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* $z^2=\frac{N\alpha}{NA}$.

Proof. Let $A=\rho B^2$ with $N\rho>0$. If $0\neq\beta\in B$, then $\rho\beta^2\in A$ and $\frac{N(\rho\beta^2)}{NA}=\left(\frac{N\beta}{NB}\right)^2$. Conversely, let $z^2=\frac{N\alpha}{NA}$, 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 $p\mid z$ then since C is primitive, p decomposes in K, i.e., $(p)=PP^\sigma$, $P\neq P^\sigma$. If $p^m\| z$ and $P\mid C$, 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 $\frac{N\alpha}{N(\sqrt{m})}=mx^2-y^2$. Therefore

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

If $m\equiv 1 \pmod 4$, then $(\sqrt{m})=\left[m,\frac{m+\sqrt{m}}{2}\right]$. 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 $A=\left[a,\frac{b+\sqrt{d}}{2}\right]$ where $NA=a>0$ and $a\mid N\left(\frac{b+\sqrt{d}}{2}\right)$. Hence

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

for some integer c. Writing $\alpha=ax+\frac{b+\sqrt{d}}{2}y\in A$, we have

$$N\alpha=\left(ax+\frac{b}{2}y\right)^2-\frac{d}{4}y^2.$$

Therefore

$$\frac{N\alpha}{NA}=z^2\Leftrightarrow(2ax+by)^2-dy^2=a(2z)^2. \tag{2}$$

Write $a=a_1a_2^2$ where a_1 is square-free. From Proposition 1 and (2), we get

$$A\approx B^2\Leftrightarrow a_1x^2+my^2=z^2 \text{ has a non-trivial solution.} \tag{3}$$

If a and b are non-zero rational integers, we shall write aRb whenever a is a square modulo b. We need the next theorem.

Theorem 2 (Legendre). *Let a and b be positive square-free integers. Then $ax^2+by^2=z^2$ has a non-trivial solution if and only if aRb, bRa, and $-\frac{ab}{(a,b)^2}R(a,b)$.* (An elementary proof can be found in [2].)

Now mRa_1 follows from (1). Since $(a_1,m)=1$, we get $-\frac{a_1m}{(a_1,m)^2}R(a_1,m)$. Therefore if $m>0$, then

$$\begin{aligned}A\approx B^2&\Leftrightarrow a_1Rm\\&\Leftrightarrow a_1Rp_i,\quad 1\le i\le s\\&\Leftrightarrow\left(\frac{a}{p_i}\right)=1,\quad 1\le i\le s.\end{aligned}$$

If $m=-m_1<0$, then

$$\begin{aligned}A\approx B^2&\Leftrightarrow a_1x^2=m_1y^2+z^2\\&\Leftrightarrow(a_1x)^2=a_1m_1y^2+a_1z^2\\&\Leftrightarrow a_1m_1Ra_1,\quad a_1Ra_1m_1,\quad\text{and}\quad -m_1Ra_1\\&\Leftrightarrow a_1Rm.\end{aligned}$$

This completes the proof of Theorem 1.

References

[1] D. Hilbert: Zahlbericht. §77, Satz 108.

[2] K. Ireland and M. Rosen: A Classical Introduction to Modern Number Theory. GTM 84, Springer-Verlag (1982).

[3] P. Kaplan: Comparaison des 2-groupes des classes d'idéaux au sens large et au sens étroit d'un corps quadratique réel. Proc. Japan Acad., **50**, 688–693 (1974).

[4] M. Saito and H. Wada: Tables of ideal class groups of real Quadratic fields. ibid., **64**A, 347–349 (1988).