23. An Elementary Proof of Gauss' Genus Theorem

By Fidel NEMENZO and Hideo WADA
Department of Mathematics, Sophia University

(Communicated by Shokichi IYANAGA, M. J. A., April 13, 1992)

§ 1. **Preliminaries.** Let $m\neq 1$ be a square-free integer and d the discriminant of $K=\boldsymbol{Q}(\sqrt{m})$. If A and B are ideals in K such that $A=(\rho)B$ and $N\rho>0$, we write $A\approx B$. Let $p_1,\cdots,p_s$ be the odd prime divisors of m. We shall prove the next theorem without using Dirichlet's theorem of arithmetical progressions.

Theorem 1 (Gauss). *Let A be an ideal such that $(A,d)=1$. Then $A\approx B^2$ for some ideal B if and only if* $\left(\frac{NA}{p_i}\right)=1$, $1\leq i\leq s$.

First we prove the next proposition.

Proposition 1. *Let A be an ideal. Then $A\approx B^2$ for some ideal B if and only if there exists a non-zero integer z and $\alpha\in A$ such that* $z^2=\dfrac{N\alpha}{NA}$.

Proof. Let $A=\rho B^2$ with $N\rho>0$. If $0\neq\beta\in B$, then $\rho\beta^2\in A$ and $\dfrac{N(\rho\beta^2)}{NA}=\left(\dfrac{N\beta}{NB}\right)^2$. Conversely, let $z^2=\dfrac{N\alpha}{NA}$, where $z\in N$ and $\alpha\in A$. Let C be an ideal such that $(\alpha)=AC$. We may assume that C is primitive. Then $z^2=NC$. If $p\,|\,z$ then since C is primitive, p decomposes in K, i.e., $(p)=PP^\sigma$, $P\neq P^\sigma$. If $p^m\|z$ and $P\,|\,C$, then $P^{2m}\|C$, $P^\sigma\nmid C$. Therefore $A\approx(\prod_{p^m\|z}P^{\sigma m})^2$.

If K is real, let r_n be the 2-rank of the ideal class group in the narrow sense and r_w be that of the ideal class group in the wide sense. Then we have the next corollary (cf. [1], [3], [4]).

Corollary. $r_n=r_w\Leftrightarrow p_i\equiv 1 \pmod 4$, $1\leq i\leq s$.

Proof. $r_n=r_w\Leftrightarrow(\sqrt{m})\approx B^2$ for some ideal B. When $m\not\equiv 1 \pmod 4$, then $(\sqrt{m})=[m,\sqrt{m}]$. Writing $\alpha=mx+\sqrt{m}y\in(\sqrt{m})$, we get $\dfrac{N\alpha}{N(\sqrt{m})}=mx^2-y^2$. Therefore

$$r_n=r_w \Leftrightarrow mx^2=y^2+z^2 \text{ has a non-trivial integral solution}$$
$$\Leftrightarrow p_i\equiv 1 \pmod 4,\quad 1\leq i\leq s.$$

If $m\equiv 1 \pmod 4$, then $(\sqrt{m})=\left[m,\dfrac{m+\sqrt{m}}{2}\right]$. We get similarly the same result.

§ 2. **Proof of Theorem 1.** Let A be a primitive ideal such that $(A,d)=1$. We can write $A=\left[a,\dfrac{b+\sqrt{d}}{2}\right]$ where $NA=a>0$ and $a\,|\,N\left(\dfrac{b+\sqrt{d}}{2}\right)$. Hence

$$b^2-4ac=d \tag{1}$$