ON GENERA OF BINARY QUADRATIC FORMS

IRVING REINER

Let $\beta = ax^2+2bxy+cy^2$ be a properly primitive form with integral coefficients, and let the determinant $D=ac-b^2$ be written as $D=\pm 2^s\Delta$, where Δ is odd and positive, and the factorization of Δ into distinct primes is $\Delta = q_1^{\alpha_1}\cdots q_r^{\alpha_r}$. Let us suppose that a is positive and prime to $2D$. The genus of β is then completely determined by the Legendre symbols $(a|q_1), \cdots, (a|q_r)$, and $(-1|a)$ if $D\equiv 0$ or 1 (mod 4), $(2|a)$ if $D\equiv 0$ or 6 (mod 8), and $(-2|a)$ if $D\equiv 0$ or 2 (mod 8).[1] These characters are not independent, however, since $-D=b^2-ac$ and $(a, b)=1$ imply that $(-D|a)=1$; from this, using the law of quadratic reciprocity, we get

$$\begin{aligned} 1 = (-D\mid a) &= (2\mid a)^s(a\mid \Delta)(-1)^{(a-1)(\mp\Delta-1)/4} \\ &= \epsilon\cdot(a\mid q_1)^{\alpha_1}\cdots(a\mid q_r)^{\alpha_r}, \end{aligned}$$

where

$$\epsilon = (2\mid a)^s(-1\mid a)^{(\mp\Delta-1)/2}$$

is a character or is trivially $+1$. Thus, the characters of any existing genus must satisfy

$$\epsilon\cdot(a\mid q_1)^{\alpha_1}\cdots(a\mid q_r)^{\alpha_r} = +1. \tag{1}$$

Conversely, given any set of characters satisfying (1), a long but elementary proof showing the existence of the corresponding genus was given by Gauss,[2] who used the method of composition of forms; he also demonstrated by this means that all existing primitive genera of the same determinant contain the same number of classes.[2] Elementary proofs were also given by Hilbert for the analogous case of ideal classes in quadratic fields.[3] The purpose of this paper is to furnish, by use of Dirichlet's theorem on the infinitude of primes in an arithmetic progression, simple proofs of the results mentioned above for forms with integral coefficients. These may be stated precisely as follows:

THEOREM 1. *For any preassigned set of characters satisfying* (1), *there exists a genus with the given characters.*

Received by the editors February 1, 1945, and, in revised form, August 2, 1945.

[1] Mathews, *Theory of numbers*, Part I, 1927 reprint, p. 134.

[2] Gauss, *Disquisitiones arithmeticae*, arts. 234–265.

[3] Hilbert, Jber. Deutschen Math. Verein. vol. 4 (1894–1895) pp. 286–316.