3/2 (2005), 123–129
tmcs@math.klte.hu
http://tmcs.math.klte.hu

Teaching
Mathematics and
Computer Science

Equivalence and range of quadratic forms

Sándor Szabó

Abstract. If two quadratic forms are equivalent, that is, if there is a linear transformation with integer coefficients and determinant 1 or -1 which takes one form to the other, then their ranges are the same and also their determinants are the same. The result of the paper is that for positive definite binary quadratic forms the converse is also true. Namely, if two positive definite binary quadratic forms of the same determinant have the same range, then they are equivalent. The arguments are guided by geometric considerations.

Key words and phrases: binary quadratic forms, equivalence of quadratic forms, geometry of numbers.

ZDM Subject Classification: F60, G90.

1. Introduction

In 1640 P. Fermat arrived at the result that an odd prime can or cannot be written as a sum of two squares depending on it is congruent to 1 or 3 modulo 4. In other words the range of the quadratic form $x^2 + y^2$ for integer substitutions contains each prime congruent to 1 modulo 4. In 1654 he announced two similar results. If p is a prime $p \equiv 1 \pmod 3$, then the equation $x^2 + 3y^2 = p$ is soluble in integers. If p is a prime $p \equiv 1$ or $3 \pmod 8$, then there are integers x, y such that $x^2 + 2y^2 = p$.

L. Euler extended Fermat's investigations to the $ax^2 + cy^2 = p$ case for various choices of the integers a and c. As a next step in 1775 L. Lagrange turned to studying the solvability of the equation $ax^2 + bxy + cy^2 = n$ in integers. He introduced the concept of equivalence and developed a reduction procedure for quadratic forms.

Plugging $\alpha x' + \beta y'$, $\gamma x' + \delta y'$ in place of x, y respectively in the quadratic form $f = ax^2 + bxy + cy^2$ leads to the quadratic form $f' = a'(x')^2 + b'x'y' + c'(y')^2$. In order to ensure that a', b', c' are integers we choose the coefficients α, β, γ, δ to be integers. To make the relation between f and f' symmetric we choose $\alpha\delta - \beta\gamma$, the determinant of the transformation, to be 1 or -1. The forms f and f' connected in this way are called properly or improperly equivalent corresponding to the determinant is 1 or -1. The quantity $ac - b^2/4$ is called the determinant of the quadratic form f. It turns out that if two quadratic forms are equivalent (properly or improperly), then their ranges are equal and also their determinants are equal. Our purpose is to show that if two positive definite binary quadratic forms of the same determinant have the same range for integer substitutions, then the two forms are equivalent.

In 1831 C. F. Gauss pointed out that there is an intimate connection between positive definite quadratic forms and lattices. Our argument exploits this connection and geometric considerations play an essential part.

2. Quadratic forms and lattices

A basis $\mathbf{u}_1, \mathbf{u}_2$ on the plane naturally gives rise to a positive definite quadratic form f. Namely, if $\mathbf{l} = x_1\mathbf{u}_1 + x_2\mathbf{u}_2$ is a typical vector of the plane, then

$$\mathbf{l}^T\mathbf{l} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} \mathbf{u}_1^T\mathbf{u}_1 & \mathbf{u}_1^T\mathbf{u}_2 \\ \mathbf{u}_2^T\mathbf{u}_1 & \mathbf{u}_2^T\mathbf{u}_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \mathbf{x}^T\mathbf{A}\mathbf{x} = f$$

is a quadratic form, which represents the square of a distance. This connection can be reversed. We can associate a basis $\mathbf{u}_1, \mathbf{u}_2$ with a given positive definite quadratic form

$$f = \mathbf{x}^T\mathbf{A}\mathbf{x} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix},$$

where $a_{12} = a_{21}$. As f is positive definite, it follows that

$$a_{11} > 0, \quad a_{11}a_{22} - a_{12}a_{21} > 0. \tag{1}$$

We try to find the basis vectors in the form

$$\mathbf{u}_1 = \begin{bmatrix} u_{11} \\ 0 \end{bmatrix}, \quad \mathbf{u}_2 = \begin{bmatrix} u_{21} \\ u_{22} \end{bmatrix}.$$

This is only a matter of choosing a coordinate system such that the first coordinate axis is parallel to $\mathbf{u}_1$. Equating

$$\mathbf{U}^T\mathbf{U} = \begin{bmatrix} \mathbf{u}_1^T\mathbf{u}_1 & \mathbf{u}_1^T\mathbf{u}_2 \\ \mathbf{u}_2^T\mathbf{u}_1 & \mathbf{u}_2^T\mathbf{u}_2 \end{bmatrix} = \begin{bmatrix} u_{11}^2 & u_{11}u_{21} \\ u_{11}u_{21} & u_{21}^2 + u_{22}^2 \end{bmatrix}$$

to

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \mathbf{A}$$

leads to the system of equations

$$u_{11}^2 = a_{11}, \quad u_{11}u_{21} = a_{12}, \quad u_{21}^2 + u_{22}^2 = a_{22}$$

which is solvable because of conditions (1). The decomposition

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} u_{11} & 0 \\ u_{21} & u_{22} \end{bmatrix} \begin{bmatrix} u_{11} & u_{21} \\ 0 & u_{22} \end{bmatrix} = \mathbf{U}^T\mathbf{U}$$

is the so-called Cholesky decomposition of $\mathbf{A}$. (For n by n matrices see Proposition 14.26 of [3] page 316.) The equation

$$\det \mathbf{A} = \det(\mathbf{U}^T\mathbf{U}) = \det \mathbf{U}^T \cdot \det \mathbf{U} = \big[\det \mathbf{U}\big]^2$$

shows how the determinant of the quadratic form and the determinant of the lattice are connected.

Replacing $\mathbf{x}$ by $\mathbf{Cx}$ in $f = \mathbf{x}^T\mathbf{Ax}$ results the quadratic form $f' = \mathbf{y}^T\mathbf{A}'\mathbf{y}$, where

$$\mathbf{A}' = \mathbf{C}^T\mathbf{AC} = \mathbf{C}^T\mathbf{U}^T\mathbf{UC} = (\mathbf{UC})^T(\mathbf{UC}).$$

So replacing the variables in f corresponds to replacing the basis vectors $\mathbf{u}_1$, $\mathbf{u}_2$ by $c_{11}\mathbf{u}_1 + c_{21}\mathbf{u}_2$, $c_{12}\mathbf{u}_1 + c_{22}\mathbf{u}_2$ respectively, where

$$\mathbf{C} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}.$$

Conversely, changing the basis corresponds to changing variables in f.

We are interested in the values of the quadratic form $f = \mathbf{x}^T\mathbf{Ax} = (\mathbf{Ux})^T(\mathbf{Ux})$ when the components of $\mathbf{x}$ are integers. Consequently, we consider the set of vectors $\mathbf{Ux} = x_1\mathbf{u}_1 + x_2\mathbf{u}_2$, where x_1, x_2 range through the integers independently. This set of vectors is called a plane lattice or simply a lattice spanned by the basis vectors $\mathbf{u}_1$, $\mathbf{u}_2$. The parallelogram spanned by $\mathbf{u}_1$, $\mathbf{u}_2$ is the basic parallelogram of the lattice. Translated copies of the basic parallelogram by lattice vectors tile the whole plane and we can visualize the lattice by this parallelogram tiling. A lattice has many different bases. The way how the plane is divided into parallelograms changes with different choices of the basis. However, the $\left|\det(\mathbf{u}_1, \mathbf{u}_2)\right|$, the area of the basic parallelogram, is independent of the choice of the basis. Similarly, the point set formed by the vertices of the parallelograms of the tiling remains the same. So the distances occurring between these points are invariant under changing the basis of the lattice. A lattice has many different bases and so to a lattice we assign many different quadratic forms. But all of them are equivalent as the linear transformation that takes a basis of the lattice to another basis has integer coefficients and determinant ±1. In short a lattice represents a family of equivalent quadratic forms.

3. Quadratic forms with common range

The quadratic forms in this section have real coefficients.

Theorem 1. *Let f and f' be positive definite binary quadratic forms of the same determinant. If f and f' have the same range for integer substitutions, then f and f' are equivalent.*

Proof. We divide the proof into smaller steps.

(1) Let L be the lattice spanned by the column vectors of the Cholesky decomposition of the matrix of f. Clearly, L as a vector set is an abelian group under addition and as a point set L is discrete, that is, it has no accumulation points. So the distances occurring between lattice points of L have a minimum value. Choose an element $\mathbf{u}$ of $L \setminus \{\mathbf{0}\}$ for which $|\mathbf{u}|$ is minimal. It is obvious that $|\mathbf{u}|^2$ is the minimum nonzero value of f for integer substitutions. We introduce a coordinate system such that the first coordinate axis is parallel to $\mathbf{u}$ and the origin of the coordinate system coincides with a lattice point. In this coordinate system $\mathbf{u}$ has coordinates u and 0.

The integer multiples of $\mathbf{u}$ form a sublattice M of L. From the minimality of $|\mathbf{u}| = u$ it follows that points from L on the first coordinate axis are identical with the points of M. These points divide the first coordinate axis into equal intervals of length u. Draw straight lines parallel to $\mathbf{u}$ through each points of L. Then consider the intersection of this family of lines by the second coordinate axis. Let S be the set of intersection points. If S has an accumulation point P, then in the square of side length $2u$ centered at P, there are infinitely many points from L. Since L does not have any accumulation point neither does S. Thus points of S divide the second coordinate axis into equal intervals of length, say v_2. There is an element $\mathbf{v}$ of $L \setminus M$ such that $|\mathbf{v}|$ is minimal. The second coordinate of $\mathbf{v}$ is v_2. Let the first coordinate of $\mathbf{v}$ be v_1. Let l_i be the translated copy of the first coordinate axis by the vector $i\mathbf{v}$. From the minimality of the distance v_2 it follows that the lines l_i together cover all points of L. Thus the vectors $\mathbf{u}$ and $\mathbf{v}$ form a basis for L.

(2) We claim that $v_2 \geq (\sqrt{3}/2)u$. In order to prove this claim consider open circular discs of radius u centered at the lattice points on the first coordinate axis. The union of these discs forms a strip. If a point P falls into the strip, say into the disc whose center is Q, then the distance between P and Q is less than u. Consequently, the strip cannot have any lattice point from L other than the centers of the discs. This verifies the claim.

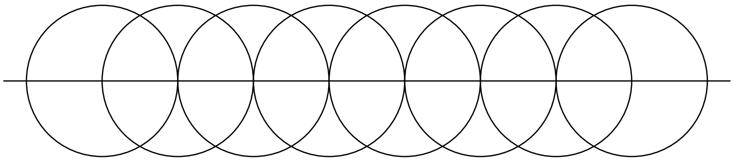

Figure 1

Further we claim that we may assume that $0 \leq v_1 \leq (1/2)u$. In order to verify this claim note that the lattice points of L on l_1 divide l_1 into intervals of length u. From the minimality of $|\mathbf{v}|$ it follows that the endpoint of $\mathbf{v}$ is the lattice point on l_1 closest to the second coordinate axis. Therefore $-(1/2)u \leq v_1 \leq (1/2)u$. If $v_1 < 0$, then we simply replace v_1 by $-v_1$ which corresponds to reflecting the whole lattice L to the second coordinate axis.

(3) Consider the circle C of radius $r = |\mathbf{v}|$ centered at the origin. We claim that C can intersect the straight line l_i only for $-1 \leq i \leq 1$. In other words we claim $r < 2v_2$. To prove the claim assume the contrary that $r \geq 2v_2$. Since $(u/2)^2 + v_2^2 \geq r^2$, it follows that $(u/2)^2 + v_2^2 \geq 4v_2^2$ and so $(u/2)^2 \geq 3v_2^2$. Using the fact that $v_2 \geq (\sqrt{3}/2)u$ we get $u^2/4 \geq (9/4)u^2$ which leads to the contradiction $1 \geq 9$.

Let L' be the lattice that corresponds to f'. In a similar way we constructed $\mathbf{u}$, $\mathbf{v}$ from f we construct $\mathbf{u}'$, $\mathbf{v}'$ from f'. We know that $|\mathbf{u}|^2$ is the minimum nonzero value of f for integer substitutions and similarly $|\mathbf{u}'|^2$ is the minimum nonzero value of f'. The ranges of f and f' are the same and so $|\mathbf{u}| = |\mathbf{u}'|$. We may assume that $\mathbf{u} = \mathbf{u}'$ since this is only a matter of changing the position of L'. The determinants of f and f' are the same and so it follows that $\big|\det(\mathbf{u}, \mathbf{v})\big| = \big|\det(\mathbf{u}, \mathbf{v}')\big|$. This gives that the endpoint of $\mathbf{v}'$ is on the line l_1. Let the coordinates of $\mathbf{v}'$ be v_1', v_2'. We know that $v_2' = v_2$. If $v_1' = v_1$, then $L' = L$ and there is nothing to prove. We may assume that $v_1 < v_1'$ since this is only a matter of exchanging the roles of f and f'.

(4) As f and f' have the same range for integer substitutions L' must have a point whose distance from the origin is r. In other words L' must have a point on the circle C. Points of L' are on the straight lines l_i. We claim that the intersections of C and l_0 are lattice points of L'.

From (3) we know that C can intersect l_i only for $-1 \leq i \leq 1$. The common points of C and l_1 are $Q = (v_1, v_2)$ and $Q^* = (-v_1, v_2)$ respectively. Here Q is the endpoint of $\mathbf{v}$ on l_1. If $Q \in L'$, then it follows that $\mathbf{v} = \mathbf{v}'$. This is not the case so $Q \notin L'$. If $Q^* \in L'$, then in the way we constructed $\mathbf{v}'$ we replaced $\mathbf{v}'$ by another vector whose endpoint is Q. Thus the only lattice point of L' in $C \cap l_1$ is Q. Similarly, the only lattice point of L' in $C \cap l_{-1}$ is the endpoint of $-\mathbf{v}$. Therefore the common points of C and l_0 must be lattice points of L'. A similar argument gives that the common points of C' and l_0 must be lattice points of L.

(5) Consider the points $Q = (v_1, v_2)$, $Q' = (v_1', v_2)$, $R = (r, 0)$, $R' = (r', 0)$. Points Q, Q' are intersection points of C, C' and l_1 respectively that have non-negative first coordinates. Points R, R' are intersection points of C, C' and l_0 respectively that have positive first coordinates. The distances between R and R' is $\alpha = r' - r$ and the distance between Q and Q' is $\beta = v_1' - v_1$.

We claim that $\alpha \geq u$. Indeed, from (4) we have that $R \in L'$. As $R \in l_0$ and along l_0 lattices L and L' identical, it follows that $R \in L$. Thus r is an integer multiple of u. From (4) we know that $R' \in L$. So a similar reasoning provides that r' is also an integer multiple of u. As $r \neq r'$, we get $\alpha = r' - r \geq u$.

Next we claim that $\beta \geq \alpha$. Indeed, a routine calculation shows that the function $g(y) = \sqrt{(r')^2 - y^2} - \sqrt{r^2 - y^2}$ attains its minimum at 0 on the interval $(-r, r)$. So $\beta = g(v_2) \geq g(0) = \alpha$ as we claimed.

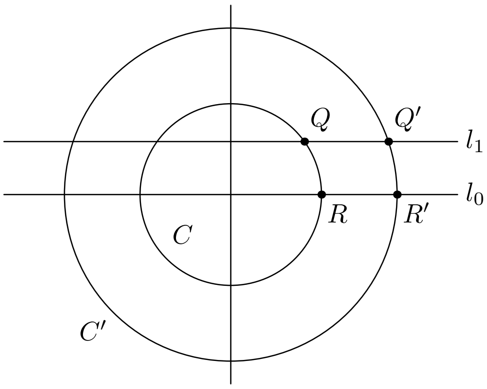

Figure 2

Note that $0 \leq v_1 < v_1' \leq u/2$ implies $u/2 \geq \beta$. Putting these facts together leads to the $u/2 \geq \beta \geq \alpha \geq u$ contradiction.

This completes the proof.

□

References

[1] C. F. Gauss, *Werke*, Vol. 2, König, Gesellschaft des Wiss, Göttingen, 1876.

[2] B. W. Jones, *The arithmetic theory of quadratic forms*, MAA Carus Math. Monographs, No. 10, 1950.

[3] K. Spindler, *Abstract algebra with applications*, Marcel Dekker, 1994.

[4] I. N. Stewart and D. O. Tall, *Algebraic number theory*, Chapman and Hall, 1987.

[5] G. L. Watson, *Integral quadratic forms*, Cambridge Univ. Press, 1960.

SÁNDOR SZABÓ
INSTITUTE OF MATHEMATICS AND INFORMATICS
UNIVERSITY OF PÉCS
H–7624 PÉCS, IFJÚSÁG U. 6.
HUNGARY

E-mail: sszabo7@hotmail.com

(Received August, 2004)