XM452 Lecture Notes 10

Erdaifu Luo

30 April 2023

§45 Introduction to Quadratic Fields

A common technique in solving an equation is factoring it.

Example 45.1

$$0 = x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right),$$

so in particular, there are no integer nor rational solutions.

Let $\mathbb{Z}$ denote the set of integers, let $\mathbb{Q}$ denote the set of rational numbers, and $\mathbb{R}$ denote the set of real numbers.

Definition 45.2 (Quadratic Fields)**.** Let d be a fixed rational number which is not a square of a rational number (e. g. $d = p$, p is a prime).

Let $\mathbb{Q}\left[\sqrt{d}\right]$ denote the set of numbers

$$a + b\sqrt{d}$$

where a and b are arbitrary real numbers.

$\mathbb{Q}\left[\sqrt{d}\right]$ is called a **quadratic field**. If $d > 0$, $\mathbb{Q}\left[\sqrt{d}\right]$ is called a **real quadratic field**. If $d < 0$, $\mathbb{Q}\left[\sqrt{d}\right]$ is called an **imaginary quadratic field**.

Example 45.3

$1 + \sqrt{2}$ and $\frac{\sqrt{2}}{3}$ are both numbers of $\mathbb{Q}\left[\sqrt{2}\right]$. Notice also that all rational numbers are members of $\mathbb{Q}\left[\sqrt{d}\right]$ since $a \in \mathbb{Q}$ means $a + 0\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$

Theorem 45.4

$a + b\sqrt{d} = c + e\sqrt{d}$ if and only if $a = c$ and $b = e$.

Proof. $a + b\sqrt{d} = c + e\sqrt{d}$ means that

$$\left(a + b\sqrt{d}\right) - \left(c + e\sqrt{d}\right) = 0.$$

This means that
$$(a-c)+(b-e)\sqrt{d}=0$$
or
$$a-c=(e-b)\sqrt{d},$$
where $a-c\in\mathbb{Q}$ and $b-e\in\mathbb{Q}$. But since $\sqrt{d}\notin\mathbb{Q}$ then $e\neq b$, $(e-b)\sqrt{d}$ is irrational. But $(e-b)\sqrt{d}=a-c$ which is rational. Thus, $e-b=0$, meaning that $e=b$, and therefore $0=a-c$, or $a=c$. □

Theorem 45.5
Let $\alpha,\beta\in\mathbb{Q}\left[\sqrt{d}\right]$. Then $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta\in\mathbb{Q}\left[\sqrt{d}\right]$ and if $\beta\neq 0$, $\frac{\alpha}{\beta}\in\mathbb{Q}\left[\sqrt{d}\right]$.

Proof. Say $\alpha=a+b\sqrt{d}$, $\beta=c+e\sqrt{d}$. Then
$$\begin{aligned}\alpha+\beta&=(a+c)+(b+e)\sqrt{d}\in\mathbb{Q}\left[\sqrt{d}\right]\\ \alpha-\beta&=(a-c)+(b-e)\sqrt{d}\in\mathbb{Q}\left[\sqrt{d}\right]\\ \alpha\beta&=(ac+bed)+(ae+bc)\sqrt{d}\in\mathbb{Q}\left[\sqrt{d}\right]\end{aligned}$$
and if $\beta\neq 0$,
$$\frac{\alpha}{\beta}=\left(\frac{ac-bed}{c^2-e^2d}\right)+\left(\frac{bc-ae}{c^2-e^2d}\right)\in\mathbb{Q}\left[\sqrt{d}\right].$$
□

Theorem 45.6
If r and s are integers, then
$$\mathbb{Q}\left[\sqrt{\frac{r}{s}}\right]=\mathbb{Q}\left[\sqrt{rs}\right]$$

Because of this it is enough to consider rational fields $\mathbb{Q}\left[\sqrt{d}\right]$ where d is an integer.

Definition 45.7. If $\alpha=a+b\sqrt{d}$, then the conjugate of α, written $\overline{\alpha}=a-b\sqrt{d}$.

So, for example,
$$\overline{\sqrt{d}}=-\sqrt{d}.$$

Theorem 45.8
If $\alpha,\beta\in\mathbb{Q}\left[\sqrt{d}\right]$, then $\overline{(\overline{\alpha})}=\alpha$, $\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$, $\overline{\alpha-\beta}=\overline{\alpha}-\overline{\beta}$, $\overline{\alpha\beta}=\overline{\alpha}\overline{\beta}$, and if $\beta\neq 0$, $\overline{\frac{\alpha}{\beta}}=\frac{\overline{\alpha}}{\overline{\beta}}$. Furthermore, $\alpha=\overline{\alpha}$ if and only if α is rational.

§46 Defining Equations and Quadratic Integers

Given an element $\alpha = a + b\sqrt{d} \in \mathbb{Q}\left[\sqrt{d}\right]$, notice that α is a solution to the quadratic equation

$$0 = \left(x - \left(a + b\sqrt{d}\right)\right) \cdot \left(x + \left(a - b\sqrt{d}\right)\right) = x^2 - 2ax + \left(a^2 - b^2 d\right).$$

Notice that $\overline{\alpha} = a - b\sqrt{d}$ is also a solution to this equation.

This polynomial has rational coefficients since $2a$ and $a^2 - b^2 d$ are rational because a, b, $d \in \mathbb{Q}$. If we multiply this equation by a common denominator for $2a$ and $a^2 - b^2 d$ we get a quadratic equation with integral coefficients that is solved by α and $\overline{\alpha}$.

Definition 46.1. If α is an irrational number in $\mathbb{Q}\left[\sqrt{d}\right]$ then the equation $ax^2+bx+c=0$ is called the defining equation for α, if α satisfies the equation and a, b, $c \in \mathbb{Z}$, $(a, b, c) = 1$, and $a > 0$.

Claim 46.2 — A defining equation exists and is unique for every irrational $\alpha \in \mathbb{Q}\left[\sqrt{d}\right]$.

Proof. Let $ax^2+bx+c=0$ be a polynomial equation satisfied by $x = \alpha$ and with integral coefficients. By the argument above, we know such a polynomial exists. Now plug in $x = \overline{\alpha}$, we egt

$$a\overline{\alpha}^2 + b\overline{\alpha}^2 + c = \overline{a}\overline{\alpha}^2 + \overline{b}\overline{\alpha} + \overline{c}$$

since a, b, $c \in \mathbb{Z}$. The previous equals to

$$\overline{\left(a\alpha^2 + b\alpha + c\right)},$$

which equals to 0 from our definition. Thus if α is a root of the equation, so is α. Since α is irrational, $\alpha \neq \overline{\alpha}$, so we can factor the polynomial

$$ax^2 + bx + c = a\left(x - \alpha\right)\left(x - \overline{\alpha}\right).$$

□

Definition 46.3. If $\alpha \in \mathbb{Q}\left[\sqrt{d}\right]$ we define the norm of α to be

$$N\left(\alpha\right) = \alpha\overline{\alpha}.$$

So if $\alpha = a + b\sqrt{d}$, $N\left(\alpha\right) = a^2 - b^2 d$ which is a rational number.

Theorem 46.4

$N(a) = a^2$ for a rational number. If $\alpha \in \mathbb{Q}\left[\sqrt{d}\right]$ then $N\left(\alpha\right)$ is rational. If $d < 0$ then $N\left(a\right) \geq 0$.

Also, if $\beta \in \mathbb{Q}\left[\sqrt{d}\right]$, then

$$N\left(\alpha\beta\right) = N\left(\alpha\right) N\left(\beta\right)$$
$$N\left(\frac{\alpha}{\beta}\right) = \frac{N\left(\alpha\right)}{N\left(\beta\right)}, \quad \beta \neq 0.$$

Proof. Observe that $\alpha = a + b\sqrt{d}$, then $N(a) = a^2 - b^2 d$. The rest is just simple calculation. □

Next, we would want to define integers in the quadratic field.

For ordinary integers, if $x^n \in \mathbb{Z}$ and x is rational, then $x \in \mathbb{Z}$. We want to keep this basic property in the notion of "integer" in $\mathbb{Q}\left[\sqrt{d}\right]$.

Notice that $\left(\sqrt{d}\right)^2 = d$, so that if $d \in \mathbb{Z}$ then we want to say that $\sqrt{d}$ is an integer in $\mathbb{Q}\left[\sqrt{d}\right]$. Our quadratic "integers" should also be closed under addition and multiplication.

So we should also have numbers of the form

$$n + m\sqrt{d}$$

where n, $m \in \mathbb{Z}$, be quadratic "integers".

Definition 46.5. A number $\alpha \in \mathbb{Q}\left[\sqrt{d}\right]$ is called a quadratic integer if either $\alpha \in \mathbb{Z}$ or if α is irrational and the coefficient of x^2 in the defining equation for α is 1. The numbers in $\mathbb{Z}$ are called "rational integers".

Theorem 46.6

If $d \not\equiv 1 \pmod 4$ then the quadratic integers of $\mathbb{Q}\left[\sqrt{d}\right]$ are those numbers of the form

$$n + m\sqrt{d},$$

where n, $m \in \mathbb{Z}$.

Theorem 46.7

If $\alpha \in \mathbb{Q}\left[\sqrt{d}\right]$ is a quadratic integer, then its norm $N(\alpha) \in \mathbb{Z}$.

Proof. By definition, if α is a quadratic integer, its defining equation is

$$0 = (x - \alpha)(x - \overline{\alpha})$$

which if $\alpha = a + b\sqrt{d}$ is equal to

$$x^2 - 2ax + \left(a^2 - b^2 d\right) = 0.$$

Since the defining equation has integral coefficients,

$$N(\alpha) = a^2 - b^2 d,$$

which is exactly the norm of α, and is in the set $\mathbb{Z}$. □

§47 Characterizing Quadratic Integers

Theorem 47.1

If $d \not\equiv 1 \pmod 4$ then the quadratic integers of $\mathbb{Q}\left[\sqrt{d}\right]$ are those numbers of the form

$$a + b\sqrt{d},$$

where a, $b \in \mathbb{Z}$. If $d \equiv 1 \pmod 4$, then the quadratic integers in $\mathbb{Q}\left[\sqrt{d}\right]$ are those numbers of the form $\frac{(a+b\sqrt{d})}{2}$, where a, $b \in \mathbb{Z}$ and a and b are both even or both odd.j

Corollary 47.2

If $d \equiv 1 \pmod 4$, a number in $\mathbb{Q}\left[\sqrt{d}\right]$ is a quadratic integer if and only if it can be written as

$$a + b\left(\frac{1+\sqrt{d}}{2}\right).$$

Proof of corollary assuming the below theorem. If a, $b \in \mathbb{Z}$,

$$a + b\left(\frac{1+\sqrt{d}}{2}\right) = \frac{(2a+b)+b\sqrt{d}}{2}$$

where $2a + b \equiv b \pmod 2$, so $2a + b$ and b are both even or odd. Therefore, by the theorem, it is a quadratic integer. Similarily, if a, b are any two integers, both even or odd,

$$\frac{a+b\sqrt{d}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2}$$

where $\frac{a-b}{2}$ both are integers. □

Proof of theorem. If $a, b \in \mathbb{Z}$, then it is clear that $a + b\sqrt{d}$ is a quadratic integer because

$$\left(x - \left(a + b\sqrt{d}\right)\right)\left(x - \left(a - b\sqrt{d}\right)\right) = x^2 - 2ax + \left(a^2 - b^2 d\right)$$

has integer coefficients. If $d \equiv 1 \pmod 4$ then

$$\left(x - \frac{a+b\sqrt{d}}{2}\right)\left(x - \frac{a-b\sqrt{d}}{2}\right) = x^2 - ax + \frac{(a^2 - b^2 d)}{4}$$

also has integral coefficients if a and b are both even or odd.

Too lazy to write further proof so gg. □