ON THE CHARACTERISTIC POLYNOMIALS OF RATIONAL SYMMETRIC MATRICES OF THE THIRD ORDER

The purpose of the present note is to prove the following theorem:

1958

SovietRxiv

Abstract

Full Text

MATHEMATICS

A. P. SHAPIRO

ON THE CHARACTERISTIC POLYNOMIALS OF RATIONAL SYMMETRIC MATRICES OF THE THIRD ORDER

(Presented by Academician A. N. Kolmogorov on 30 XI 1957)

The purpose of the present note is to prove the following theorem:

Theorem. *In order that an irreducible polynomial $f(x)$ of the third degree with rational coefficients be the characteristic polynomial of a rational symmetric matrix, it is necessary and sufficient that all its roots be real.*

In papers ([13]) some sufficient conditions are given.

In paper ([2]) it is proved that, for the assertion of the theorem to hold, it is necessary and sufficient that there exist, in the field of algebraic numbers generated by a root θ of the polynomial $f(x)$, a number λ such that the quadratic form

$$g = \operatorname{Sp} \lambda (x\omega_1 + y\omega_2 + z\omega_3)^2,$$

where $\omega_1, \omega_2, \omega_3$ is a basis of the field $R(\theta)$, is equivalent (over the rationals) to a sum of three squares. For this, first of all it is necessary that $DN(\lambda)$ (D is the discriminant of the field $R(\theta)$)—the discriminant of the quadratic form g—be the square of a rational number. In what follows we shall denote this condition by $(*)$ and assume it to be fulfilled.

According to ([4]), the necessary and sufficient conditions for the rational equivalence of quadratic forms are: a) their equivalence over the field of real numbers; b) equivalence over the field R_p of p-adic numbers for every p. In our case a) means the positivity of λ together with its conjugates.

Lemma 1. *If $(p) = \gamma_1\gamma_2\gamma_3$ in $K = R(\theta)$, i.e. under extension of R to R_p $(p \neq 2)$ K_p decomposes into a direct sum of three fields, then a sufficient p-adic condition for the equivalence of g to a sum of three squares is that λ and p be relatively prime.*

Indeed, in this case $K_p = R_p^{(1)} + R_p^{(2)} + R_p^{(3)}$, and $g_p = \lambda_1 {x'}^2 + \lambda_2 {y'}^2 + \lambda_3 {z'}^2$, where g_p is the p-adic form corresponding to the form g, and λ_i is the component of λ contained in $R_p^{(i)}$. Condition $(*)$ gives that $\lambda_1\lambda_2\lambda_3$ is a square, and the lemma is proved by considering the cases: λ_i is a quadratic residue modulo the ideal γ_i; λ_i is a nonresidue.

Lemma 2. *If* $(p) = \gamma_1\gamma_2^2$, *i.e.* K_p $(p \neq 2)$ *decomposes into a direct sum* $R_p^{(1)} + Q_p^{(2)}$, *where* $R_p^{(1)} \cong R_p$, *and* $Q_p^{(2)}$ *is a quadratic ramified extension of* R_p, *then a sufficient* p*-adic condition for* λ *is the divisibility of* λ *by* γ_2 *to an odd degree.*

Lemma 3. *If* $(p) = \gamma_1\gamma_2$ *(*γ_1 *of degree 1,* γ_2 *of degree 2) and* $p \neq 2$, *i.e.* $K_p = R_p^{(1)} + Q_p^{(2)}$ *(*$Q_p^{(2)}$ *is here an unramified quadratic extension of* R_p*), then a sufficient condition for the equivalence of* g_p *to a sum of three squares is* $(\lambda, p) = 1$.

Lemma 4. *Let* $p \neq 2, 3$. *If* $(p) = \gamma^3$ *or* p *does not decompose in* K, *which corresponds to the case when* K_p *is a local field of the third degree,*

a sufficient condition for p-adic equivalence is: λ is divisible by γ (or by p) to an even power.

Here one must take into account the easily proved assertion that, in a local field of degree three, a number whose norm is a square is itself a square. Therefore condition $(*)$ determines λ up to a square. It remains to verify that for $\lambda = D$ the form g_p is equivalent to a sum of three squares.

Remark. $p = 3$ presents no difficulty, since the discriminant K_3 is a power of the number 3, and then it is represented by the form $x^2 + 2y^2$, and, according to ([3]), λ may be any 3-adic number satisfying $(*)$. In particular, $\lambda = D$.

In proving Lemmas 1, 2, 3 and 4 one should take into account:

$$
\begin{array}{lll}
1) & \nu x^2 + \nu y^2 + z^2 \sim x^2 + y^2 + z^2 & \text{for all } p; \\
 & \left.\begin{array}{l} px^2 + py^2 + z^2 \sim x^2 + y^2 + z^2 \end{array}\right\} & \text{only for } p = 4n+1; \\
 & p\nu x^2 + p\nu y^2 + z^2 \sim x^2 + y^2 + z^2 & \\
 & \nu x^2 + py^2 + p\nu z^2 \sim x^2 + y^2 + z^2 & \text{only for } p = 4n+3.
\end{array}
$$

Here ν is a quadratic non-residue modulo p, and $\sim$ denotes p-adic equivalence.

2) There are very few local fields of degrees 2 and 3. They can be listed. For example, there are only three local fields of degree two: $R_p(\sqrt{p})$, $R_p(\sqrt{\nu})$, $R_p(\sqrt{p\nu})$.

Let us consider separately the case $p = 2$:

1) $(2) = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$. Here a sufficient condition for λ is $\lambda \equiv 1 \pmod 8$, since the numbers $\equiv 1 \pmod 8$ are squares.

2) If 2 does not split in K, then $\lambda \equiv 1 \pmod 8$. This follows from the normality of the unramified extension and ([3]).

3) $(2) = \mathfrak{a}^3$. In this case $K_2(\theta)$ contains $\sqrt[3]{2}$, while $K(\theta)$ contains π such that

$$\pi \equiv \sqrt[3]{2} \pmod 8.$$

Indeed, let α be a number of $K(\theta)$ divisible by $\mathfrak{a}$ to the first power. Then $\alpha^3 = 2\eta$, where $(\eta, 2) = 1$. But any number relatively prime to 2 is congruent modulo 8 to the cube of another number. Therefore $\eta \equiv \beta^3 \pmod 8$, and $(\alpha/\beta)^3 = 2\eta_1$, where $\eta_1 \equiv 1 \pmod 8$. It remains to put $\pi = \alpha/\beta$, since the cube root of unity is unity. A sufficient condition for λ in this case will be:

$$\lambda \equiv -1 + \pi + 2\pi^2 \pmod 8.$$

4) $(2) = \mathfrak{a}_1\mathfrak{a}_2^2$ or $(2) = \mathfrak{a}\mathfrak{b}$, where $\mathfrak{b}$ is a prime ideal of the second degree. Here one must consider subcases depending on the discriminant a of the quadratic extension $R_2(\sqrt{a})$ corresponding to $\mathfrak{a}_2^2$ or $\mathfrak{b}$.

For $a = 2$, $\lambda \equiv -5 \pmod 8$; for $a = -2$, $\lambda \equiv 5 \pmod 8$; for $a = 5$, $\lambda \equiv -1 \pmod 8$; for $a = -5$, $\lambda \equiv 1 \pmod 8$; for $a = 10$, $\lambda \equiv -1 \pmod 8$; for $a = -10$, $\lambda \equiv 1 \pmod 8$; for $a = -1$, $\lambda \equiv 1 + 2\rho \pmod 8$. ρ is a number of $R(\theta)$ which in $R_2(\sqrt{-1})$ satisfies the congruence

$$\rho \equiv \sqrt{-1} \pmod 8.$$

The proof of the existence of ρ is analogous to the proof of the existence of π.

Note. λ may be multiplied by the square of any number.

Put $\lambda = Dx$, where x is a number whose norm is a square, $N(x) = m^2$. It is known that such x are representable in the form $x = \mu'\mu''$ ($N(\mu) = m$, μ' and μ'' are conjugate to μ), $\lambda = D\mu'\mu''$. For such λ, condition $(*)$ is satisfied automatically. Lemmas 1, 3 and 4 give no conditions on μ, except $(\mu, p) = 1$. Lemma 2 shows that μ must be divisible by γ_2. The 2-adic conditions in cases 1), 2), 4) (except $a = -1$) can be satisfied, taking into account the note,

$$\mu \equiv 1 \pmod 8. \tag{I}$$

In case 3), $D = 4D_1$, $D_1 \equiv 1 \pmod 4$, and

$$\mu \equiv 1 + \pi - \pi^2 \pmod 8. \tag{II}$$

In case 4) and $a = -1$

$$\mu \equiv 1 - 2\rho \pmod 8. \tag{III}$$

Take the product γ_2 over all p satisfying the condition of Lemma 2, $\gamma_2^{(1)}\gamma_2^{(2)}\cdots\gamma_2^{(k)}$. According to the generalized theorem on arithmetic progression [(5)], there exists a prime ideal c such that $\gamma_2^{(1)}\gamma_2^{(2)}\cdots\gamma_2^{(k)}c = (\mu)$ is a principal ideal and μ satisfies conditions (I), (II), or (III), depending on the arithmetic structure of the discriminant D. Then all p-adic conditions for the equivalence of g to a sum of squares will be satisfied, except, possibly, the condition for p whose divisor is c. We shall prove the fulfillment of the p-adic condition also for this p.

For this purpose consider the algebra of generalized quaternions over the field R with basis $1, i, j, k$ and multiplication table

$$i^2 = -D\mu'\mu'', \quad j^2 = -D\mu''\mu', \quad k^2 = -D\mu\mu',$$

$$ij = -ji = \sqrt{D\mu''}\,k, \quad jk = -kj = \sqrt{D\mu}\,i, \quad ki = -ik = \sqrt{D\mu'}\,j.$$

The equivalence of this algebra to the algebra of ordinary quaternions is equivalent to the equivalence of g to a sum of three squares. The same may be said about the p-adic equivalence of algebras and quadratic forms (the transformation of the variables of the form corresponds to the transformation of the basis in the algebra). But for algebras the reciprocity law [(5)] holds, according to which the fulfillment of the conditions of real and p-adic equivalence for all p, except one, entails the p-adic equivalence of the algebras also for this last p. In view of the correspondence indicated above, the same is true for quadratic forms. The theorem is proved.

Leningrad State University
named after A. A. Zhdanov

Received
5 IX 1957

REFERENCES

[1] D. S. Gorshkov, DAN, 31, No. 9 (1941).
[2] D. K. Faddeev, DAN, 58, No. 5 (1947).
[3] D. K. Faddeev, DAN, 47, No. 8 (1945).
[4] H. Hasse, Math. Ann., 107, 731 (1933).
[5] H. Hasse, *Zahlentheorie*, Berlin, 1949.

Note: Figure translations are in progress. See original paper for figures.