Contents

Part I

Linear Algebra

Part II

Field Theory

Part III

Ring Theory

Part IV

Number Theory

Chapter 1

The Ideal Class Group

Definition 1. Let K be an algebraic number field, $\mathcal{O}_K$ its ring of integers. The constant H_K for which all $\alpha \in K$ there exists a $\beta \in \mathcal{O}_K$ and a nonzero integer $t \in \mathbb{Z} \setminus \{0\}$ with $|t| \leq H_K$ such that

$$|N(t\alpha - \beta)| < 1$$

is called the Hurwitz constant.

Example 1.1. Let $K = \mathbb{Q}(\sqrt{-5})$ be an algebraic number field.

Proof. □

Definition 2 (Equivalence of Fractional Ideals)**.** Let R be a integral domain. Two fractional ideals $\mathcal{A}$ and $\mathcal{B}$ of R are said to be equivalent if there exist α and β in R such that

$$(\alpha)\mathcal{A} = (\beta)\mathcal{B}.$$

In this case, we write $\mathcal{A} \sim \mathcal{B}$ or simply $\mathcal{A} = \mathcal{B}$. Indeed, this relation is a equivalence relation.

Proof. Let $\mathcal{A}$ and $\mathcal{B}$ be two fractional ideals of an integral domain R. We show that the relation $\mathcal{A} \sim \mathcal{B}$ as defined above is a equivalence relation.

1. **Reflexivity.** Trivially, $(\alpha)\mathcal{A} = (\alpha)\mathcal{A}$ for any $\alpha \in R$, and we have $\mathcal{A} \sim \mathcal{A}$.

2. **Symmetry.** If $\mathcal{A} \sim \mathcal{B}$, then $(\alpha)\mathcal{A} = (\beta)\mathcal{B}$, and again it is trivial that $(\beta)\mathcal{B} = (\alpha)\mathcal{A}$, hence $\mathcal{B} \sim \mathcal{A}$.

3. **Transitivity.** Let $\mathcal{A} \sim \mathcal{B}$ and $\mathcal{B} \sim \mathcal{C}$ hold. There are $\alpha, \beta, \gamma, \theta \in R$ such that

   $$(\alpha)\mathcal{A} = (\beta)\mathcal{B} \quad \text{and} \quad (\gamma)\mathcal{B} = (\theta)\mathcal{C}.$$

   Multiplying both sides of both equalities by (γ) and (β) respectively yields

   $$(\gamma)(\alpha)\mathcal{A} = (\gamma)(\beta)\mathcal{B} \quad \text{and} \quad (\beta)(\gamma)\mathcal{B} = (\beta)(\theta)\mathcal{C}.$$

   Therefore, we have that $(\alpha\gamma)\mathcal{A} = (\beta\theta)\mathcal{C}$ or in other words $\mathcal{A} \sim \mathcal{C}$.

□

Theorem 3. Each equivalence class of fractional ideals has an integral ideal representative.

Theorem 4. The number of equivalence classes of fractional ideals of a integral domain is finite.

Definition 5. The class number of an algebraic number field K, denoted by $h(K)$ is the cardinality of the group of equivalence classes of fractional ideals.

Example 5.1. The class number of $K = \mathbb{Q}(\sqrt{-5})$ is 2.

Proof. The ring of integer of K is $\mathbb{Z}[\sqrt{-5}]$ that has the integral basis $\left\{1, \sqrt{-5}\right\}$. For the integral basis we have the conjugations

$$1^{(1)} = 1 \qquad \sqrt{-5}^{(1)} = \sqrt{-5}$$
$$1^{(2)} = 1 \qquad \sqrt{-5}^{(2)} = -\sqrt{-5}$$

and we can compute the Hurwitz constant

$$H_K = \left(|1| + |\sqrt{-5}|\right)\left(|1| + |-\sqrt{-5}|\right) = (1 + \sqrt{5})^2 = 10.47\dots$$

□

Diophantine Equations

Example 5.2. The equation $x^2 + 5 = y^3$ has no integral solution.

Proof. Assume there are integers x and y that solve the equation above.

1. **y must be odd.** If y is even, then $y^3 = x^2 + 5$ is even too, so x^2 is odd implying x is odd. Moreover, if y is even, then y^3 is divisible by 4, so $x^2 + 5 \equiv 0 \mod 4$, hence $x^2 \equiv 3 \mod 4$, but this is impossible because squares of integers are congruent to 0 or 1 modulo 4. Therefore, y cannot be even.

2. **x and y are coprime.** If there is a prime that divides both x and y, then p also divides $y^3 = x^2 + 5$, so p divides 5 because x^2 is divisible by p. p divides 5 implies $p = 5$. If we divide the given equation by 5, we get

$$\frac{x^2}{5} + 1 = \frac{y^3}{5}.$$

$5^{-1}x^2$ and $5^{-1}y^3$ are still divisible by 5, so reducing this equation modulo 5 yields

$$1 \equiv 0 \mod 5$$

which cannot be. Thus, x and y are coprime.

Consider the factorization $(x + \sqrt{-5})(x - \sqrt{-5}) = y^3$ in the ring of integers $\mathbb{Z}[\sqrt{-5}]$. We will investigate the ideals generated by the factors, i.e. $(x + \sqrt{-5})$ and $(x - \sqrt{-5})$.

3. **The ideals $(x + \sqrt{-5})$ and $(x - \sqrt{-5})$ of $\mathbb{Z}[\sqrt{-5}]$ are coprime ideals.** Suppose there is a prime ideal $\mathfrak{p}$ that divides the greatest common divisor of $(x + \sqrt{-5})$ and $(x - \sqrt{-5})$. By definition, we have

$$\mathfrak{p} \supseteq \gcd((x + \sqrt{-5}), (x - \sqrt{-5})) = (x + \sqrt{-5}) + (x - \sqrt{-5}) = (2x),$$

i.e. $\mathfrak{p}$ divides $(2x)$. On the other hand, since $\mathfrak{p}$ divides both factors of (y^3), we have that $\mathfrak{p}$ divides (y) too. y was odd, so $\mathfrak{p}$ does not divide (2), thus $\mathfrak{p}$ divides (x). But $\mathfrak{p}$ cannot divide both (x) and (y) since they were coprime. Hence $(x + \sqrt{-5})$ and $(x - \sqrt{-5})$ are coprime ideals.

There are ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathbb{Z}[\sqrt{-5}]$ such that

$$\mathfrak{a}^3 = (x + \sqrt{-5}) \quad \text{and} \quad \mathfrak{b}^3 = (x - \sqrt{-5}).$$

4. **$\mathfrak{a}$ and $\mathfrak{b}$ are principal.**

$\square$