathbb{Q}[\sqrt{d}]$. Then $\alpha = s + t\sqrt{d}$ for some $s, t \in \mathbb{Q}$, from which we can see

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

for some $a, b, c \in \mathbb{Z}$ sharing no common prime factors. If $b = 0$, then $\alpha = \frac{a}{c} \in \mathbb{Q}$. So if α is also in $\mathfrak{O}_K$, we have $\alpha \in \mathbb{Q} \cap \mathfrak{O}_K = \mathbb{Z}$, and $c = 1$. Now suppose that $b \neq 0$. The minimal polynomial for α over $\mathbb{Q}$ is

$$p(x) = \left(x - \frac{a + b\sqrt{d}}{c}\right)\left(x - \frac{a - b\sqrt{d}}{c}\right) = x^2 - \frac{2a}{c} + \frac{a^2 - b^2 d}{c^2} \in \mathbb{Q}[x].$$

Then $\alpha \in \mathfrak{O}_K$ if and only if

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}. \tag{1}$$

Suppose $\alpha \in \mathfrak{O}_K$. If $q \neq 2$ is a prime integer and $q|c$, then $q|(2a)$ implies that $q|a$ and $q^2|a^2$. Since $q|c$ and $c^2|(a^2 - b2d)$, it follows that $q^2|(a^2 - b^2 d)$, and hence $q^2|(b^2 d)$. Since d is square-free, $q|b$. We have shown that q is a common factor of a, b and c, However, a, b and c share no prime factors. So at this point, we can conclude that c must be a power of 2. If $4|c$, then $c|(2a)$ would imply that $2|a$, and repeating the above argument, we would get that a, b and c all share a factor of 2, which is not the case. It follows that $c = 1$ or $c = 2$.

If $c = 1$, then

$$\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}].$$

Now consider the case where $c = 2$. In that case, we need that $4|(a^2 - b^2 d)$. From this, if a or b is even, then we may conclude that both a and b are even (since d is square-free). Since a, b and c share no factors, it must be that both a and b are odd. Hence, $a^2 = b^2 = 1 \bmod 4$. We have

$$a^2 - b^2 d = 1 - d = 0 \bmod 4.$$

So if $c = 2$, then $d = 1 \bmod 4$.

Therefore, if $d \neq 1 \bmod 4$, we must have $c = 1$, in which case (1) says that $\alpha \in \mathfrak{O}_K$. So if $d \neq 1 \bmod 4$, then $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$. If $d = 1 \bmod 4$, then (1) holds if and only if $c = 1$ or if $c = 2$ and both a and b are odd. We then claim that $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. We know that $\frac{1+\sqrt{d}}{2} \in \mathfrak{O}_K$ and that $\mathfrak{O}_K$ is a ring. Hence, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathfrak{O}_K$. For the reverse inclusion, suppose that $\alpha \in \mathbb{Z}[\sqrt{d}]$. We have seen that either $\alpha = a + b\sqrt{d}$ for some $a, b \in \mathbb{Z}$, in which case

$$\alpha = a + b\sqrt{d} = (a - b) + 2b\left(\frac{1 + \sqrt{d}}{2}\right) \in \mathbb{Z}[\tfrac{1+\sqrt{d}}{2}],$$

or $\alpha = \frac{a+b\sqrt{d}}{2}$ where a and b are both odd, in which case,

$$\alpha = \frac{a+b\sqrt{d}}{2} = \left(\frac{a-b}{2}\right) + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\tfrac{1+\sqrt{d}}{2}].$$

We sum up our discussion with the theorem below.

Theorem 6. Let K be a field extension of $\mathbb{Q}$ with $[K:\mathbb{Q}] = 2$. Then $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Its ring of integers is

$$\mathfrak{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \neq 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d = 1 \bmod 4. \end{cases}$$

We have $\mathbb{Z}[\sqrt{d}] = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{d}\}$, and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathrm{Span}_{\mathbb{Z}}\{1, \frac{1+\sqrt{d}}{2}\}$.