XM452 Lecture Notes 11

Erdaifu Luo

30 April 2023

§48 Factorization into Quadratic Primes

Definition 48.1. If α and β are quadratic integers in $\mathbb{Q}\left[\sqrt{d}\right]$, we say that α **divides** β and write $\alpha \mid \beta$ if there is a quadratic integer γ such that

$$\alpha\gamma = \beta.$$

We want a notion of a *prime quadratic integer*, where it cannot be decomposed as a product. However, every $n \in \mathbb{Z}$ can be decomposed as

$$(1)\,(n) \text{ or } (-1)\,(-n)\,,$$

so we need to exclude ± 1 as factors.

In the quadratic integers we need to exclude any quadratic integer ϵ so that $\epsilon \mid 1$. Such a quadratic integer is called a **unit** in the set.

The reason we need to exclude units from our definition of quadratic prime is because if ϵ is a unit, so there is a quadratic integer γ such that $\epsilon\gamma = 1$, then if α is any quadratic integer it can be decomposed as

$$\alpha = \alpha\epsilon\gamma.$$

Theorem 48.2

If ϵ_1 and ϵ_2 are units in $\mathbb{Q}\left[\sqrt{d}\right]$, then $\overline{\epsilon_1}$, $\epsilon_1\epsilon_2$, and $\frac{\epsilon_1}{\epsilon_2}$ (in particularm $\frac{1}{\epsilon_2}$), are all units.

Proof. Since ϵ_1 and ϵ_2 are units in the set, there are quadratic integers γ_1 and γ_1 so that $\epsilon_{1\gamma_1=\epsilon_2\gamma_2=1}$. Notice that

$$\begin{gathered}
\overline{\epsilon_1\gamma_1} = \overline{\epsilon_1\gamma_1} = \overline{1} = 1 \\
(e_{1e_2})\,(\gamma_1\gamma_2) = \epsilon_1\gamma_1\epsilon_2\gamma_2 = 1 \cdot 1 = 1 \\
\frac{\epsilon_1}{\epsilon_2}\frac{\gamma_1}{\gamma_2} = \frac{\epsilon_1\gamma_1}{\epsilon_{2\gamma_2}} = \frac{1}{1} = 1.
\end{gathered}$$

So these numbers are all units as well. □

Theorem 48.3

If $d < -1$ and $d \neq 3$, then $\mathbb{Q}\left[\sqrt{d}\right]$ has exactly two units, ± 1. Also, $\mathbb{Q}\left[\sqrt{-1}\right]$ has four units: ± 1, $\pm\sqrt{-1}$. $\mathbb{Q}\left[\sqrt{-3}\right]$ has six units,

$$\pm 1, \pm\left(-1 + \frac{\sqrt{-3}}{2}\right), \pm\left(-1 - \frac{\sqrt{-3}}{2}\right).$$

If $d > 0$, $\mathbb{Q}\left[\sqrt{d}\right]$ has infinitely many units.

Proposition 48.4

If ϵ is a quadratic integer in $\mathbb{Q}\left[\sqrt{d}\right]$, then ϵ is a unit if and only if the norm $N(\epsilon) = \pm 1$.

Proof. If $N(\epsilon) = 1$, then $\epsilon \cdot \overline{\epsilon} = N(\epsilon) = 1$, so ϵ is a unit. Similarily, if $N(\epsilon) = -1$, then $\epsilon \cdot (-\overline{\epsilon}) = 1$, and again ϵ is a unit. To show the converse, suppose ϵ is a unit. So there is a quadratic integer γ so that $\epsilon\gamma = 1$. Thus, $N(\epsilon)(\gamma) = N(\epsilon\gamma) = N(1) = 1$.

Since ϵ and γ are quadratic integers, $N(\epsilon)$ and $N(\gamma)$ are in $\mathbb{Z}$. Thus $N(\epsilon) \mid 1$ in $\mathbb{Z}$. This implies $N(\gamma) = \pm 1$. □

Definition 48.5. A quadratic integer $\theta \in \mathbb{Q}\left[\sqrt{d}\right]$ which neither 0 or a unit is called a **prime** if for every decomposition of θ into a product of two integers, $\theta = \alpha\beta$, then either α or β is a unit.

Theorem 48.6

If α is a quadratic integer in $\mathbb{Q}\left[\sqrt{d}\right]$, and if $N(\alpha) \in \mathbb{Z}$ is a prime number, then α is prime.

Proof. Since $N(\alpha)$ is a prime number, α is not 0 or a unit, by the above theorem. Now suppose

$$\alpha = \beta\gamma$$

where they are both quadratic integers. Then $N(\alpha) = N(\beta)N(\gamma)$ is a decomposition of the prime number $N(\alpha)$ into a product of integers. This means that either $N(\beta)$ or $N(\gamma)$ is ± 1. Hence by the above theorem, either β or γ is a unit. □

§49 Unique Factorization

Definition 49.1. Suppose $\mathbb{Q}\left[\sqrt{d}\right]$ has the following peoperty: if α is a non-unit, nonzero quadratic integer, and we have two factorizations of α into primes

$$\alpha = \epsilon\pi_1\pi_2\ldots\pi_r, \quad \alpha = \epsilon'\pi_1'\pi_2'\ldots\pi_r'$$

where ϵ, ϵ' are units and the π's are primes in $\mathbb{Q}\left[\sqrt{d}\right]$, then the π_i's can be reordered so that $\frac{\pi_i}{\pi_i'}$ is a unit for $i = 1, \ldots, r$.

We then say that $\mathbb{Q}\left[\sqrt{d}\right]$ is a **unique factorization domain**. Or, abbreviated, U.F.D.

Theorem 49.2

The integers of $\mathbb{Q}\left[\sqrt{d}\right]$ form a UFD if and only if $\mathbb{Q}\left[\sqrt{d}\right]$ has the following property:

If $\pi \mid \alpha\beta$ where π is prime and α and β are quadratic integers in $\mathbb{Q}\left[\sqrt{d}\right]$, then $\pi \mid \alpha$ or $\pi \mid \beta$.

Proof. Suppose that $\mathbb{Q}\left[\sqrt{d}\right]$ is a UFD and $\pi \mid \alpha\beta$. Thus there is an integer $\gamma \in \mathbb{Q}\left[\sqrt{d}\right]$ so that $\pi\gamma = \alpha\beta$. Writing γ in prime factorization,

$$\gamma = \epsilon\pi\pi^1\pi^2 \dots \pi_n.$$

Then 1. $\pi\gamma = \epsilon\pi\pi^1\pi_2 \dots \pi_n$ is a prime factorization of $\pi\gamma = \alpha\beta$. Similarily, if $\alpha = \epsilon_1\pi_1'\pi_2' \dots \pi_r'$ and $\beta = \epsilon_2\pi_1''\pi_2'' \dots \pi_s''$ are prime factorizations, then 2.

$$\alpha\beta = \epsilon_1\epsilon_2\pi_1'\pi_2' \dots \pi_r'\pi_1''\pi_2'' \dots \pi_s''$$

is another prime factorization. By the uniqueness property in a UFD, since π appears in factorization 1 of $\alpha\beta$, an associate π appears in the factorization 2 of $\alpha\beta$.

But since the primes in factorization 2 all divide either α or β, then an associate of π, say π', divides one of α or β or both. But since π and π' are associate, then $\pi' = \epsilon\pi$ where ϵ is an unit. Thus π also divides either α or β, as claimed.

Conversely, assume $\mathbb{Q}\left[\sqrt{d}\right]$ has the property that if $\pi \mid \alpha\beta$, where π is a prime and α and β are any integers in then π divides α or β. We wish to show $\mathbb{Q}\left[\sqrt{d}\right]$ is a UFD.

So suppose

$$\alpha = \epsilon\pi_1\pi_2 \dots \pi_r, \quad \alpha = \epsilon'\pi_1'\pi_2' \dots \pi_s'$$

are two prime factorizations. By induction, one can easy show that easy π_i must divide one of the primes $\pi_1', \dots, \pi_s'$.

Say $\pi_i \mid \pi_j'$. That is, there is an integer e so that $\pi_j' = e\pi_i$. Since π_j' is a prime, e is a unit. Thus, i_j and π_j' are associates. The unique factorization property now follows. □