RATIONAL POINTS ON LINEAR SUBSPACES. REPRESENTATION OF AN INTEGER AS A SUM OF SQUARES WITH ACCESSORY CONDITIONS

T. S. MOTZKIN

1. Introduction. The present study was motivated by an investigation of algebraic conjugates in the complex plane (cf. **4** for one of the results) where some of its concepts are extended and applied.

Let F be a flat (linear subspace) in real affine n-space. The points $z = (\zeta_1, \ldots, \zeta_n)$ on F for which the least common denominator of the co-ordinates ζ_ν is minimum form a grid G, the *main grid* of F, studied in § 3. The minimum denominator κ, and a corresponding numerator ι, for a flat given by a system of linear equations with integral coefficients, and for a flat F through given points with rational co-ordinates, are determined in § 2. This section, which contains, in nuce, a geometric theory of systems of linear diophantine equations (with rational solutions), is concluded by a remarkable law of duality.

The volume of the fundamental cell of the main grid G depends on the denominator κ and on the *anomaly*, that is, the volume of the fundamental cell of the main grid of a parallel flat through an integral point. The anomalies are equal for orthogonal rational flats of m and $n - m$ dimensions. The square ω of the anomaly is a sum of squares without a common divisor, of integers that are minors of a matrix and therefore connected by bilinear relations. For $n \geqslant 5$, ω can be any positive integer; for $n \leqslant 4$, there are certain restrictions, which are completely determined in § 4.

2. The numerator and the denominator of a flat

2.1. A flat is multiplied or divided by a number λ by multiplying or dividing by λ every co-ordinate of each of its points.

A flat is *integral* if it contains a point with integral co-ordinates. An integral flat F is *primitive* if no F/ι is integral for integral $\iota > 1$. Let ι and κ be coprime positive integers, and

$$F' = (\iota/\kappa)F.$$

The number ι is the *numerator*, κ the *denominator*, and F is the *primitive* of F'. For a flat through O we define $\iota = 0$, $\kappa = 1$.

If F' consists of a single (rational) point r, then κ is the least common denominator, and ι is the greatest common divisor of the numerators, of the co-ordinates of r.

Received January 11, 1962.

The subspace $\rho F'$ with rational ρ is integral if and only if $\rho = \sigma\kappa/\iota$ with integral σ. The denominator κ is the least positive integer for which $\kappa F'$ is integral, and the least among the denominators of points of F'.

We have $\kappa = 1$ if and only if F' is integral, and $\kappa = \iota = 1$ if and only if F' is primitive.

It is easily seen that a linear transformation $\zeta_\nu' = \sum c_{\nu\lambda}\zeta_\lambda$ with a unimodular matrix $(c_{\nu\lambda})$, and no other linear transformation, leaves the numerator and denominator of every flat unchanged.

2.2. *The denominator κ of F' divides the denominator κ_1 of an arbitrary point r_1 of F'.*

Proof. The subspace F' contains a point r of denominator κ. Let

$$\kappa' = \sigma\kappa + \sigma_1\kappa_1$$

be the greatest common divisor of κ and κ_1. Then

$$r_2 = (\sigma\kappa r + \sigma_1\kappa_1 r_1)/\kappa'$$

is a point on the straight line through r and r_1. The denominator κ_2 of r_2 divides κ', hence also κ. Since $\kappa \leqslant \kappa_2$, we have $\kappa_2 = \kappa$ and $\kappa = \kappa'$.

2.3. A rational hyperplane H has an equation

$$\sum \sigma_\nu \zeta_\nu = \iota/\kappa$$

with coprime $\iota \geqslant 0$ and $\kappa \geqslant 1$, where ζ_ν are the co-ordinates of a point κ of H and the σ_ν are integers with no common divisor.

The numbers ι and κ are the numerator and the denominator of H.

Proof. The case $\iota = 0$ is trivial. For $\iota \neq 0$, note that the hyperplane $\sum \sigma_\nu \zeta_\nu = 1$ is integral and hence obviously primitive.

2.4. *A rational flat R* is given by a system of l equations

$$\sum \sigma_{\lambda\nu}\zeta_\nu = \sigma_\lambda, \qquad \lambda = 1, \ldots, l,$$

with integral $\sigma_{\lambda\nu}$ and σ_λ. Let a_μ be the greatest common divisor of the minors of order μ of the matrix $(\sigma_{\lambda\nu})$, and c_μ the greatest common divisor of all minors of order μ of the matrix $(\sigma_{\lambda\nu}, \sigma_\nu)$ that are not minors of the matrix $(\sigma_{\lambda\nu})$. Then R is integral if and only if a_μ divides c_μ for every $\mu = 1, \ldots, n - m$, where m is the number of dimensions of R (also, by a theorem of Frobenius, if and only if a_{n-m} divides c_{n-m}; cf. **2**, p. 84).

2.5. For every rational R we have:

The numerator and denominator of R are the numerator and denominator of the point $r = (c_1/a_1, \ldots, c_{n-m}/a_{n-m})$ of $(n - m)$-space.

Proof. If we multiply R by a prime p, then σ_λ, $\sigma_{\lambda\nu}$, c_μ, a_μ, r become in turn $\sigma_\lambda p$, $\sigma_{\lambda\nu}$, $c_\mu p$, a_μ, rp. If we divide R by p, they become σ_λ, $\sigma_{\lambda\nu}p$, $c_\mu p^{\mu-1}$, $a_\mu p^\mu$, r/p. Since the condition for integral R and r is the same, it follows that R and r have the same numerator and denominator.

If the flat R is given by another system of equations, the point r may change (the numerator and denominator remain, of course, unchanged). For example, for the system $\zeta_1 = 3, 3\zeta_2 = 3$, we have $r = (3, 1)$, while for $3\zeta_1 = 9$, $3\zeta_2 = 3$, we have $r = (1, 1)$.

2.6. For the smallest flat R through l given points

$$(\sigma_{\lambda 1}/\sigma_\lambda, \ldots, \sigma_{\lambda n}/\sigma_\lambda), \qquad \lambda = 1, \ldots, l,$$

with integral $\sigma_{\lambda\nu}$ and σ_λ, again let a_ν be the greatest common divisor of the minors of order μ of the matrix $(\sigma_{\lambda\nu})$, and c_μ the greatest common divisor of all other minors of order μ of the matrix $(\sigma_{\lambda\nu}, \sigma_\lambda)$. The point $r = (c_1/a_1, \ldots, c_{m+1}/a_{m+1})$ of $(m + 1)$-space (m being again the number of dimensions of R) may have its last co-ordinate equal to ∞; in this case we define $\iota(r) = 1$, $\kappa(r) = 0$. Then we have:

The flat R is integral if and only if $\iota(r) = 1$.

Proof. The four kinds of elementary transformations (change of sign of a row or column, addition of a row or column to another) that are sufficient to bring the matrix $(\sigma_{\lambda\nu})$ into its normal form, together with the corresponding changes of the σ_λ, affect neither the supposition nor the assertion. We may therefore assume $\sigma_{\mu\mu} = a_\mu/a_{\mu-1}$ (with $a_0 = 1$), $\mu = 1, \ldots, m + 1$, and all other $\sigma_{\kappa\nu} = 0$. If $a_{m+1} = 0$, $c_{m+1} \neq 0$, then R contains O. Otherwise, the equations of R are

$$\sum \sigma_\mu \zeta_\mu / \sigma_{\mu\mu} = 1, \qquad \zeta_{m+2} = \ldots = \zeta_n = 0.$$

Integral solutions ζ_μ exist if and only if the numerator of $(\sigma_1/\sigma_{11}, \ldots, \sigma_{m+1}/\sigma_{m+1,m+1})$ is 1. But a prime p is contained in every σ_μ to a higher power than in the corresponding $\sigma_{\mu\mu}$, if and only if the same is true for the numbers c_μ and a_μ. This completes the proof.

2.7. *For every rational R we obtain (defining r as in 2.6):*

$$\iota(R) = \kappa(r), \qquad \kappa(R) = \iota(r).$$

Proof. This follows from the preceding theorem by observing that if R is multiplied by a prime p (or $1/p$), then $\sigma_\lambda, \sigma_{\lambda\nu}, c_\mu, a_\mu, r$ become $\sigma_\lambda, \sigma_{\lambda\nu}p, c_\mu p^{\mu-1}$, $a_\mu p^\mu$, r/p (or respectively $\sigma_\lambda p$, $\sigma_{\lambda\nu}$, $c_\mu p$, a_μ, r/p).

2.8. By 2.5 and 2.7 we have:

The duality in which the point $\rho_1, \ldots, \rho_n$ corresponds to the hyperplane $\sum \rho_\nu \zeta_\nu = 1$ has the effect of interchanging the numerator and denominator of rational flats.

Corresponding flats are thus also arithmetically "reciprocal."

Using the last remark of 2.1 it is seen that the same duality law holds for every correlation $\sum \rho_\nu c_{\nu\lambda} \zeta_\lambda = 1$ with a unimodular matrix $(c_{\nu\lambda})$, and for no other correlation.

2.9. The *rational part* F_r of a flat F is the smallest flat of F_r that contains the rational points of F; it is the largest rational flat in F.

The rational points of F are dense in F_r.

Proof. Let $z = r_0 + \sum \zeta_\mu r_\mu$ with rational r_0, r_μ be a general point of F_r. In every neighbourhood of z there are points $r_0 + \sum \rho_\mu r_\mu$ with rational ρ_μ.

The numerator and denominator are defined for every flat F through a rational point.

Proof. They are the same as for F_r.

3. The main grid

3.1. The *main grid* of F is the set of the points of F with minimum denominator κ.

The main grid of F has the same dimension as F_r.

Proof. Let $s_0/\kappa + \sum \rho_\mu s_\mu$ with integral s_0 and s_μ and rational ρ_μ be a general rational point of F. Then there exist points $s_0/\kappa + \sigma \sum \rho_\mu s_\mu$, $\sigma \neq 0$, of denominator κ: choose σ so that the $\sigma \rho_\mu$ are integers.

3.2 The *relative co-ordinates* λ_μ of a point z of F_r are defined with regard to a basis $r_0 + r_\mu$ of the main grid of F, as the coefficients in the representation

$$z = r_0 + \sum \lambda_\mu r_\mu.$$

Rational points $r = r_0 + \sum \rho_\mu r_\mu$ have rational relative co-ordinates ρ_μ.

The denominator κ_1 of a rational point r of F equals $\kappa\kappa'$, where κ is the denominator of F and κ' is the common denominator of the ρ_μ.

Proof. By 2.2, κ divides κ_1. Put $\kappa_1 = \kappa\kappa_2$ with integral κ_2. The point

$$\kappa\kappa_2 r = \kappa\kappa_2 r_0 + \sum \kappa_2 \rho_\mu \cdot \kappa r_\mu$$

is integral only when the $\kappa_2 \rho_\mu$ are integers. Hence $\kappa_2 = \kappa'$.

3.3. *A system of m integral points z_μ forms a basis of the main grid of a flat through* 0 *if and only if the $\binom{n}{m}$ minors $d(\nu_1, \ldots, \nu_m)$, formed by the ν_1th, ..., ν_mth column, $1 \leqslant \nu_1 < \ldots < \nu_m \leqslant n$, of the matrix $\begin{pmatrix} z_1 \\ \ldots \\ z_m \end{pmatrix}$, have no common divisor* (**2**, p. 84, Frobenius).

Proof. The flat R through O and the points z_μ has the dimension m if the minors $d(\lambda_1, \ldots, \lambda_m)$ are not all 0. The points z_μ form a basis of the main grid of R if and only if the coefficients σ_μ are integers whenever $\sum \sigma_\mu z_\mu$ is integral. If the integral points z_μ are not a basis, then there exists an integral point $s = \sum \sigma_\mu z_\mu$ such that the coefficients σ_μ are not all integers, that is, that $(\sigma_1, \ldots, \sigma_m)$ has a denominator $\kappa > 1$, and $\kappa s = \sum(\kappa\sigma_\mu)z_\mu$ shows that the linear congruences $0 \equiv \sum \tau_\mu z_\mu$ modulo a prime p dividing κ have a solution τ_μ such that not all $\tau_\mu \equiv 0$; hence all the $\binom{n}{m}$ minors are $\equiv 0$ and have, therefore, the common divisor p. Conversely, if the minors are $\equiv 0$ modulo a prime p, then the congruences $0 \equiv \sum \tau_\mu z_\mu$ have a solution τ_μ such that not all $\tau_\mu \equiv 0$, and $\sum(\tau_\mu/p)z_\mu$ is integral while not all τ_μ/p are integers.

3.4. The $\binom{n}{m}$ minors $d(\nu_1, \ldots, \nu_m)$ fulfil the bilinear relations

$$d(\nu_1, \ldots, \nu_m)d(\nu'_1, \ldots, \nu'_m) = \sum_\mu d(\nu_1, \ldots, \nu_{m-1}, \nu'_\mu)d(\nu'_1, \ldots, \nu'_{\mu-1}, \nu_m, \nu'_{\mu+1}, \ldots, \nu'_m),$$

($d(\nu_2, \nu_1, \ldots)$ being defined as $-d(\nu_1, \nu_2, \ldots)$, etc.), $\binom{n}{m} - m(n-m) - 1$ of which are independent, and every $\binom{n}{m}$ numbers fulfilling these relations are minors of a matrix with rational elements (for example, **5**, p. 22).

Every $\binom{n}{m}$ integers that have no common divisor and fulfil these bilinear relations are minors of a matrix with integral elements.

Proof. The given integers are minors of a matrix $\begin{pmatrix} y_1 \\ \ldots \\ y_m \end{pmatrix}$ with rational elements. Let R be the rational flat of dimension m through O and the points $y_1, \ldots, y_m$, and let $z_1, \ldots, z_m$ be a basis of the main grid of R. Then $y_\mu = \sum c_{\nu\rho} z_\rho$, and the minors of the two matrices $\begin{pmatrix} y_1 \\ \ldots \\ y_m \end{pmatrix}$ and $\begin{pmatrix} z_1 \\ \ldots \\ z_m \end{pmatrix}$ differ by the constant factor

$$c = \begin{vmatrix} c_{11} & . & . & . \\ . & . & . & . \\ . & . & . & c_{mm} \end{vmatrix}.$$

The minors of either matrix being integers with no common divisor, we have $c = \pm 1$. For $c = -1$ replace z_1 by $-z_1$.

4. Values of the anomaly

4.1. The *cell size* of a flat F through a rational point is the volume of the fundamental cell of the main grid of F. If F contains only one rational point, the cell size is defined as 1.

The *anomaly* of a flat F is the cell size of a parallel flat F_0 through O. Its square ω is the sum of the squares of the minors $d(\nu_1, \ldots, \nu_m)$ of a basis of the main grid of F_0; hence ω is an integer.

The cell size of a flat of denominator κ with a rational part of m' dimensions is the square root of a rational number $\omega\kappa^{-2m'}$ and is greater than or equal to $\kappa^{-m'}$.

Proof. The number $\sqrt{\omega}$ is the cell size of κF and equal to $\kappa^{m'}$ times the cell size of F, and $\sqrt{\omega} \geqslant 1$.

4.2. *The anomalies of any two orthogonal rational flats of m and $n - m$ dimensions are equal.*

Proof. Suppose $0 < m < n$. Let $z_1, \ldots, z_m$ be a basis of the main grid of a rational flat R through O. There exist $z_{m+1}, \ldots, z_n$ such that $z_1, \ldots, z_n$ is a basis of the main grid of n-space.* Let the matrix $(y_1, \ldots, y_n)$ be the transpose of the inverse of the matrix $(z_1, \ldots, z_n)$; then y_ν is one of the two primitive points of the line through O orthogonal to the flat through O and all z_ρ with $\rho \neq \nu$. Now every minor of either matrix equals the complementary minor of the other (for example, **1**, p. 31). The flat through O determined by $y_{m+1}, \ldots, y_n$, which is orthogonal to R, has therefore the same anomaly as R.

In case $m = 1$, the proposition can also easily be verified as follows. The fundamental cell of the main grid of the hyperplane $\sum \sigma_\nu \zeta_\nu = 0$ (where the coefficients σ_ν are integers without a common divisor) is a side of a fundamental cell C of the grid of all integral points. The opposite side is on $\sum \sigma_\nu \zeta_\nu = 1$ (or -1), so that the distance between these sides is $(\sum \sigma_\nu^2)^{-\frac{1}{2}}$. The volume of C being 1, the volume of the side equals $(\sum \sigma_\nu^2)^{\frac{1}{2}}$, which is the anomaly of the straight line, orthogonal to the hyperplane, through O and $(\sigma_1, \ldots, \sigma_n)$.

4.3. *The square ω of the anomaly of a rational flat of a given number m of dimensions in n-space can be any positive integer for $n \geqslant 5$. For $n \leqslant 4$ there are the following exceptions:*

m (*or* $n - m$)	$n - m$ (m)	*Impossible values: integers of the form*
1	1	$4k$ *or* $(4l + 3)k$
1	2	$4k$ *or* $8k + 7$
1	3	$8k$
2	2	$16k$ *or* $16k + 12$ *or* $8k + 7$

By 3.4 this is equivalent to saying that every positive integer, with exceptions as stated, is the sum of $\binom{n}{m}$ squares of integers without a common divisor and connected by the bilinear relations indicated in 3.4.

By 4.2, the range of ω remains the same if m and $n - m$ are interchanged. Since the anomaly of a flat of m dimensions in n-space is also the anomaly

*A special case of this long-known result was reviewed as new in Math. Reviews, 7 (1946), 242 (the fourth paper).

https://doi.org/10.4153/CJM-1963-024-3 Published online by Cambridge University Press

of the same flat in $(n + 1)$-space, the range of ω cannot decrease for constant m and increasing $n - m$, hence the same is true for constant $n - m$ and increasing m. Our assertions need therefore only be proved for the given combinations $(m, n - m)$, and (the absence of exceptions) for $(1, 4)$ and $(2, 3)$, that is, in 5-space.

4.4. *Proof for* $m = 1$. There are no bilinear relations. The representation of an integer as a sum of n squares without a common divisor has been frequently treated. For $n = 3$, the numbers without a representation were given by Legendre (**2**, p. 261, footnote 5). For $n = 5$ one of the squares can be assumed to be 1; for $n = 4$, if a representation exists, it can be assumed to be 0 or 1.

Since 1/4 (1/8) of the representations of a positive integer ω as a sum of 2 (4) squares of integers (given, for example, in **3**, pp. 103-4 (113)) is a multiplicative function $f(\omega)$, the same is true for the function $g(\omega)$ whose value is 1/4 (1/8) of the number of *primitive* representations of ω. This follows easily from the formula

$$g(\omega) = f(\omega) - \sum f(\omega/p^2) + \sum f(\omega/(p^2q^2)) - + \dots,$$

where $p, q, \dots$ are the different primes whose squares divide ω. Therefore we have, for $\omega = \Pi p^\alpha$,

$$g(\omega) = \Pi(f(p^\alpha) - f(p^{\alpha-2})),$$

with $f(1) = 1$, $f(p^{-1}) = 0$. This gives immediately the value (**2**, pp. 241, 242, 288, 303) of $g(\omega)$ for every ω, and the above cases of $g(\omega) = 0$.

4.5. *Proof for* $m = 2$. For $n - m = 2$, let $s = (\sigma_1, \dots, \sigma_4)$, $s' = (\sigma_1', \dots, \sigma_4')$ be a basis of the main grid of a rational flat through O. The six minors of order 2 are connected by a single bilinear relation. The number ω is a sum of six squares

$$\sum a_i^2 + \sum b_i^2, \qquad i = 1, 2, 3,$$

with no common divisor and connected by the relation

$$\sum a_i b_i = 0,$$

whence $\omega = \sum (a_i + b_i)^2$. This is impossible for $\omega = 8k + 7$. For $\omega = 4k$, two squares belonging to the same i, say $i = 1$, are even, the others odd. Then $a_i^2 + b_i^2$, $i = 2, 3$, is 2 or 10 (mod 16), according as $a_i b_i$ is ± 1 or ± 3 (mod 8). Hence if $a_1^2 + b_1^2$ is 0, 4, or 8 (mod 16), with $a_1 b_1$ respectively 0, 0, or 4 (mod 8), then ω is 4, 8, or 4, and never 0 or 12 (mod 16).

To represent $\omega \not\equiv 4k, 8k + 7$, put all $b_i = 0$ (choosing $\sigma_4 = \sigma_4' = 0$). For $\omega = 16k + 4$ and $\omega = 16k + 8$, express $\omega/4$ as a sum $\sum c_i^2$ of three squares with no common divisor; supposing, as we may, c_2 even and c_3 odd, put

$$a_1 = 2c_1, \quad a_2 = a_3 = c_2 + c_3, \quad b_1 = 0, \quad b_2 = -b_3 = c_2 - c_3 \quad (\sigma_3 = \sigma_4, \sigma_3' = \sigma_4').$$

By 3.4, for every solution a_i, b_i there exists a matrix s, s'.

https://doi.org/10.4153/CJM-1963-024-3 Published online by Cambridge University Press

For $(m, n-m) = (2, 3)$, ω can be any positive integer. Indeed, the numbers excepted both for $(1, 3)$ and for $(2, 2)$ are those divisible by 16. But $s_1 = (1, 1, 0, 0, 0)$, $s_2 = (2, 0, \sigma_1, \sigma_2, \sigma_3)$ yields $\omega = 2\sum\sigma_i^2 + 4$; and every number $8k + 6$ is a sum $\sum\sigma_i^2$ with not all σ_i even.

References

1. M. Bôcher, *Higher algebra* (New York, 1907, 1947).
2. L. E. Dickson, *History of the theory of numbers*, Vol. II (Washington, 1920, 1934).
3. E. Landau, *Zahlentheorie*, Vol. I (Leipzig, 1927).
4. T. S. Motzkin, *Sur l'équation irréductible* $z_n + a_1 z^{n-1} + \ldots + a_n = 0$, $n > 1$, *à coefficients complexes entiers, dont toutes les racines sont sur une droite. Les 11 classes de droites admissibles.* C. R. Acad. Sci. Paris, *222* (1945), 221–223.
5. B. L. van der Waerden, *Algebraische Geometrie* (Berlin, 1939).

University of California, Los Angeles