GAUSS'S GENUS THEORY

XUEJUN GUO

Department of Mathematics, Columbia University

Abstract: This short note is based on Hilbert's Zahlbericht.

1. **Notations**

Let $F = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, where d is a square free integer. Let $\mathrm{Gal}(F/\mathbb{Q}) = \{1,\ \sigma\}$. Let D be the discriminant of F. For each nontrivial positive square free divisor m of D, let $[m]$ be the product of the distinct ramified primes above the prime divisors of m. Let $\mathrm{Cl}(F)$ be the class group of F, $\mathrm{Cl}^+(F)$ the narrow class group of F. Let

$$\alpha = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2 \text{ or } 3,\ \pmod 4, \\ (1+\sqrt{d})/2, & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{2.1}$$

Then $\{1,\ \alpha\}$ is a basis of $\mathcal{O}_F$.

Let ${}_2\mathrm{Cl}^+(F)$ be the 2-torsion elements of $\mathrm{Cl}^+(F)$. Assume that $I \in {}_2\mathrm{Cl}^+(F)$. Then $I^2 = (x)$ for some totally positive $x \in F$. Then $\mathrm{Norm}_{F/\mathbb{Q}}(x) = \mathrm{Norm}_{F/\mathbb{Q}}(I)^2 = a^2$ for some positive $a \in \mathbb{Q}$. Hence by the Hilbert 90,

$$x = a \cdot \frac{y}{\sigma(y)},$$

for some $y \in F$. We can assume that y has no rational factor and y is totally positive (the reason is that $y/\sigma(y)$ is totally positive). Hence

$$x = a \cdot \mathrm{Norm}_{F/\mathbb{Q}}(y) \cdot \frac{1}{\sigma(y)^2}.$$

Let $b = a \cdot \mathrm{Norm}_{F/\mathbb{Q}}(y)$ and $J = (\sigma(y))I$. Then $I = J \in {}_2\mathrm{Cl}^+(F)$ and $J^2 = (b)$, where $b \in \mathbb{Q}$.

We just prove that any $I \in {}_2\mathrm{Cl}^+(F)$ is equivalent to some J such that $J^2 = (b)$, where $b \in \mathbb{Q}$. By multiplying some positive rational to J, we can assume that b is a square free integer. Hence we get a very important result

$$b|D.$$

Hence we prove that ${}_2\mathrm{Cl}^+(F)$ is generated by the ramified prime ideals. Assume that there are t ramified primes in F. Assume that there are t-ramified primes in F.

Gauss's genus theory says that

$$\#({}_2\mathrm{Cl}^+(F)) = 2^{t-1}.$$

We will study the linear dependence of the ramified primes.

2. Imaginary quadratic number field

In this section, d is negative but distinct from -1 and -3. The result is very easy. The only relation is that $(\sqrt{d}) = 1 \in {}_2\mathrm{Cl}^+(F) = {}_2\mathrm{Cl}(F)$.

3. Real quadratic number field

In this section, d positive. The result is a little different. Let ε be the fundamental unit.

If $\mathrm{Norm}_{F/\mathbb{Q}}(\varepsilon) = -1$, then only relation is that $(\varepsilon\sqrt{d}) = 1 \in {}_2\mathrm{Cl}^+(F) = {}_2\mathrm{Cl}(F)$ or $(-\varepsilon\sqrt{d}) = 1 \in {}_2\mathrm{Cl}^+(F) = {}_2\mathrm{Cl}(F)$.

If $\mathrm{Norm}_{F/\mathbb{Q}}(\varepsilon) = 1$, then by Hilbert 90, $\varepsilon = y/\sigma(y)$ for some $y \in F$. We have seen that y can be chosen to be totally positive and integral and divided only by the ramified primes. Hence the only relation is $(y) = 1 \in {}_2\mathrm{Cl}^+(F)$.

4. It is very easy to compute y in the relation if you know ε

Let $d = 21$. Then $\varepsilon = (5+\sqrt{21})/2$. Assume that $y = \alpha + \beta\sqrt{21}$. Then

$$\begin{aligned}\frac{5+\sqrt{21}}{2} &= \frac{y}{\sigma y}\\ &= \frac{\alpha+\beta\sqrt{21}}{\alpha-\beta\sqrt{21}}\\ &= \frac{\alpha^2+21\beta^2+2\alpha\beta\sqrt{21}}{\alpha^2-21\beta^2}\end{aligned}$$

which implies

$$\begin{aligned}2(\alpha^2+21\beta^2) &= 5(\alpha^2-21\beta^2),\\ \alpha^2-21\beta^2 &= 4\alpha\beta.\end{aligned}$$

Hence $\alpha = 7\beta$. Hence we can let $y = (7+\sqrt{21})/2$. Therefore $[7] = 1$ and ${}_2\mathrm{Cl}^+(F)$ is generated by $[3]$.

References

[1] D. Hilbert, The theory of algebraic number fields.