Number Theory

Lectured by Meng T. Heang

June 30, 2022

Chapter 1

Quadratic Ring

1.1 Some definitions

The motivation of this comes from the fact that solving equations like $x^n + y^n = z^n$ is rather hard to solve. For example, case $n = 2$, the equation becomes

$$z^2 = x^2 + y^2 = (x + \mathrm{i}y)(x - \mathrm{i}y)$$

so we need a language to say that $(x + \mathrm{i}y)$ is a divisor of z^2, I guess. And here comes the

Definition 1.1
For any square-free (not a perfect square) integer d, we define

$$\mathbb{Q}[\sqrt{d}] := \{x + y\sqrt{d} \ : \ x, y \in \mathbb{Q}\}.$$

In $\mathbb{Q}[\sqrt{d}]$, we define the usual addition and multiplication as follow: for $a + b\sqrt{d},\ x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, then

$$(a + b\sqrt{d}) + (x + y\sqrt{d}) = (a + x) + (b + y)\sqrt{d}$$

and

$$(a + b\sqrt{d})(x + y\sqrt{d}) = (ax + byd) + (ay + bx)\sqrt{d}.$$

As we can see that $\mathbb{Z}[\sqrt{d}]$ is indeed a ring. But it's more than that. In fact, it's a field. To see why, let $a + b\sqrt{d} \neq 0 \in \mathbb{Z}[\sqrt{d}]$, and we choose $x = \frac{a}{a^2 - db^2}$ and $y = \frac{-b}{a^2 - db^2}$. We then have

$$(a + b\sqrt{d})(x + y\sqrt{d}) = 1.$$

Example 1.1 For special case of d:

- When $d = 2$, we have $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$.
- When $d = -1$, we then have $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{-1}]$. In is field, a special subset is considered, the subring $\mathbb{Z}[\mathrm{i}] \subset \mathbb{Q}[\mathrm{i}]$, which is called *the set*

of Gaussian Integers.

We can consider $\mathbb{Q}[\sqrt{d}]$ as a vector space over the field $\mathbb{Q}$. Moreover we can setup an isomophism $\mathbb{Q}[\sqrt{d}]$ to $\mathbb{Q}^2$ by sending $a + b\sqrt{q}$ to (a, b).

1.2 Norm and Trace

Let $L = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. We define the

- conjugate $\overline{L} := x = y\sqrt{d}$
- trace $T(L) = \text{trace}(L) := L + \overline{L} = 2x$
- norm $N(L) := L \cdot \overline{L} = x^2 - y^2 d$

Proposition 1.1

Let L, L_1, $L_2 \in \mathbb{Q}[\sqrt{d}]$. The the following are true:

- $\overline{L_1 + L_2} = \overline{L_1} + \overline{L_2}$
- $\overline{L_1 L_2} = \overline{L_1 L_2}$
- $N(L_1 L_2) = N(L_1) N(L_2)$
- $N(L) = 0 \iff L = 0$.

Proof The first three properties can be derived from direct computation of conjugate and norm. We only give the proof for the last one.

If $L = 0$, the clearly $N(L) = 0$. Now we assume that $N(L) = 0$, and try to prove that $L = 0$. Let $L = x + y\sqrt{d}$. Thus

$$0 = N(L) = x^2 - y^2\sqrt{d}$$

(to be continued ...) ■

1.3 Algebraic Integers

Definition 1.2

The number $L \in \mathbb{Q}[\sqrt{d}]$ is said to be an *algebraic integer* if $T(L) \in \mathbb{Z}$ and $N(L) \in \mathbb{Z}$.

What are the algebraic numbers in $\mathbb{Q}[\sqrt{d}]$? The theorem below illustrates this

Theorem 1.2

The set of all algebraic, aka quadratic ring, *of* $\mathbb{Q}[\sqrt{d}]$ *is*

$$\begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Definition 1.3

An algebraic integer L is said to be a *unit* if its inverse L^{-1} is also an algebraic integer.

Proposition 1.3

Let L be an algebraic integer. Then L is a unit if and only if $N(1) = \pm 1$.

Yeah, I know it's boring to have "theorem, definition" style, but let's keep it that way.