ON RATIONAL AUTOMORPHS OF BINARY QUADRATIC FORMS*

BY GORDON PALL

1. *Introduction.* We consider in this paper those rational automorphs which carry an integral solution (x, y) of

$$ax^2 + bxy + cy^2 = n \tag{1}$$

into an integral solution. Further properties are treated in §§6, 7.

By classical methods for finding all algebraic automorphs, and expressing the conditions for the coefficients to be rational, we have the following known result.

THEOREM 1. *The general proper rational automorph (of determinant* 1*) of a primitive form* $f = [a, b, c]$ *of non-zero discriminant* $d = b^2 - 4ac$ *is*

$$A = \begin{pmatrix} (t - bu)/2 & -cu \\ au & (t + bu)/2 \end{pmatrix}, \tag{2}$$

and the general improper rational automorph (of determinant -1*) is*

$$B = \begin{pmatrix} (t - bu)/2 & (b/a)(t - bu)/2 + cu \\ au & -(t - bu)/2 \end{pmatrix}, \tag{3}$$

where t, u *range over all rational solutions of*

$$t^2 - du^2 = 4. \tag{4}$$

The reciprocal automorph is obtained from (2) by changing u to $-u$, from (3) by changing the signs of both t and u; thus $B^{-1} = -B$.

2. *Denominator of a Rational Automorph.* The *denominator* of a rational automorph is the least common denominator of its four coefficients. To obtain all automorphs (2) having denominator m we write $t = T/m$, $u = U/m$, where T, U, m are any integers satisfying

$$T^2 - dU^2 = 4m^2, \qquad \text{g.c.d. } (m, U) = 1. \tag{5}$$

* Presented to the Society, October 26, 1935.

For any common divisor of m, aU, $(T+bU)/2$, $(T-bU)/2$, cU is a divisor of aU, bU, cU, and hence is 1, f being primitive.

Let Δ denote the denominator of (3) with the substitution $t=T/m$, $u=U/m$ satisfying (5). Evidently $\Delta \mid am$. Further $aU/m=k/\Delta$, $U/m=k/(a\Delta)$, where U/m is in lowest terms. Hence $m \mid a\Delta$.

3. *Transform of an Automorph.* If A is a rational automorph of f, and S is a unitary integral transformation carrying f into $f'=[a', b', c']$, then $A' \equiv S^{-1}AS$ is a rational automorph of f' having the same denominator as A. For multiplication by integral matrices cannot increase the denominator, and we can solve for $A=SA'S^{-1}$.

Let ξ_i denote the matrix of one column consisting of two elements x_i, y_i. Let the integral solution ξ_1 of (1) be carried into the integral solution $\xi_2=A^{-1}\xi_1$, by the rational automorph A. Then the automorph $S^{-1}AS$ of f' carries the integral solution $S^{-1}\xi_1$ of

$$a'x^2 + b'xy + c'y^2 = n \tag{6}$$

into the integral solution $S^{-1}\xi_2$ of (6).

4. THEOREM 2. *The denominator of any rational automorph of* $[a, b, c]$ *which carries an integral solution of* (1) *into an integral solution must be a divisor of* n.

As regards (2), we merely multiply by $-y$ and x and combine

$$\frac{1}{2}(T - bU)x - cUy \equiv 0, \quad aUx + \frac{1}{2}(T + bU)y \equiv 0 \pmod{m},$$

to obtain $U(ax^2+bxy+cy^2)\equiv 0$, whence $n\equiv 0 \pmod{m}$.

For (3) we have similarly $aUx-(T-bU)y/2\equiv 0 \pmod{m}$,

$$\frac{1}{2}(T - bU)ax + \left\{\frac{1}{2}(T - bU)b + acU\right\}y \equiv 0 \pmod{am},$$

whence $(T+bU)ax/2+acUy\equiv 0 \pmod{m}$, $aU(ax^2+bxy+cy^2)\equiv 0$, and finally $an\equiv 0 \pmod{m}$. Thus $\Delta \mid a^2n$. Employing as in §3 an equivalent form with a' prime to a, $\Delta \mid a'^2n$. Hence $\Delta \mid n$.

5. THEOREM 3. *Any two integral solutions of* (1) *can be transformed into each other by proper (and improper) rational automorphs of* $[a, b, c]$.

For from $ax_i^2+bx_iy_i+cy_i^2=n$, $(i=1, 2)$, follows

$$T^2 - dU^2 = 4n^2, \quad T = 2ax_1x_2 + b(x_1y_2 + x_2y_1) + 2cy_1y_2, \quad U = x_1y_2 - x_2y_1. \tag{7}$$

Let A denote (2) with $(t, u)=(T/n, -U/n)$. We find that $A^{-1}\xi_1=\xi_2$. If B denotes (3) for this (t, u), $B\xi_1=(x_2+by_2/a, -y_2)$.

Let $\delta=$g.c.d.(x_2, y_2). Let the unitary transformation

$$S = \begin{pmatrix} x_2/\delta & h \\ y_2/\delta & k \end{pmatrix}, \qquad (kx_2 - hy_2 = \delta),$$

carry f into f', where $a'=n/\delta^2$. Evidently $S^{-1}\xi_2$ is the solution $x=\delta$, $y=0$ of (6). Define T', U' by (7) with f' for f, $S^{-1}\xi_1$ and $S^{-1}\xi_2$ for ξ_1 and ξ_2, and let B' denote the corresponding automorph (3) of f' with $t=-T'/n$, $u=U'/n$. Then B' carries $S^{-1}\xi_1$ into $S^{-1}\xi_2$, and the automorph $SB'S^{-1}$ of f carries ξ_1 into ξ_2.

6. *Product of Rational Automorphs.* Let A_i and B_i denote (2) and (3), respectively, with $(t, u)=(T_i/m_i, U_i/m_i)$; and let $m_3=m_1m_2$, $T_i^2-dU_i^2=4m_i^2$, $(i=1, 2, 3)$. Then $A_1A_2=A_3$ and $A_1B_2=B_3$, where

$$2T_3 = T_1T_2 + dU_1U_2, \qquad 2U_3 = T_1U_2 + T_2U_1. \tag{8}$$

Also $B_1B_2=A_3$ and $B_1A_2=B_3$, where in place of (8) we have

$$2T_3 = T_1T_2 - dU_1U_2, \qquad 2U_3 = U_1T_2 - U_2T_1. \tag{9}$$

COROLLARIES. $A_1A_2=A_2A_1$, $B_1B_2=(B_2B_1)^{-1}$, $A_1B_2=A_2B_1=B_1A_2^{-1}=B_2A_1^{-1}$.

7. *Rational Automorphs of Denominator mn.* It is not in general true, even if m and n are relative-prime, that a rational automorph of denominator mn can be expressed as a product of rational automorphs of denominators m and n. This is true of a wide variety of classes even with $h(d)>1$; for example, of $[2, 1, 3]$ of discriminant $d=-23$. But for the principal form $[1, 1, 6]$ of this discriminant there are rational automorphs of denominator 6, but none (proper or improper) of denominators 2 and 3.

The parametric solution of (5) may be useful; for each factorization $d=rs$, we have $m=(ru_1^2-su_2^2)/4$, $u=u_1u_2$, $t=(ru_1^2+su_2^2)/2$, where u_1 and u_2 are integers of g.c.d. 1 or 2, and m is an integer prime to u.

Two rational automorphs A_1 and A_2 of f may be called *right-equivalent* if there exists an integral automorph I of f such that $A_1 I = A_2$. If (T_1, U_1) and (T_2, U_2) belong to the same set* of solutions of (5), the corresponding automorphs (with $t = T_i/m$, $u = U_i/m$) are readily seen to be right-equivalent.

McGILL UNIVERSITY

A NOTE ON RECURSIVE FUNCTIONS†

BY S. C. KLEENE

The notion of a recursive function of natural numbers, which is familiar in the special cases associated with primitive recursions, Ackermann-Péter multiple recursions, and others, has received a general formulation from Herbrand and Gödel. The resulting notion is of especial interest, since the intuitive notion of a "constructive" or "effectively calculable" function of natural numbers can be identified with it very satisfactorily.‡ Consider the operation of passing from a function $\rho(x_1, \cdots, x_n, y)$, such that for each set of values of $x_1, \cdots, x_n$ the equation $\rho(x_1, \cdots, x_n, y) = 0$ has solutions for y, to the function "$\epsilon y[\rho(x_1, \cdots, x_n, y) = 0]$" of which the least solution is $x_1, \cdots, x_n$. We have shown that the (general) recursive functions are the functions which are derivable from the primitive recursive functions by one application of this operation and of substitution.§ Herein we note the related result, that the recursive functions are the functions obtainable by repeated applications of the operation just described and of substitution from the three particular functions $x+y$ (sum), $x \cdot y$ (product), δ_y^x (Kronecker delta). This result follows from the other by an adaptation of an argument used by Gödel in proof that every

---

* For definition of set, see Pall, Transactions of this Society, vol. 35 (1933), p. 491; or Dirichlet, *Vorlesungen über Zahlentheorie*, §87.

† Presented to the Society, January 1, 1936.

‡ See A. Church, *An unsolvable problem of elementary number theory*, American Journal of Mathematics, vol. 58 (1936), pp. 345–363, §7.

§ S. C. Kleene, *General recursive functions of natural numbers*, Mathematische Annalen, vol. 112 (1936), No. 5, IV and V.