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.

THEOREM 2. *All existing properly primitive genera of binary quadratic forms of a given determinant contain the same number of classes.*

Remark. The proofs given in this paper may easily be extended to the case of primitive forms with odd middle coefficient.

For the proof of Theorem 1, we observe that by Dirichlet's theorem, a prime a may be found such that $(a, 2D)=1$ and the set of Legendre symbols $(a|q_1), \cdots, (a|q_r)$ and $(-1|a)$ or $(2|a)$ or $(-2|a)$ (or combinations of the last three symbols, depending on the value of D) coincide with the preassigned set of values of the characters. (1) then implies that $(-D|a)=+1$, whence there exists an integer b for which $b^2\equiv -D \pmod{a}$, that is, $-D=b^2-ac$ with integral a, b and c; the form $ax^2+2bxy+cy^2$ then has the preassigned characters.

The proof of Theorem 2 will proceed as follows: Let $\beta_1, \cdots, \beta_k$ be nonequivalent representative forms of the classes in a given genus β, and let $\phi_1, \cdots, \phi_{k'}$ be the forms of another given genus ϕ, both genera having the same determinant. It is sufficient to show that we can find a transformation taking the β_i into the ϕ_j, and that no two of the ϕ_j thus obtained are equivalent. In that case $k' \geqq k$. By reversing the process, we shall have $k \geqq k'$, from which it will follow that $k=k'$, which gives the theorem.

The following will be shown:

A. Starting with a form β of a given genus, it can be transformed into a form $p\phi$, where ϕ is a form in another given genus of the same determinant as β, and where p is a prime determined by the genera β and ϕ.

B. If from β_1 and β_2 we get forms ϕ_1 and ϕ_2, then $\phi_1 \sim \phi_2$ implies $\beta_1 \sim \beta_2$.[4]

Let the given form be $\beta=ax^2+2bxy+cy^2$, and set $ac-b^2=D=\pm 2^s\Delta$ as before. Let p be a prime such that $(p, 2aD)=1$ and $(-D|p)=1$. Then there exist integers x and y, with $y \not\equiv 0 \pmod{p}$, such that

$$(ax+by)^2 \equiv -Dy^2 \pmod{p}.$$

Hence there exists an integer r for which

$$ar^2+2br+c \equiv 0 \pmod{p}.$$

The transformation J:

$$x \rightarrow px+ry, \qquad y \rightarrow y$$

[4] The notation $\phi_1 \sim \phi_2$ will mean that ϕ_1 is equivalent to ϕ_2, that is, there is a transformation with integral elements and of determinant $+1$ taking ϕ_1 into ϕ_2.

of determinant p takes β into $p\psi$, where

$$\psi = apx^2 + 2(ar + b)xy + dy^2,$$

and d is an integer; it is clear that β and ψ have the same determinant.

Let $\phi = a'x^2 + 2b'xy + c'y^2$ be a form of another given genus of the same determinant as β. If we show that p can be chosen so that $\psi \text{ v } \phi$,[5] we shall have proved A. Since β and ϕ are representatives of classes of properly primitive forms, and in every such class there is a form with leading coefficient odd and prime to the determinant of the form,[6] we may take $(a, 2D) = (a', 2D) = 1$. If the following relations are satisfied it will follow that $\psi \text{ v } \phi$, for their generic characters will be the same.

$$(2) \qquad \begin{gathered} (ap \mid q_1) = (a' \mid q_1), \cdots, (ap \mid q_r) = (a' \mid q_r), \\ (-1 \mid ap) = (-1 \mid a'), \qquad (2 \mid ap) = (2 \mid a'). \end{gathered}$$

From these we may conclude that $(-D|ap) = (-D|a')$. Since $(-D|a) = (-D|a') = 1$, this means that $(-D|p) = 1$. Hence, if we choose a prime p which satisfies (2) and is prime to $2aD$ (this is possible by Dirichlet's theorem), then there exists a transformation J taking β into ϕ. This completes the proof of A.

To prove B, let $\beta_1 \text{ v } \beta_2$; we may choose $\beta_1 \equiv \beta_2 \pmod{p}$, for we shall show that there exists a form in the class of β_2 which is congruent (mod p) to β_1. To show this, it is sufficient to show that by a transformation of determinant $+1$, β_2 may be taken into a form congruent to β_1. Let

$$(3) \qquad \beta_1 = a_1x^2 + 2b_1xy + c_1y^2, \qquad \beta_2 = a_2x^2 + 2b_2xy + c_2y^2,$$

where $(a_1, 2D) = (a_2, 2D) = 1$. If all congruences are modulo p, the congruence

$$a_2\beta_2 \equiv (a_2x + b_2y)^2 + Dy^2 \equiv a_1a_2$$

certainly has a solution with not both x and y congruent to 0, provided that we impose the restriction $(p, 2a_1a_2D) = 1$. Let $x = x_0$, $y = y_0$ be such a solution, and choose integers x_1 and y_1 such that $x_0y_1 - x_1y_0 = 1$. The transformation of determinant $+1$:

$$x \to x_0x + (x_0t + x_1)y, \qquad y \to y_0x + (y_0t + y_1)y$$

takes β_2 into a form

$$\beta_3 = a_3x^2 + 2(a_3t + b_3)xy + c_3y^2,$$

[5] $\phi_1 \text{ v } \phi_2$ means that ϕ_1 and ϕ_2 are of the same genus.

[6] Mathews, loc. cit. p. 133.

where $a_3 \equiv a_1 \not\equiv 0$. If we choose t so that $a_3t + b_3 \equiv b_1$, it is clear from the fact that β_1 and β_3 have the same determinant that $\beta_3 \equiv \beta_1 \pmod{p}$.

Thus, let $\beta_2 \equiv \beta_1 \pmod{p}$, where β_1 and β_2 are defined by equations (3). The transformation J obtained for β_1 may also be used for β_2. If now ϕ_1 and ϕ_2 are equivalent forms obtained from β_1 and β_2 respectively by use of J, and if A takes ϕ_1 into ϕ_2, then JAJ^{-1} takes β_1 into β_2. Let

$$A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.$$

Then

$$\begin{aligned} JAJ^{-1} &= \begin{bmatrix} p & r \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1/p & -r/p \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} \alpha + r\gamma/p & -r\alpha - r^2\gamma/p + p\beta + r\delta \\ \gamma/p & -r\gamma/p + \delta \end{bmatrix}. \end{aligned}$$

If we show that p divides γ we are through, since $|A| = 1$ implies $|JAJ^{-1}| = 1$, whence $\beta_1 \sim \beta_2$. We have

$$\phi_1 = a_1px^2 + 2(a_1r + b_1)xy + d_1y^2,$$
$$\phi_2 = a_2px^2 + 2(a_2r + b_2)xy + d_2y^2.$$

Since A takes ϕ_1 into ϕ_2, we obtain

$$a_1p\alpha^2 + 2(a_1r + b_1)\alpha\gamma + d_1\gamma^2 = a_2p,$$
$$a_1p\alpha\beta + (a_1r + b_1)(\alpha\delta + \beta\gamma) + d_1\gamma\delta = a_2r + b_2.$$

If all congruences are modulo p, we have

$$2(a_1r + b_1)\alpha\gamma + d_1\gamma^2 \equiv 0, \quad (a_1r + b_1)(\alpha\delta + \beta\gamma) + d_1\gamma\delta \equiv a_2r + b_2.$$

If d is eliminated between these two congruences and the fact that $\alpha\delta - \beta\gamma = 1$ is used, it follows that

$$\gamma(a_1r + b_1) \equiv -\gamma(a_2r + b_2).$$

If p does not divide γ, then this shows that $a_1r + b_1 \equiv 0$, since $\beta_1 \equiv \beta_2$. But in this case it follows that $b_1r + c_1 \equiv 0$, by virtue of $a_1r^2 + 2b_1r + c_1 \equiv 0$. Eliminating r between the two congruences, we get $D = a_1c_1 - b_1^2 \equiv 0$, or $(p, D) \neq 1$. Since this is impossible, p must divide γ, and Theorem 2 is proved.

Cornell University